



Morgan Lewis

# INVESTMENT ADVISER PERSPECTIVES:

**DIGITAL ADVICE ROUNDTABLE**

Supplementary Materials

## table of contents

### tab

Compliance Options for Offering Affiliated Funds and Managers under ERISA and IRC Section 4975	1
OCC Supervisory Guidance on Model Risk Management (April 2011)	2
Investor Alert: Automated Investment Tools (May 2015)	3
Report on Digital Investment Advice (March 2016)	4
J.P. Morgan Securities LLC No-Action Letter (April 2018)	5
IM Guidance Update 2017 – 02 on Robo-Advisers (February 2017)	6
Investor Bulletin: Robo-Advisers (February 2017)	7
Risk Alert: Observations from Cybersecurity Examinations (August 2017)	8
SEC Electronic Investment Advice Initiative – Redacted Information Request (September 2017)	9
CFPB Consumer Protection Principles for Consumer-Authorized Financial Data Sharing and Aggregation (October 2017)	10
Examination Priorities for 2018	11
U.S. Government Accountability Office Report on Financial Technology: Additional Steps by Regulators to Better Protect Consumers and Aid Regulatory Oversight (March 2018)	12
Proposed Commission Interpretation on Investment Adviser Standards of Conduct (April 2018)	13
SIFMA White Paper: Promoting Innovation in Financial Services (April 2018)	14
SIFMA Data Aggregation Principles (April 2018)	15
OCC Policy Statement on National Bank Charters for Financial Technology Companies (July 2018)	16
U.S. Department of the Treasury Report on Nonbank Financials, Fintech and Innovation (July 2018)	17
Quantitative Investment Models Enforcement Actions: Transamerica Entities and Related Persons (August 2018)	18
Risk Alert: Compliance Issues on the Cash Solicitation Rule (October 2018)	19

Tab 1

# Compliance Options for Offering Affiliated Funds and Managers Under ERISA and IRC Section 4975

<u>Approach*</u>	<u>Conditions/Requirements</u>	<u>Pros/Cons/Considerations</u>
<p><b>Prohibited Transaction Exemption 77-4</b></p> <ul style="list-style-type: none"> <li>Available for advised brokerage and advisory (non-discretionary and discretionary)</li> <li>Applies equally to ERISA plans and IRAs</li> <li>Available only for affiliated open-end investment companies/mutual funds/ETFs <ul style="list-style-type: none"> <li>Not available for closed-end funds, non-registered investment companies or other collective investment funds</li> </ul> </li> <li>Only available for cash purchases <ul style="list-style-type: none"> <li>Not available for in-kind purchases</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>No sales commissions or 12b-1 fees payable to the fund investment adviser or its affiliates may be charged to the Plan or IRA;</li> <li>No redemption fees may be charged to the Plan or IRA, unless (i) paid to the mutual fund and (ii) disclosed in the fund's prospectus in effect both at the time of purchase and the time of sale;</li> <li>The Plan or IRA may not pay duplicative investment advisory fees. Plan- or IRA-level advisory fees can either be waived or offset by advisory or similar fees received at the mutual fund level;</li> <li>The arrangement must be disclosed to, and approved by, an independent Plan or IRA fiduciary, who must receive a current prospectus and full and detailed disclosure of the investment advisory and other fees charged to or paid by the Plan or IRA and the mutual fund;</li> <li>Any changes in fees must be approved, in writing, by the independent fiduciary;</li> <li>ERISA Plan fiduciaries are required to meet their obligations of prudence, exclusive benefit and diversification when authorizing investment of Plan assets in proprietary mutual funds; and</li> <li>Prior to the DOL Fiduciary Rule being vacated, required to meet the impartial conduct standards – “best interest,” reasonable compensation, and no misleading statements.</li> </ul>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>Commonly used</li> <li>Specifically available for affiliated mutual funds</li> <li>Broad relief for secondary service fees</li> <li>Fixed fee credit back approach may work, so long as credit always exceeds the mutual fund management/advisory fee</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>No double layer of management/advisory fees, pricing issues where program includes both affiliated and third-party funds as account-level program fee may be too high for third-party funds where there is no credit back</li> <li>Express/wet signatures required for fee changes/adding new funds</li> <li>Prospectus delivery before initial purchase</li> <li>Complicated fee disclosures to clients</li> <li>Credit backs are difficult to administer/many get them wrong</li> <li>Does not cover affiliated managers or models</li> </ul>
<p><b>Direct Expenses</b></p> <ul style="list-style-type: none"> <li>Available for advised brokerage and advisory (non-discretionary and discretionary)</li> <li>Applies equally to ERISA plans and IRAs</li> <li>Available for affiliated mutual funds and managers</li> </ul>	<ul style="list-style-type: none"> <li>Subject to various requirements, regulations under ERISA (which also apply to the IRC) permit transactions in which service providers and fiduciaries receive only direct expenses under the “but for” test and no indirect or other expenses (including overhead).</li> <li>Under the “but for” test a fee or compensation is paid in connection with or as a result of such transaction or service if the fee or compensation would not have been paid ‘but for’ the transaction or service or if eligibility for or the amount of the fee or compensation is based in whole or in part on the transaction or service.</li> </ul>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>Statutorily permitted</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>Administratively cumbersome to operationalize</li> <li>Allocations between clients, products, etc. difficult</li> <li>No additional revenue to firm</li> </ul>



# Compliance Options for Offering Affiliated Funds and Managers Under ERISA and IRC Section 4975

Approach*	Conditions/Requirements	Pros/Cons/Considerations
<b>Offset/COUNTRY Trust</b> <ul style="list-style-type: none"> <li>Available for advised brokerage and advisory (non-discretionary and discretionary)</li> <li>Applies equally to ERISA plans and IRAs</li> <li>Available for affiliated mutual funds and managers</li> </ul>	<b>Three Separate Approaches (Need to comply with one)</b> <ul style="list-style-type: none"> <li>“Dollar-for-dollar” credit of the exact amount of additional compensation it receives as a result of client investments in funds the fiduciary recommends or invests in. The DOL approved this approach in DOL Adv. Op. 2005-10A.</li> <li>Fixed Fee Credits (not addressed by DOL guidance) where the fiduciary provides an automatic fixed fee credit generally based on the highest amount of compensation the fiduciary can receive from any fund against the client’s account-level fee, and would also generally credit back to the client account any amounts the fiduciary (or its affiliates) receives from the funds in excess of the fixed fee credit amount.</li> <li>Fund-Level Compensation Waivers: Another approach would be for the fiduciary to waive its right to receive any additional compensation it (or its affiliate) would otherwise be entitled to receive from or with respect to services provided at the fund level. Difficult to apply where such compensation is receivable by affiliates.</li> </ul>	<b>Pros</b> <ul style="list-style-type: none"> <li>Broad application with minimal client disclosures</li> <li>Flexibility in adding new funds/models/affiliated managers</li> <li>May work well with dedicated fund family</li> <li>May be able to qualify as “Level Fee Fiduciary” under BIC Exemption</li> </ul> <b>Cons</b> <ul style="list-style-type: none"> <li>No secondary service fees</li> <li>Difficult to price program that involves both inside and outside funds</li> <li>Unlike PTE 77-4—can’t waive account-level fee in lieu of fund-level fee</li> <li>Fixed fee credit back approach may not be available</li> <li>No additional revenue to firm</li> </ul>
<b>SunAmerica</b> <ul style="list-style-type: none"> <li>Available for advisory (non-discretionary and discretionary)</li> <li>Applies to ERISA plans and IRAs (but certain limits for IRAs may apply)</li> <li>Guidance applies to affiliated mutual funds</li> </ul>	<ul style="list-style-type: none"> <li>Level client fee that remains the same regardless of the underlying investments.</li> <li>Non-discretionary investment advice or discretionary investment decisions must be provided by an unaffiliated investment professional or software developed by an independent entity.</li> <li>May provide non-advisory “support” to the independent expert in the form of financial information, models, etc.</li> <li>No discretion to deviate from the independent entity’s determinations.</li> </ul>	<b>Pros</b> <ul style="list-style-type: none"> <li>Commonly used</li> <li>Generally structured to avoid conflicts</li> <li>Though not specifically covered by the guidance, should generally be available for use of affiliated managers and models, in addition to funds</li> </ul> <b>Cons</b> <ul style="list-style-type: none"> <li>Need third party to develop software</li> <li>Unclear how to create universe of funds/managers/models for expert to choose from for IRAs, including proprietary products and products that pay third-party compensation. For plans, the independent plan fiduciary can bless universe; For IRAs, DOL questions whether IRA owner is competent to make such determination.</li> <li>No specific guidance covering affiliated managers/ models</li> <li>May not be able to qualify as “Level Fee Fiduciary” under BIC Exemption</li> </ul>

# Compliance Options for Offering Affiliated Funds and Managers Under ERISA and IRC Section 4975

<u>Approach*</u>	<u>Conditions/Requirements</u>	<u>Pros/Cons/Considerations</u>
<b>ETFs (Creation Unit Approach)</b> <ul style="list-style-type: none"><li>• Available for advised brokerage and advisory (non-discretionary and discretionary)</li><li>• Applies equally to ERISA plans and IRAs</li><li>• Available for affiliated exchange traded fund</li></ul>	<ul style="list-style-type: none"><li>• Fiduciary investments do not create additional compensation because such trading is within a range of normal floats, and additional creation units are not created.</li><li>• Fund use will be discontinued where trading volume limits are violated</li><li>• Policies and procedures are adopted to managed and address trading volume analysis</li></ul>	<b>Pros</b> <ul style="list-style-type: none"><li>• Broad application with minimal client disclosures</li><li>• Flexibility in adding new funds</li></ul> <b>Cons</b> <ul style="list-style-type: none"><li>• No secondary service fees</li><li>• Difficult to create effective compliance rules</li><li>• Issues arise where funds violate trading levels</li></ul>

# Compliance Options for Offering Affiliated Funds and Managers Under ERISA and IRC Section 4975

Approach*	Conditions/Requirements	Pros/Cons/Considerations
<p><b>ERISA § 408(g)/IRC § 4975(f)(8) for Human Investment Advice</b></p> <ul style="list-style-type: none"> <li>• Available non-discretionary advice only</li> <li>• Applies equally to ERISA plans and IRAs</li> <li>• Available for affiliated mutual funds and managers</li> </ul>	<ul style="list-style-type: none"> <li>• Level fees to the advice provider entity (and representative) : direct or indirect fees or compensation from any party (including an affiliate of the fiduciary adviser entity) paid to the fiduciary advice provider entity (including any employee, agent, or registered representative thereof, but not affiliates that do not provide advice) must not vary based on investment selection. Thus, a separate entity must be used to separate advice provider from variable compensation.</li> <li>• Investment advice (generated exclusively by advice provider entity): <ul style="list-style-type: none"> <li>○ is based on generally accepted investment theories that at least take into account historic risk and returns of different asset classes over defined periods of time;</li> <li>○ considers fees and expenses; and</li> <li>○ considers participant and beneficiary information relating to age, time horizons, risk tolerance, current investments in designated investment options, other assets or sources of income, and investment preferences. <ul style="list-style-type: none"> <li>• Must seek the information and consider it to the extent provided.</li> </ul> </li> </ul> </li> <li>• Arrangement must be authorized by plan fiduciary or IRA beneficiary, who, subject to certain exceptions, is not the person offering the advice program (or an affiliate) or the person providing investment options under the plan (or an affiliate).</li> <li>• Independent audit required at least annually to confirm compliance with these requirements and report findings to plan fiduciaries and IRAs, and noncompliance findings reported to DOL.</li> <li>• Written disclosure to participants before initial advice and updates, on such items as past performance, fees to be received, fiduciary status.</li> <li>• Written disclosure to fiduciary that authorizes arrangement.</li> <li>• Other miscellaneous requirements: fiduciary adviser compensation is reasonable, transactions at arm's length, other disclosure</li> <li>• Six year recordkeeping requirement.</li> </ul>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Broad applicability</li> <li>• May cover rollover advice, but currently unclear</li> <li>• No impartial conduct standards required</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• Need separate entity</li> <li>• Currently in limited use, but coming on line</li> <li>• Need for independent auditor to certify program compliance annually</li> <li>• Need wet signature</li> <li>• Limited to non-discretionary advice only, but can use negative consent changes broadly</li> <li>• Need for separate entity to segregate advice provider from recipient of variable compensation</li> <li>• Need to ensure advice providers, including portfolio managers, are segregated from compensation incentives and arrangements</li> <li>• Need to meet "generally accepted investment theories"</li> </ul>
<p><b>ERISA § 408(g)/IRC § 4975(f)(8) for Computer Models</b></p> <ul style="list-style-type: none"> <li>• Same as directly above</li> </ul>	<ul style="list-style-type: none"> <li>• Same as directly above, plus</li> <li>• The only advice provided must be advice generated by a computer model.</li> <li>• Computer model must meet certain standards specified in the statute and the regulations</li> <li>• An investment expert (who meets certain specific criteria) must certify, in writing, that the computer model meets specified requirements prior to use and upon any material modification of the computer model.</li> </ul>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• No need for separate entity</li> <li>• Broad applications</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• Need computer expert in addition to independent auditor</li> <li>• Need new certification for each change in algorithm</li> <li>• Need to ensure no human interaction with creation and transmission of advice</li> <li>• Likely to not qualify as "Level Fee Fiduciary"/streamlined BIC where proprietary products are used</li> </ul>

# Compliance Options for Offering Affiliated Funds and Managers Under ERISA and IRC Section 4975

<u>Approach*</u>	<u>Conditions/Requirements</u>	<u>Pros/Cons/Considerations</u>
<b>ERISA § 408(b)(4)/IRC § 4975(d)(4)</b> <ul style="list-style-type: none"><li>• Available for advised brokerage and advisory (non-discretionary and discretionary)</li><li>• Applies equally to ERISA plans and IRAs</li><li>• Available for bank deposits</li></ul>	<ul style="list-style-type: none"><li>• Investments made in deposits of a financial institution that is a bank (within the meaning of Section 581 of the IRC) that is supervised by the United States or a State and that is an affiliate of the fiduciary;</li><li>• The deposits bear a reasonable rate of interest; and</li><li>• The investment is expressly authorized by either (i) a plan provision authorizing investments in deposits of the specific bank, by name, that bear a reasonable rate of interest, or (ii) a plan fiduciary independent of the bank.</li></ul>	

# Compliance Options for Offering Affiliated Funds and Managers Under ERISA and IRC Section 4975

Approach*	Conditions/Requirements	Pros/Cons/Considerations
<p><b>Best Interest Contract (“BIC”) Exemption (So-Called “Full BIC”)</b></p> <ul style="list-style-type: none"> <li>Available for advised brokerage and non-discretionary advisory (does not apply to discretionary management or “robo” advice)</li> <li>Available for IRAs and small plans (does not apply to recommendations made to sophisticated (\$50MM) fiduciaries)</li> <li>Covers variable compensation and Riskless Principal Transactions (as defined in the BIC Exemption)</li> <li><b>NOTE:</b> May be vacated by a recent court decision</li> </ul>	<ul style="list-style-type: none"> <li>Impartial conduct standards (“ICS”); best interest advice, reasonable compensation, and no misleading statements</li> <li>Policies and procedures reasonably and prudently designed to ensure that FAs adhere to ICS. Focus on material conflicts of interest and FA compensation arrangements and programs.</li> <li>Contracts for non-ERISA plans and IRAs and disclosures for ERISA plans: prohibited contractual provisions (exculpatory provisions, class action waivers and unreasonable arbitration/mediation provisions), copy of contract on web, fiduciary acknowledgement, adherence to ICS, warranties for adherence to policies and procedures and material conflicts of interest).</li> <li>Single document disclosure requirement</li> <li>Transaction, upon-request, and web disclosures</li> <li>Required “conflicts officer”; internally designated</li> <li>Recordkeeping and notice requirements. Must notify DOL of intent to rely on Full BIC</li> <li>Special rules for platform limitations, such as proprietary products/third-party compensation</li> </ul> <p><b>NOTE – THIS EXEMPTION WAS VACATED BY FIFTH CIRCUIT DECISION. DOL/IRS NON-ENFORCEMENT POLICY IN EFFECT BASED ON GOOD FAITH EFFORTS TO COMPLY WITH IMPARTIAL CONDUCT STANDARDS.</b></p>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>Broad applicability to keep variable compensation</li> <li>Use consistent with DOL’s intent</li> <li>Does not require separate entities, but separate entities may be helpful for compliance</li> <li>May be used as a competitive advantage</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>Private right of action for IRAs and state court class action risk</li> <li>Burdensome; difficult to comply with from both technical and practical standpoints</li> <li>Lack of guidance regarding technical compliance</li> <li>Application of ICS may, in practice, require material leveling of compensation to FAs and potentially to firm</li> <li>Lack of guidance on determination and scope of material conflicts of interest</li> <li>Concerns/exposure relating to reasonable compensation under the BIC</li> <li>Does not cover extensions of credit</li> <li>Does not apply to “robo” advice</li> </ul>



# Compliance Options for Offering Affiliated Funds and Managers Under ERISA and IRC Section 4975

Approach*	Conditions/Requirements	Pros/Cons/Considerations
<p><b>Streamlined or Level Fee Fiduciary BIC</b></p> <ul style="list-style-type: none"> <li>Available for recommendations into level/asset based fee advisory program and arrangements, including “robo” advice products</li> <li>Available for IRAs and small plans (does not apply to recommendations made to sophisticated (\$50MM) fiduciaries)</li> <li><b>NOTE:</b> May be vacated by a recent court decision</li> </ul>	<ul style="list-style-type: none"> <li>Firm and its affiliates (and FA) can only receive level, non-transaction-based compensation. Sales commissions and other transaction-based compensation prohibited.</li> <li>Impartial conduct standards (“ICS”); best interest advice, reasonable compensation, and no misleading statements</li> <li>Must provide written acknowledgment of fiduciary status</li> <li>Document specific bases for recommendation; different requirements apply with respect to plan to IRA vs. IRA to IRA.</li> <li>Technically, special rules for platform limitations, such as proprietary product/third-party compensation, but unclear if such limitations are actually permissible.</li> </ul> <p><b>NOTE – THIS EXEMPTION WAS VACATED BY FIFTH CIRCUIT DECISION. DOL/IRS NON-ENFORCEMENT POLICY IN EFFECT BASED ON GOOD FAITH EFFORTS TO COMPLY WITH IMPARTIAL CONDUCT STANDARDS.</b></p>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>No contract requirements</li> <li>Limited disclosures required</li> <li>Use consistent with DOL’s intent</li> <li>May be used as a competitive advantage</li> <li>Easier to comply with as compared to Full BIC</li> <li>Covers recommendation generated by computer/algorithm</li> <li>ICS exposure limited to enrollment/rollover recommendation</li> <li>Covers “robo” advice</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>Narrow, limited, and potentially changing guidance with respect to qualifying arrangements.</li> <li>Unclear whether: <ul style="list-style-type: none"> <li>Products with affiliated bank sweep qualify</li> <li>Credit backs are permitted (Frost/Country Trust)</li> <li>Reliance on other exemptions, including PTE 77-4, is permissible</li> </ul> </li> <li>Potential for private right of action for IRAs and state court class action risk by reason of the fiduciary acknowledgement</li> <li>Concerns/exposure over reasonable compensation under the BIC</li> </ul>

Tab 2

---

Board of Governors of the Federal Reserve System  
Office of the Comptroller of the Currency

---

April 4, 2011

**SUPERVISORY GUIDANCE ON  
MODEL RISK MANAGEMENT**

**CONTENTS**

I. Introduction .....	1
II. Purpose and Scope .....	2
III. Overview of Model Risk Management.....	3
IV. Model Development, Implementation, and Use .....	5
V. Model Validation .....	9
VI. Governance, Policies, and Controls .....	16
VII. Conclusion.....	21

**I. INTRODUCTION**

Banks rely heavily on quantitative analysis and models in most aspects of financial decision making.<sup>1</sup> They routinely use models for a broad range of activities, including underwriting credits; valuing exposures, instruments, and positions; measuring risk; managing and safeguarding client assets; determining capital and reserve adequacy; and many other activities. In recent years, banks have applied models to more complex products and with more ambitious scope, such as enterprise-wide risk measurement, while the markets in which they are used have also broadened and changed. Changes in regulation have spurred some of the recent developments, particularly the U.S. regulatory capital rules for market, credit, and operational risk based on the framework developed by the Basel Committee on Banking Supervision. Even apart from these regulatory considerations, however, banks have been increasing the use of data-driven, quantitative decision-making tools for a number of years.

The expanding use of models in all aspects of banking reflects the extent to which models can improve business decisions, but models also come with costs. There is the direct cost of devoting resources to develop and implement models properly. There are also the potential indirect costs of relying on models, such as the possible adverse consequences (including financial loss) of decisions based on models that are incorrect or misused. Those consequences should be addressed by active management of model risk.

---

<sup>1</sup> Unless otherwise indicated, *banks* refers to national banks and all other institutions for which the Office of the Comptroller of the Currency is the primary supervisor, and to bank holding companies, state member banks, and all other institutions for which the Federal Reserve Board is the primary supervisor.

This guidance describes the key aspects of effective model risk management. Section II explains the purpose and scope of the guidance, and Section III gives an overview of model risk management. Section IV discusses robust model development, implementation, and use. Section V describes the components of an effective validation framework. Section VI explains the salient features of sound governance, policies, and controls over model development, implementation, use, and validation. Section VII concludes.

## II. PURPOSE AND SCOPE

The purpose of this document is to provide comprehensive guidance for banks on effective model risk management. Rigorous model validation plays a critical role in model risk management; however, sound development, implementation, and use of models are also vital elements. Furthermore, model risk management encompasses governance and control mechanisms such as board and senior management oversight, policies and procedures, controls and compliance, and an appropriate incentive and organizational structure.

Previous guidance and other publications issued by the OCC and the Federal Reserve on the use of models pay particular attention to model validation.<sup>2</sup> Based on supervisory and industry experience over the past several years, this document expands on existing guidance—most importantly by broadening the scope to include all aspects of model risk management. Many banks may already have in place a large portion of these practices, but all banks should ensure that internal policies and procedures are consistent with the risk management principles and supervisory expectations contained in this guidance. Details may vary from bank to bank, as practical application of this guidance should be customized to be commensurate with a bank’s risk exposures, its business activities, and the complexity and extent of its model use. For example, steps taken to apply this guidance at a community bank using relatively few models of only moderate complexity might be significantly less involved than those at a larger bank where use of models is more extensive or complex.

---

<sup>2</sup> For instance, the OCC provided guidance on model risk, focusing on model validation, in OCC 2000-16 (May 30, 2000), other bulletins, and certain subject matter booklets of the *Comptroller’s Handbook*. The Federal Reserve issued SR Letter 09-01, “Application of the Market Risk Rule in Bank Holding Companies and State Member Banks,” which highlights various concepts pertinent to model risk management, including standards for validation and review, model validation documentation, and back-testing. The Federal Reserve’s *Trading and Capital-Markets Activities Manual* also discusses validation and model risk management. In addition, the advanced-approaches risk-based capital rules (12 CFR 3, Appendix C; 12 CFR 208, Appendix F; and 12 CFR 225, Appendix G) contain explicit validation requirements for subject banking organizations.

### III. OVERVIEW OF MODEL RISK MANAGEMENT

For the purposes of this document, the term *model* refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. A *model* consists of three components: an information input component, which delivers assumptions and data to the model; a processing component, which transforms inputs into estimates; and a reporting component, which translates the estimates into useful business information. Models meeting this definition might be used for analyzing business strategies, informing business decisions, identifying and measuring risks, valuing exposures, instruments or positions, conducting stress testing, assessing adequacy of capital, managing client assets, measuring compliance with internal limits, maintaining the formal control apparatus of the bank, or meeting financial or regulatory reporting requirements and issuing public disclosures. The definition of *model* also covers quantitative approaches whose inputs are partially or wholly qualitative or based on expert judgment, provided that the output is quantitative in nature.<sup>3</sup>

Models are simplified representations of real-world relationships among observed characteristics, values, and events. Simplification is inevitable, due to the inherent complexity of those relationships, but also intentional, to focus attention on particular aspects considered to be most important for a given model application. Model quality can be measured in many ways: precision, accuracy, discriminatory power, robustness, stability, and reliability, to name a few. Models are never perfect, and the appropriate metrics of quality, and the effort that should be put into improving quality, depend on the situation. For example, precision and accuracy are relevant for models that forecast future values, while discriminatory power applies to models that rank order risks. In all situations, it is important to understand a model's capabilities and limitations given its simplifications and assumptions.

The use of models invariably presents model risk, which is the potential for adverse consequences from decisions based on incorrect or misused model outputs and reports. Model risk can lead to financial loss, poor business and strategic decision making, or damage to a bank's reputation. Model risk occurs primarily for two reasons:

- The model may have fundamental errors and may produce inaccurate outputs when viewed against the design objective and intended business uses. The mathematical calculation and quantification exercise underlying any model generally involves application of theory, choice of sample design and numerical routines, selection of inputs and estimation, and implementation in information systems. Errors can occur at any point from design through implementation. In addition, shortcuts, simplifications, or approximations used to manage complicated problems could compromise the integrity and reliability of outputs

---

<sup>3</sup> While outside the scope of this guidance, more qualitative approaches used by banking organizations—i.e., those not defined as models according to this guidance—should also be subject to a rigorous control process.



from those calculations. Finally, the quality of model outputs depends on the quality of input data and assumptions, and errors in inputs or incorrect assumptions will lead to inaccurate outputs.

- The model may be used incorrectly or inappropriately. Even a fundamentally sound model producing accurate outputs consistent with the design objective of the model may exhibit high model risk if it is misapplied or misused. Models by their nature are simplifications of reality, and real-world events may prove those simplifications inappropriate. This is even more of a concern if a model is used outside the environment for which it was designed. Banks may do this intentionally as they apply existing models to new products or markets, or inadvertently as market conditions or customer behavior changes. Decision makers need to understand the limitations of a model to avoid using it in ways that are not consistent with the original intent. Limitations come in part from weaknesses in the model due to its various shortcomings, approximations, and uncertainties. Limitations are also a consequence of assumptions underlying a model that may restrict the scope to a limited set of specific circumstances and situations.

Model risk should be managed like other types of risk. Banks should identify the sources of risk and assess the magnitude. Model risk increases with greater model complexity, higher uncertainty about inputs and assumptions, broader use, and larger potential impact. Banks should consider risk from individual models and in the aggregate. Aggregate model risk is affected by interaction and dependencies among models; reliance on common assumptions, data, or methodologies; and any other factors that could adversely affect several models and their outputs at the same time. With an understanding of the source and magnitude of model risk in place, the next step is to manage it properly.

A guiding principle for managing model risk is "effective challenge" of models, that is, critical analysis by objective, informed parties who can identify model limitations and assumptions and produce appropriate changes. Effective challenge depends on a combination of incentives, competence, and influence. Incentives to provide effective challenge to models are stronger when there is greater separation of that challenge from the model development process and when challenge is supported by well-designed compensation practices and corporate culture. Competence is a key to effectiveness since technical knowledge and modeling skills are necessary to conduct appropriate analysis and critique. Finally, challenge may fail to be effective without the influence to ensure that actions are taken to address model issues. Such influence comes from a combination of explicit authority, stature within the organization, and commitment and support from higher levels of management.

Even with skilled modeling and robust validation, model risk cannot be eliminated, so other tools should be used to manage model risk effectively. Among these are establishing limits on model use, monitoring model performance, adjusting or revising models over time, and supplementing model results with other analysis and information. Informed conservatism, in either the inputs or the design of a model or through explicit

adjustments to outputs, can be an effective tool, though not an excuse to avoid improving models.

As is generally the case with other risks, materiality is an important consideration in model risk management. If at some banks the use of models is less pervasive and has less impact on their financial condition, then those banks may not need as complex an approach to model risk management in order to meet supervisory expectations. However, where models and model output have a material impact on business decisions, including decisions related to risk management and capital and liquidity planning, and where model failure would have a particularly harmful impact on a bank's financial condition, a bank's model risk management framework should be more extensive and rigorous.

Model risk management begins with robust model development, implementation, and use. Another essential element is a sound model validation process. A third element is governance, which sets an effective framework with defined roles and responsibilities for clear communication of model limitations and assumptions, as well as the authority to restrict model usage. The following sections of this document cover each of these elements.

#### **IV. MODEL DEVELOPMENT, IMPLEMENTATION, AND USE**

Model risk management should include disciplined and knowledgeable development and implementation processes that are consistent with the situation and goals of the model user and with bank policy. Model development is not a straightforward or routine technical process. The experience and judgment of developers, as much as their technical knowledge, greatly influence the appropriate selection of inputs and processing components. The training and experience of developers exercising such judgment affects the extent of model risk. Moreover, the modeling exercise is often a multidisciplinary activity drawing on economics, finance, statistics, mathematics, and other fields. Models are employed in real-world markets and events and therefore should be tailored for specific applications and informed by business uses. In addition, a considerable amount of subjective judgment is exercised at various stages of model development, implementation, use, and validation. It is important for decision makers to recognize that this subjectivity elevates the importance of sound and comprehensive model risk management processes.<sup>4</sup>

##### *Model Development and Implementation*

An effective development process begins with a clear statement of purpose to ensure that model development is aligned with the intended use. The design, theory, and logic

---

<sup>4</sup> Smaller banks that rely on vendor models may be able to satisfy the standards in this guidance without an in-house staff of technical, quantitative model developers. However, even if a bank relies on vendors for basic model development, the bank should still choose the particular models and variables that are appropriate to its size, scale, and lines of business and ensure the models are appropriate for the intended use.

underlying the model should be well documented and generally supported by published research and sound industry practice. The model methodologies and processing components that implement the theory, including the mathematical specification and the numerical techniques and approximations, should be explained in detail with particular attention to merits and limitations. Developers should ensure that the components work as intended, are appropriate for the intended business purpose, and are conceptually sound and mathematically and statistically correct. Comparison with alternative theories and approaches is a fundamental component of a sound modeling process.

The data and other information used to develop a model are of critical importance; there should be rigorous assessment of data quality and relevance, and appropriate documentation. Developers should be able to demonstrate that such data and information are suitable for the model and that they are consistent with the theory behind the approach and with the chosen methodology. If data proxies are used, they should be carefully identified, justified, and documented. If data and information are not representative of the bank's portfolio or other characteristics, or if assumptions are made to adjust the data and information, these factors should be properly tracked and analyzed so that users are aware of potential limitations. This is particularly important for external data and information (from a vendor or outside party), especially as they relate to new products, instruments, or activities.

An integral part of model development is testing, in which the various components of a model and its overall functioning are evaluated to determine whether the model is performing as intended. Model testing includes checking the model's accuracy, demonstrating that the model is robust and stable, assessing potential limitations, and evaluating the model's behavior over a range of input values. It should also assess the impact of assumptions and identify situations where the model performs poorly or becomes unreliable. Testing should be applied to actual circumstances under a variety of market conditions, including scenarios that are outside the range of ordinary expectations, and should encompass the variety of products or applications for which the model is intended. Extreme values for inputs should be evaluated to identify any boundaries of model effectiveness. The impact of model results on other models that rely on those results as inputs should also be evaluated. Included in testing activities should be the purpose, design, and execution of test plans, summary results with commentary and evaluation, and detailed analysis of informative samples. Testing activities should be appropriately documented.

The nature of testing and analysis will depend on the type of model and will be judged by different criteria depending on the context. For example, the appropriate statistical tests depend on specific distributional assumptions and the purpose of the model. Furthermore, in many cases statistical tests cannot unambiguously reject false hypotheses or accept true ones based on sample information. Different tests have different strengths and weaknesses under different conditions. Any single test is rarely sufficient, so banks should apply a variety of tests to develop a sound model.

Banks should ensure that the development of the more judgmental and qualitative aspects of their models is also sound. In some cases, banks may take statistical output from a model and modify it with judgmental or qualitative adjustments as part of model development. While such practices may be appropriate, banks should ensure that any such adjustments made as part of the development process are conducted in an appropriate and systematic manner, and are well documented.

Models typically are embedded in larger information systems that manage the flow of data from various sources into the model and handle the aggregation and reporting of model outcomes. Model calculations should be properly coordinated with the capabilities and requirements of information systems. Sound model risk management depends on substantial investment in supporting systems to ensure data and reporting integrity, together with controls and testing to ensure proper implementation of models, effective systems integration, and appropriate use.

### *Model Use*

Model use provides additional opportunity to test whether a model is functioning effectively and to assess its performance over time as conditions and model applications change. It can serve as a source of productive feedback and insights from a knowledgeable internal constituency with strong interest in having models that function well and reflect economic and business realities. Model users can provide valuable business insight during the development process. In addition, business managers affected by model outcomes may question the methods or assumptions underlying the models, particularly if the managers are significantly affected by and do not agree with the outcome. Such questioning can be healthy if it is constructive and causes model developers to explain and justify the assumptions and design of the models.

However, challenge from model users may be weak if the model does not materially affect their results, if the resulting changes in models are perceived to have adverse effects on the business line, or if change in general is regarded as expensive or difficult. User challenges also tend not to be comprehensive because they focus on aspects of models that have the most direct impact on the user's measured business performance or compensation, and thus may ignore other elements and applications of the models. Finally, such challenges tend to be asymmetric, because users are less likely to challenge an outcome that results in an advantage for them. Indeed, users may incorrectly believe that model risk is low simply because outcomes from model-based decisions appear favorable to the institution. Thus, the nature and motivation behind model users' input should be evaluated carefully, and banks should also solicit constructive suggestions and criticism from sources independent of the line of business using the model.

Reports used for business decision making play a critical role in model risk management. Such reports should be clear and comprehensible and take into account the fact that decision makers and modelers often come from quite different backgrounds and may interpret the contents in different ways. Reports that provide a range of estimates for different input-value scenarios and assumption values can give decision makers important

indications of the model's accuracy, robustness, and stability as well as information on model limitations.

An understanding of model uncertainty and inaccuracy and a demonstration that the bank is accounting for them appropriately are important outcomes of effective model development, implementation, and use. Because they are by definition imperfect representations of reality, all models have some degree of uncertainty and inaccuracy. These can sometimes be quantified, for example, by an assessment of the potential impact of factors that are unobservable or not fully incorporated in the model, or by the confidence interval around a statistical model's point estimate. Indeed, using a range of outputs, rather than a simple point estimate, can be a useful way to signal model uncertainty and avoid spurious precision. At other times, only a qualitative assessment of model uncertainty and inaccuracy is possible. In either case, it can be prudent for banks to account for model uncertainty by explicitly adjusting model inputs or calculations to produce more severe or adverse model output in the interest of conservatism. Accounting for model uncertainty can also include judgmental conservative adjustments to model output, placing less emphasis on that model's output, or ensuring that the model is only used when supplemented by other models or approaches.<sup>5</sup>

While conservative use of models is prudent in general, banks should be careful in applying conservatism broadly or claiming to make conservative adjustments or add-ons to address model risk, because the impact of such conservatism in complex models may not be obvious or intuitive. Model aspects that appear conservative in one model may not be truly conservative compared with alternative methods. For example, simply picking an extreme point on a given modeled distribution may not be conservative if the distribution was misestimated or misspecified in the first place. Furthermore, initially conservative assumptions may not remain conservative over time. Therefore, banks should justify and substantiate claims that model outputs are conservative with a definition and measurement of that conservatism that is communicated to model users. In some cases, sensitivity analysis or other types of stress testing can be used to demonstrate that a model is indeed conservative. Another way in which banks may choose to be conservative is to hold an additional cushion of capital to protect against potential losses associated with model risk. However, conservatism can become an impediment to proper model development and application if it is seen as a solution that dissuades the bank from making the effort to improve the model; in addition, excessive conservatism can lead model users to discount the model outputs.

As this section has explained, robust model development, implementation, and use is important to model risk management. But it is not enough for model developers and users to understand and accept the model. Because model risk is ultimately borne by the bank as a whole, the bank should objectively assess model risk and the associated costs and benefits using a sound model-validation process.

---

<sup>5</sup> To the extent that models are used to generate amounts included in public financial statements, any adjustments for model uncertainty must comply with generally accepted accounting principles.



## V. MODEL VALIDATION

Model validation is the set of processes and activities intended to verify that models are performing as expected, in line with their design objectives and business uses. Effective validation helps ensure that models are sound. It also identifies potential limitations and assumptions, and assesses their possible impact. As with other aspects of effective challenge, model validation should be performed by staff with appropriate incentives, competence, and influence.

All model components, including input, processing, and reporting, should be subject to validation; this applies equally to models developed in-house and to those purchased from or developed by vendors or consultants. The rigor and sophistication of validation should be commensurate with the bank's overall use of models, the complexity and materiality of its models, and the size and complexity of the bank's operations.

Validation involves a degree of independence from model development and use. Generally, validation should be done by people who are not responsible for development or use and do not have a stake in whether a model is determined to be valid. Independence is not an end in itself but rather helps ensure that incentives are aligned with the goals of model validation. While independence may be supported by separation of reporting lines, it should be judged by actions and outcomes, since there may be additional ways to ensure objectivity and prevent bias. As a practical matter, some validation work may be most effectively done by model developers and users; it is essential, however, that such validation work be subject to critical review by an independent party, who should conduct additional activities to ensure proper validation. Overall, the quality of the process is judged by the manner in which models are subject to critical review. This could be determined by evaluating the extent and clarity of documentation, the issues identified by objective parties, and the actions taken by management to address model issues.

In addition to independence, banks can support appropriate incentives in validation through compensation practices and performance evaluation standards that are tied directly to the quality of model validations and the degree of critical, unbiased review. In addition, corporate culture plays a role if it establishes support for objective thinking and encourages questioning and challenging of decisions.

Staff doing validation should have the requisite knowledge, skills, and expertise. A high level of technical expertise may be needed because of the complexity of many models, both in structure and in application. These staff also should have a significant degree of familiarity with the line of business using the model and the model's intended use. A model's developer is an important source of information but cannot be relied on as an objective or sole source on which to base an assessment of model quality.

Staff conducting validation work should have explicit authority to challenge developers and users and to elevate their findings, including issues and deficiencies. The individual or unit to whom those staff report should have sufficient influence or stature within the

bank to ensure that any issues and deficiencies are appropriately addressed in a timely and substantive manner. Such influence can be reflected in reporting lines, title, rank, or designated responsibilities. Influence may be demonstrated by a pattern of actual instances in which models, or the use of models, have been appropriately changed as a result of validation.

The range and rigor of validation activities conducted prior to first use of a model should be in line with the potential risk presented by use of the model. If significant deficiencies are noted as a result of the validation process, use of the model should not be allowed or should be permitted only under very tight constraints until those issues are resolved. If the deficiencies are too severe to be addressed within the model's framework, the model should be rejected. If it is not feasible to conduct necessary validation activities prior to model use because of data paucity or other limitations, that fact should be documented and communicated in reports to users, senior management, and other relevant parties. In such cases, the uncertainty about the results that the model produces should be mitigated by other compensating controls. This is particularly applicable to new models and to the use of existing models in new applications.

Validation activities should continue on an ongoing basis after a model goes into use, to track known model limitations and to identify any new ones. Validation is an important check on model use during periods of benign economic and financial conditions, when estimates of risk and potential loss can become overly optimistic, and when the data at hand may not fully reflect more stressed conditions. Ongoing validation activities help to ensure that changes in markets, products, exposures, activities, clients, or business practices do not create new model limitations. For example, if credit risk models do not incorporate underwriting changes in a timely manner, flawed and costly business decisions could be made before deterioration in model performance becomes apparent.

Banks should conduct a periodic review—at least annually but more frequently if warranted—of each model to determine whether it is working as intended and if the existing validation activities are sufficient. Such a determination could simply affirm previous validation work, suggest updates to previous validation activities, or call for additional validation activities. Material changes to models should also be subject to validation. It is generally good practice for banks to ensure that all models undergo the full validation process, as described in the following section, at some fixed interval, including updated documentation of all activities.

Effective model validation helps reduce model risk by identifying model errors, corrective actions, and appropriate use. It also provides an assessment of the reliability of a given model, based on its underlying assumptions, theory, and methods. In this way, it provides information about the source and extent of model risk. Validation also can reveal deterioration in model performance over time and can set thresholds for acceptable levels of error, through analysis of the distribution of outcomes around expected or predicted values. If outcomes fall consistently outside this acceptable range, then the models should be redeveloped.

### *Key Elements of Comprehensive Validation*

An effective validation framework should include three core elements:

- Evaluation of conceptual soundness, including developmental evidence
- Ongoing monitoring, including process verification and benchmarking
- Outcomes analysis, including back-testing

#### 1. Evaluation of Conceptual Soundness

This element involves assessing the quality of the model design and construction. It entails review of documentation and empirical evidence supporting the methods used and variables selected for the model. Documentation and testing should convey an understanding of model limitations and assumptions. Validation should ensure that judgment exercised in model design and construction is well informed, carefully considered, and consistent with published research and with sound industry practice. Developmental evidence should be reviewed before a model goes into use and also as part of the ongoing validation process, in particular whenever there is a material change in the model.

A sound development process will produce documented evidence in support of all model choices, including the overall theoretical construction, key assumptions, data, and specific mathematical calculations, as mentioned in Section IV. As part of model validation, those model aspects should be subjected to critical analysis by both evaluating the quality and extent of developmental evidence and conducting additional analysis and testing as necessary. Comparison to alternative theories and approaches should be included. Key assumptions and the choice of variables should be assessed, with analysis of their impact on model outputs and particular focus on any potential limitations. The relevance of the data used to build the model should be evaluated to ensure that it is reasonably representative of the bank's portfolio or market conditions, depending on the type of model. This is an especially important exercise when a bank uses external data or the model is used for new products or activities.

Where appropriate to the particular model, banks should employ sensitivity analysis in model development and validation to check the impact of small changes in inputs and parameter values on model outputs to make sure they fall within an expected range. Unexpectedly large changes in outputs in response to small changes in inputs can indicate an unstable model. Varying several inputs simultaneously as part of sensitivity analysis can provide evidence of unexpected interactions, particularly if the interactions are complex and not intuitively clear. Banks benefit from conducting model stress testing to check performance over a wide range of inputs and parameter values, including extreme values, to verify that the model is robust. Such testing helps establish the boundaries of model performance by identifying the acceptable range of inputs as well as conditions under which the model may become unstable or inaccurate.

Management should have a clear plan for using the results of sensitivity analysis and other quantitative testing. If testing indicates that the model may be inaccurate or unstable in some circumstances, management should consider modifying certain model properties,

putting less reliance on its outputs, placing limits on model use, or developing a new approach.

Qualitative information and judgment used in model development should be evaluated, including the logic, judgment, and types of information used, to establish the conceptual soundness of the model and set appropriate conditions for its use. The validation process should ensure that qualitative, judgmental assessments are conducted in an appropriate and systematic manner, are well supported, and are documented.

## 2. Ongoing Monitoring

The second core element of the validation process is ongoing monitoring. Such monitoring confirms that the model is appropriately implemented and is being used and is performing as intended.

Ongoing monitoring is essential to evaluate whether changes in products, exposures, activities, clients, or market conditions necessitate adjustment, redevelopment, or replacement of the model and to verify that any extension of the model beyond its original scope is valid. Any model limitations identified in the development stage should be regularly assessed over time, as part of ongoing monitoring. Monitoring begins when a model is first implemented in production systems for actual business use. This monitoring should continue periodically over time, with a frequency appropriate to the nature of the model, the availability of new data or modeling approaches, and the magnitude of the risk involved. Banks should design a program of ongoing testing and evaluation of model performance along with procedures for responding to any problems that appear. This program should include process verification and benchmarking.

Process verification checks that all model components are functioning as designed. It includes verifying that internal and external data inputs continue to be accurate, complete, consistent with model purpose and design, and of the highest quality available. Computer code implementing the model should be subject to rigorous quality and change control procedures to ensure that the code is correct, that it cannot be altered except by approved parties, and that all changes are logged and can be audited. System integration can be a challenge and deserves special attention because the model processing component often draws from various sources of data, processes large amounts of data, and then feeds into multiple data repositories and reporting systems. User-developed applications, such as spreadsheets or ad hoc database applications used to generate quantitative estimates, are particularly prone to model risk. As the content or composition of information changes over time, systems may need to be updated to reflect any changes in the data or its use. Reports derived from model outputs should be reviewed as part of validation to verify that they are accurate, complete, and informative, and that they contain appropriate indicators of model performance and limitations.

Many of the tests employed as part of model development should be included in ongoing monitoring and be conducted on a regular basis to incorporate additional information as it becomes available. New empirical evidence or theoretical research may suggest the need to modify or even replace original methods. Analysis of the integrity and applicability of

internal and external information sources, including information provided by third-party vendors, should be performed regularly.

Sensitivity analysis and other checks for robustness and stability should likewise be repeated periodically. They can be as useful during ongoing monitoring as they are during model development. If models only work well for certain ranges of input values, market conditions, or other factors, they should be monitored to identify situations where these constraints are approached or exceeded.

Ongoing monitoring should include the analysis of overrides with appropriate documentation. In the use of virtually any model, there will be cases where model output is ignored, altered, or reversed based on the expert judgment of model users. Such overrides are an indication that, in some respect, the model is not performing as intended or has limitations. Banks should evaluate the reasons for overrides and track and analyze override performance. If the rate of overrides is high, or if the override process consistently improves model performance, it is often a sign that the underlying model needs revision or redevelopment.

Benchmarking is the comparison of a given model's inputs and outputs to estimates from alternative internal or external data or models. It can be incorporated in model development as well as in ongoing monitoring. For credit risk models, examples of benchmarks include models from vendor firms or industry consortia and data from retail credit bureaus. Pricing models for securities and derivatives often can be compared with alternative models that are more accurate or comprehensive but also too time consuming to run on a daily basis. Whatever the source, benchmark models should be rigorous and benchmark data should be accurate and complete to ensure a reasonable comparison.

Discrepancies between the model output and benchmarks should trigger investigation into the sources and degree of the differences, and examination of whether they are within an expected or appropriate range given the nature of the comparison. The results of that analysis may suggest revisions to the model. However, differences do not necessarily indicate that the model is in error. The benchmark itself is an alternative prediction, and the differences may be due to the different data or methods used. If the model and the benchmark match well, that is evidence in favor of the model, but it should be interpreted with caution so the bank does not get a false degree of comfort.

### 3. Outcomes Analysis

The third core element of the validation process is outcomes analysis, a comparison of model outputs to corresponding actual outcomes. The precise nature of the comparison depends on the objectives of a model, and might include an assessment of the accuracy of estimates or forecasts, an evaluation of rank-ordering ability, or other appropriate tests. In all cases, such comparisons help to evaluate model performance, by establishing expected ranges for those actual outcomes in relation to the intended objectives and assessing the reasons for observed variation between the two. If outcomes analysis produces evidence of poor performance, the bank should take action to address those issues. Outcomes analysis typically relies on statistical tests or other quantitative measures. It can also



include expert judgment to check the intuition behind the outcomes and confirm that the results make sense. When a model itself relies on expert judgment, quantitative outcomes analysis helps to evaluate the quality of that judgment. Outcomes analysis should be conducted on an ongoing basis to test whether the model continues to perform in line with design objectives and business uses.

A variety of quantitative and qualitative testing and analytical techniques can be used in outcomes analysis. The choice of technique should be based on the model's methodology, its complexity, data availability, and the magnitude of potential model risk to the bank. Outcomes analysis should involve a range of tests because any individual test will have weaknesses. For example, some tests are better at checking a model's ability to rank-order or segment observations on a relative basis, whereas others are better at checking absolute forecast accuracy. Tests should be designed for each situation, as not all will be effective or feasible in every circumstance, and attention should be paid to choosing the appropriate type of outcomes analysis for a particular model.

Models are regularly adjusted to take into account new data or techniques, or because of deterioration in performance. Parallel outcomes analysis, under which both the original and adjusted models' forecasts are tested against realized outcomes, provides an important test of such model adjustments. If the adjusted model does not outperform the original model, developers, users, and reviewers should realize that additional changes—or even a wholesale redesign—are likely necessary before the adjusted model replaces the original one.

Back-testing is one form of outcomes analysis; specifically, it involves the comparison of actual outcomes with model forecasts during a sample time period not used in model development and at an observation frequency that matches the forecast horizon or performance window of the model. The comparison is generally done using expected ranges or statistical confidence intervals around the model forecasts. When outcomes fall outside those intervals, the bank should analyze the discrepancies and investigate the causes that are significant in terms of magnitude or frequency. The objective of the analysis is to determine whether differences stem from the omission of material factors from the model, whether they arise from errors with regard to other aspects of model specification such as interaction terms or assumptions of linearity, or whether they are purely random and thus consistent with acceptable model performance. Analysis of in-sample fit and of model performance in holdout samples (data set aside and not used to estimate the original model) are important parts of model development but are not substitutes for back-testing.

A well-known example of back-testing is the evaluation of value-at-risk (VaR), in which actual profit and loss is compared with a model forecast loss distribution. Significant deviation in expected versus actual performance and unexplained volatility in the profits and losses of trading activities may indicate that hedging and pricing relationships are not adequately measured by a given approach. Along with measuring the frequency of losses in excess of a single VaR percentile estimator, banks should use other tests, such as

assessing any clustering of exceptions and checking the distribution of losses against other estimated percentiles.

Analysis of the results of even high-quality and well-designed back-testing can pose challenges, since it is not a straightforward, mechanical process that always produces unambiguous results. The purpose is to test the model, not individual forecast values. Back-testing may entail analysis of a large number of forecasts over different conditions at a point in time or over multiple time periods. Statistical testing is essential in such cases, yet such testing can pose challenges in both the choice of appropriate tests and the interpretation of results; banks should support and document both the choice of tests and the interpretation of results.

Models with long forecast horizons should be back-tested, but given the amount of time it would take to accumulate the necessary data, that testing should be supplemented by evaluation over shorter periods. Banks should employ outcomes analysis consisting of “early warning” metrics designed to measure performance beginning very shortly after model introduction and trend analysis of performance over time. These outcomes analysis tools are not substitutes for back-testing, which should still be performed over the longer time period, but rather very important complements.

Outcomes analysis and the other elements of the validation process may reveal significant errors or inaccuracies in model development or outcomes that consistently fall outside the bank’s predetermined thresholds of acceptability. In such cases, model adjustment, recalibration, or redevelopment is warranted. Adjustments and recalibration should be governed by the principle of conservatism and should undergo independent review.

Material changes in model structure or technique, and all model redevelopment, should be subject to validation activities of appropriate range and rigor before implementation. At times banks may have a limited ability to use key model validation tools like back-testing or sensitivity analysis for various reasons, such as lack of data or of price observability. In those cases, even more attention should be paid to the model’s limitations when considering the appropriateness of model usage, and senior management should be fully informed of those limitations when using the models for decision making. Such scrutiny should be applied to individual models and models in the aggregate.

#### *Validation of Vendor and Other Third-Party Products*

The widespread use of vendor and other third-party products—including data, parameter values, and complete models—poses unique challenges for validation and other model risk management activities because the modeling expertise is external to the user and because some components are considered proprietary. Vendor products should nevertheless be incorporated into a bank’s broader model risk management framework following the same principles as applied to in-house models, although the process may be somewhat modified.

As a first step, banks should ensure that there are appropriate processes in place for selecting vendor models. Banks should require the vendor to provide developmental evidence explaining the product components, design, and intended use, to determine whether the model is appropriate for the bank's products, exposures, and risks. Vendors should provide appropriate testing results that show their product works as expected. They should also clearly indicate the model's limitations and assumptions and where the product's use may be problematic. Banks should expect vendors to conduct ongoing performance monitoring and outcomes analysis, with disclosure to their clients, and to make appropriate modifications and updates over time.

Banks are expected to validate their own use of vendor products. External models may not allow full access to computer coding and implementation details, so the bank may have to rely more on sensitivity analysis and benchmarking. Vendor models are often designed to provide a range of capabilities and so may need to be customized by a bank for its particular circumstances. A bank's customization choices should be documented and justified as part of validation. If vendors provide input data or assumptions, or use them to build models, their relevance for the bank's situation should be investigated. Banks should obtain information regarding the data used to develop the model and assess the extent to which that data is representative of the bank's situation. The bank also should conduct ongoing monitoring and outcomes analysis of vendor model performance using the bank's own outcomes.

Systematic procedures for validation help the bank to understand the vendor product and its capabilities, applicability, and limitations. Such detailed knowledge is necessary for basic controls of bank operations. It is also very important for the bank to have as much knowledge in-house as possible, in case the vendor or the bank terminates the contract for any reason, or if the vendor is no longer in business. Banks should have contingency plans for instances when the vendor model is no longer available or cannot be supported by the vendor.

## **VI. GOVERNANCE, POLICIES, AND CONTROLS**

Developing and maintaining strong governance, policies, and controls over the model risk management framework is fundamentally important to its effectiveness. Even if model development, implementation, use, and validation are satisfactory, a weak governance function will reduce the effectiveness of overall model risk management. A strong governance framework provides explicit support and structure to risk management functions through policies defining relevant risk management activities, procedures that implement those policies, allocation of resources, and mechanisms for evaluating whether policies and procedures are being carried out as specified. Notably, the extent and sophistication of a bank's governance function is expected to align with the extent and sophistication of model usage.

### *Board of Directors and Senior Management*

Model risk governance is provided at the highest level by the board of directors and senior management when they establish a bank-wide approach to model risk management. As part of their overall responsibilities, a bank's board and senior management should establish a strong model risk management framework that fits into the broader risk management of the organization. That framework should be grounded in an understanding of model risk—not just for individual models but also in the aggregate. The framework should include standards for model development, implementation, use, and validation.

While the board is ultimately responsible, it generally delegates to senior management the responsibility for executing and maintaining an effective model risk management framework. Duties of senior management include establishing adequate policies and procedures and ensuring compliance, assigning competent staff, overseeing model development and implementation, evaluating model results, ensuring effective challenge, reviewing validation and internal audit findings, and taking prompt remedial action when necessary. In the same manner as for other major areas of risk, senior management, directly and through relevant committees, is responsible for regularly reporting to the board on significant model risk, from individual models and in the aggregate, and on compliance with policy. Board members should ensure that the level of model risk is within their tolerance and direct changes where appropriate. These actions will set the tone for the whole organization about the importance of model risk and the need for active model risk management.

### *Policies and Procedures*

Consistent with good business practices and existing supervisory expectations, banks should formalize model risk management activities with policies and the procedures to implement them. Model risk management policies should be consistent with this guidance and also be commensurate with the bank's relative complexity, business activities, corporate culture, and overall organizational structure. The board or its delegates should approve model risk management policies and review them annually to ensure consistent and rigorous practices across the organization. Those policies should be updated as necessary to ensure that model risk management practices remain appropriate and keep current with changes in market conditions, bank products and strategies, bank exposures and activities, and practices in the industry. All aspects of model risk management should be covered by suitable policies, including model and model risk definitions; assessment of model risk; acceptable practices for model development, implementation, and use; appropriate model validation activities; and governance and controls over the model risk management process.

Policies should emphasize testing and analysis, and promote the development of targets for model accuracy, standards for acceptable levels of discrepancies, and procedures for review of and response to unacceptable discrepancies. They should include a description

of the processes used to select and retain vendor models, including the people who should be involved in such decisions.

The prioritization, scope, and frequency of validation activities should be addressed in these policies. They should establish standards for the extent of validation that should be performed before models are put into production and the scope of ongoing validation. The policies should also detail the requirements for validation of vendor models and third-party products. Finally, they should require maintenance of detailed documentation of all aspects of the model risk management framework, including an inventory of models in use, results of the modeling and validation processes, and model issues and their resolution.

Policies should identify the roles and assign responsibilities within the model risk management framework with clear detail on staff expertise, authority, reporting lines, and continuity. They should also outline controls on the use of external resources for validation and compliance and specify how that work will be integrated into the model risk management framework.

### *Roles and Responsibilities*

Conceptually, the roles in model risk management can be divided among ownership, controls, and compliance. While there are several ways in which banks can assign the responsibilities associated with these roles, it is important that reporting lines and incentives be clear, with potential conflicts of interest identified and addressed.

Business units are generally responsible for the model risk associated with their business strategies. The role of model owner involves ultimate accountability for model use and performance within the framework set by bank policies and procedures. Model owners should be responsible for ensuring that models are properly developed, implemented, and used. The model owner should also ensure that models in use have undergone appropriate validation and approval processes, promptly identify new or changed models, and provide all necessary information for validation activities.

Model risk taken by business units should be controlled. The responsibilities for risk controls may be assigned to individuals, committees, or a combination of the two, and include risk measurement, limits, and monitoring. Other responsibilities include managing the independent validation and review process to ensure that effective challenge takes place. Appropriate resources should be assigned for model validation and for guiding the scope and prioritization of work. Issues and problems identified through validation and other forms of oversight should be communicated by risk-control staff to relevant individuals and business users throughout the organization, including senior management, with a plan for corrective action. Control staff should have the authority to restrict the use of models and monitor any limits on model usage. While they may grant exceptions to typical procedures of model validation on a temporary basis, that authority should be subject to other control mechanisms, such as timelines for completing validation work and limits on model use.

Compliance with policies is an obligation of model owners and risk-control staff, and there should be specific processes in place to ensure that these roles are being carried out effectively and in line with policy. Documentation and tracking of activities surrounding model development, implementation, use, and validation are needed to provide a record that makes compliance with policy transparent.

### *Internal Audit*

A bank's internal audit function should assess the overall effectiveness of the model risk management framework, including the framework's ability to address both types of model risk described in Section III, for individual models and in the aggregate. Findings from internal audit related to models should be documented and reported to the board or its appropriately delegated agent. Banks should ensure that internal audit operates with the proper incentives, has appropriate skills, and has adequate stature in the organization to assist in model risk management. Internal audit's role is not to duplicate model risk management activities. Instead, its role is to evaluate whether model risk management is comprehensive, rigorous, and effective. To accomplish this evaluation, internal audit staff should possess sufficient expertise in relevant modeling concepts as well as their use in particular business lines. If some internal audit staff perform certain validation activities, then they should not be involved in the assessment of the overall model risk management framework.

Internal audit should verify that acceptable policies are in place and that model owners and control groups comply with those policies. Internal audit should also verify records of model use and validation to test whether validations are performed in a timely manner and whether models are subject to controls that appropriately account for any weaknesses in validation activities. Accuracy and completeness of the model inventory should be assessed. In addition, processes for establishing and monitoring limits on model usage should be evaluated. Internal audit should determine whether procedures for updating models are clearly documented, and test whether those procedures are being carried out as specified. Internal audit should check that model owners and control groups are meeting documentation standards, including risk reporting. Additionally, internal audit should perform assessments of supporting operational systems and evaluate the reliability of data used by models.

Internal audit also has an important role in ensuring that validation work is conducted properly and that appropriate effective challenge is being carried out. It should evaluate the objectivity, competence, and organizational standing of the key validation participants, with the ultimate goal of ascertaining whether those participants have the right incentives to discover and report deficiencies. Internal audit should review validation activities conducted by internal and external parties with the same rigor to see if those activities are being conducted in accordance with this guidance.

### *External Resources*

Although model risk management is an internal process, a bank may decide to engage external resources to help execute certain activities related to the model risk management framework. These activities could include model validation and review, compliance functions, or other activities in support of internal audit. These resources may provide added knowledge and another level of critical and effective challenge, which may improve the internal model development and risk management processes. However, this potential benefit should be weighed against the added costs for such resources and the added time that external parties require to understand internal data, systems, and other relevant bank-specific circumstances.

Whenever external resources are used, the bank should specify the activities to be conducted in a clearly written and agreed-upon scope of work. A designated internal party from the bank should be able to understand and evaluate the results of validation and risk-control activities conducted by external resources. The internal party is responsible for: verifying that the agreed upon scope of work has been completed; evaluating and tracking identified issues and ensuring they are addressed; and making sure that completed work is incorporated into the bank's overall model risk management framework. If the external resources are only utilized to do a portion of validation or compliance work, the bank should coordinate internal resources to complete the full range of work needed. The bank should have a contingency plan in case an external resource is no longer available or is unsatisfactory.

### *Model Inventory*

Banks should maintain a comprehensive set of information for models implemented for use, under development for implementation, or recently retired. While each line of business may maintain its own inventory, a specific party should also be charged with maintaining a firm-wide inventory of all models, which should assist a bank in evaluating its model risk in the aggregate. Any variation of a model that warrants a separate validation should be included as a separate model and cross-referenced with other variations.

While the inventory may contain varying levels of information, given different model complexity and the bank's overall level of model usage, the following are some general guidelines. The inventory should describe the purpose and products for which the model is designed, actual or expected usage, and any restrictions on use. It is useful for the inventory to list the type and source of inputs used by a given model and underlying components (which may include other models), as well as model outputs and their intended use. It should also indicate whether models are functioning properly, provide a description of when they were last updated, and list any exceptions to policy. Other items include the names of individuals responsible for various aspects of the model development and validation; the dates of completed and planned validation activities; and the time frame during which the model is expected to remain valid.

### *Documentation*

Without adequate documentation, model risk assessment and management will be ineffective. Documentation of model development and validation should be sufficiently detailed so that parties unfamiliar with a model can understand how the model operates, its limitations, and its key assumptions. Documentation provides for continuity of operations, makes compliance with policy transparent, and helps track recommendations, responses, and exceptions. Developers, users, control and compliance units, and supervisors are all served by effective documentation. Banks can benefit from advances in information and knowledge management systems and electronic documentation to improve the organization, timeliness, and accessibility of the various records and reports produced in the model risk management process.

Documentation takes time and effort, and model developers and users who know the models well may not appreciate its value. Banks should therefore provide incentives to produce effective and complete model documentation. Model developers should have responsibility during model development for thorough documentation, which should be kept up-to-date as the model and application environment changes. In addition, the bank should ensure that other participants in model risk management activities document their work, including ongoing monitoring, process verification, benchmarking, and outcomes analysis. Also, line of business or other decision makers should document information leading to selection of a given model and its subsequent validation. For cases in which a bank uses models from a vendor or other third party, it should ensure that appropriate documentation of the third-party approach is available so that the model can be appropriately validated.

Validation reports should articulate model aspects that were reviewed, highlighting potential deficiencies over a range of financial and economic conditions, and determining whether adjustments or other compensating controls are warranted. Effective validation reports include clear executive summaries, with a statement of model purpose and an accessible synopsis of model and validation results, including major limitations and key assumptions.

## **VII. CONCLUSION**

This document has provided comprehensive guidance on effective model risk management. Many of the activities described in this document are common industry practice. But all banks should confirm that their practices conform to the principles in this guidance for model development, implementation, and use, as well as model validation. Banks should also ensure that they maintain strong governance and controls to help manage model risk, including internal policies and procedures that appropriately reflect the risk management principles described in this guidance. Details of model risk management practices may vary from bank to bank, as practical application of this guidance should be commensurate with a bank's risk exposures, its business activities, and the extent and complexity of its model use.



Tab 3

## Investor Alerts and Bulletins

---

# Investor Alert: Automated Investment Tools

**May 8, 2015**

*The SEC's Office of Investor Education and Advocacy (OIEA) and the Financial Industry Regulatory Authority, Inc. (FINRA) are issuing this alert to provide investors with a general overview of automated investment tools.*

At the swipe of a fingertip on a mobile device or the click of a mouse on a desktop computer, investors can access a broad range of automated investment tools. These tools range from personal financial planning tools (such as online calculators) to portfolio selection or asset optimization services (such as services that provide recommendations on how to allocate your 401(k) or brokerage account) to online investment management programs (such as robo-advisors that select and manage investment portfolios).

Many financial professionals have used automated investment tools for decades to help customers build and manage their investment portfolios, and a growing number of these tools are now available directly to investors from a variety of sources. While automated investment tools may offer clear benefits—including low cost, ease of use, and broad access—it is important to understand their risks and limitations before using them. Investors should be wary of tools that promise better portfolio performance.

### **Automated Investment Tool Tips**

Consider the following five tips before using any automated investment tool:

#### **1. Understand any terms and conditions.**

Review all relevant disclosures for an automated investment tool. Understand any terms and conditions, such as the fees and expenses associated with using the tool or with selling or purchasing investments. Find out how you can terminate any agreement or relationship, and how long it may take to cash out any investments if you decide to stop using the tool. If anything is unclear or you need additional information, directly contact the automated tool sponsor.

Ask an automated investment tool sponsor whether it receives any form of compensation for offering, recommending, or selling certain services or investments.

#### **2. Consider the tool's limitations, including any key assumptions.**

One type of automated tool called an investment analysis tool provided by [registered securities firms and individuals](#) must describe the criteria and methodology used, including the tool's limitations and key assumptions.

Be aware that an automated tool may rely on assumptions that could be incorrect or do not apply to your individual situation. For example, an automated investment tool may be programmed to use economic assumptions that will not react to shifts in the market. If the automated tool assumes that interest rates will remain low but, instead, interest rates rise, the tool's output will be flawed.

In addition, an automated investment tool, like other investment programs, may be programmed to consider limited options. For example, an automated investment tool may only consider investments offered by an affiliated firm.

#### **3. Recognize that the automated tool's output directly depends on what information it seeks from you and what information you provide.**

Which questions the tool asks and how they are framed may limit or influence the information you provide, which in turn directly impacts the output that an automated investment tool generates. If any of the questions are unclear or you do not understand why the information is being sought, ask the tool sponsor. Be aware that a tool may ask questions that are over-generalized, ambiguous, misleading, or designed to fit you into the tool's predetermined options.

In addition, be very careful when inputting your answers or information. If you make a mistake, the resulting output may not be right for you.

#### **4. Be aware that an automated tool's output may not be right for your financial needs or goals.**

An automated investment tool may not assess all of your particular circumstances, such as your age, financial situation and needs, investment experience, other holdings, tax situation, willingness to risk losing your investment money for potentially higher investment returns, time horizon for investing, need for cash, and investment goals. Consequently, some tools may suggest investments (including asset-allocation models) that may not be right for you.

For example, an automated investment tool may estimate a time horizon for your investments based only on your age, but not take into account that you need some of your investment money back in a few years to buy a new home. In addition, automated tools typically do not take into account that your financial goals may change.

If the automated investment tool does not allow you to interact with an actual person, consider that you may lose the value that human judgment and oversight, or more personalized service, may add to the process.

#### **5. Safeguard your personal information.**

Be aware that an automated tool sponsor may be collecting your personal information for purposes unrelated to the tool. Understand when and with whom your personal information may be shared. If you have questions that are not answered in the tool's privacy policy, contact the tool's sponsor for more information.

Also, look out for phishing and other scams designed to trick you into revealing personal financial information. Unless you are accessing an account that you established, do not provide bank or brokerage account numbers, passwords, PINs, credit card information, Social Security numbers, or other personally identifiable information.

When using investment tools online, take these steps to protect your personal financial information:

- Do not provide payment information if the address bar of the website indicates that the web address begins with "http" (instead of "https").
- Pick a "strong" password, keep it secure, and change it regularly.
- Password-protect mobile devices that are linked to investment tools or accounts.
- Avoid accessing investment tools or accounts on a shared computer or through an unsecure wireless connection.

For more online security tips, read [Investor Bulletin: Protecting Your Online Brokerage Accounts from Fraud](#) and ["Phishing" and Other Online Identity Theft Scams: Don't Take the Bait](#).

While automated investment tools are programmed to generate outputs based on preset options, it is up to you to decide whether and when to rely on these tools in making your investment decisions.

#### **For More Information**

Check the SEC's [Investment Adviser Public Disclosure \(IAPD\)](#) database or FINRA's [BrokerCheck](#) to research the background, including registration or license status and disciplinary history, of any individual or firm offering, recommending, or selling an investment.

Receive the latest Investor Alerts and Bulletins from OIEA by [email](#) or [RSS feed](#). Visit [Investor.gov](#), the SEC's website for individual investors. Like OIEA on [Facebook](#) at [www.facebook.com/secinvestoreducation](http://www.facebook.com/secinvestoreducation). Follow

OIEA on [Twitter](#) @SEC\_Investor\_Ed.

[Ask a question](#) or call the SEC at (800) 732-0330 (or 1-202-551-6551 from outside of the U.S.).

The Office of Investor Education and Advocacy has provided this information as a service to investors. It is neither a legal interpretation nor a statement of SEC policy. If you have questions concerning the meaning or application of a particular law or rule, please consult with an attorney who specializes in securities law.

*Modified: May 8, 2015*

Tab 4

# Report on Digital Investment Advice

MARCH 2016

## Contents

Introduction	1
A Note on Terminology	2
A Brief History of Digital Investment Advice	2
Governance and Supervision	3
Investor Profiling	8
Rebalancing	11
Training	12
Lessons for Investors	13
Conclusion	14
Appendix	14
Endnotes	17

## A REPORT FROM THE FINANCIAL INDUSTRY REGULATORY AUTHORITY

### Introduction

Technology has long played a central role in financial services innovation. It continues to do so today as many firms in the securities industry introduce new digital investment advice tools to assist in developing and managing investment portfolios. FINRA undertook a review of selected digital investment advice tools to assess these developments.

The observations and practices in this report are drawn from FINRA's discussions with a range of financial services firms that provide or use digital investment advice tools, vendors and foreign securities regulators as well our regulatory experience. This report uses the term "financial services firms" to include both broker-dealers and investment advisers. The rules discussed in this report apply to broker-dealers. The effective practices we discuss are specifically intended for FINRA-registered firms, but may be valuable to financial professionals generally.<sup>1</sup>

The adoption of digital investment advice tools has stimulated discussions about the role of financial professionals and the evolving relationship between financial intermediaries and their clients. What role will financial professionals play in conjunction with digital services in providing investment advice? To what degree will investors rely primarily on digital investment advice? How well can software know a client? Can the skill, knowledge and service provided by well-trained and ethical financial professionals be incorporated in software? Can that software provide sound personal advice, especially for clients with more complex advice needs?

Without venturing to answer these questions, what is clear is that the role technology plays in supporting investment advice to clients will increase at many securities firms.<sup>2</sup> With that in mind, FINRA issues this report to remind broker-dealers of their obligations under FINRA rules as well as to share effective practices related to digital investment advice, including with respect to technology management, portfolio development and conflicts of interest mitigation. The report also raises considerations for investors in evaluating investment advice derived entirely or in part from digital investment advice tools.

This report does not create any new legal requirements or change any existing broker-dealer regulatory obligations. Throughout the report, we identify practices that we believe firms should consider and tailor to their business model.

## Questions/Further Information

Inquiries regarding this report may be directed to Daniel M. Sibears, Executive Vice President, Regulatory Operations/Shared Services, at (202) 728 6911; or Steven Polansky, Senior Director, Regulatory Operations/Shared Services, at (202) 728 8331.

## A Note on Terminology

As used here, digital investment advice tools (also referred to as digital advice tools) support one or more of the following core activities in managing an investor's portfolio: customer profiling, asset allocation, portfolio selection, trade execution, portfolio rebalancing, tax-loss harvesting<sup>3</sup> and portfolio analysis. These investment advice tools can be broken down into two groups: tools that financial professionals use, referred to here as “financial professional-facing” tools, and tools that clients use, referred to here as “client-facing” tools. Client-facing tools that incorporate the first six activities—customer profiling through tax-loss harvesting—are frequently referred to as “robo advisors” or “robos.”<sup>4</sup>

**Figure 1: Investment advice value chain**



\* Functionally typical in financial professional- and client-facing digital investment advice tools

\*\* Functionally typical in financial professional-facing tools only

## A Brief History of Digital Investment Advice

Financial professionals have used digital investment advice tools for years. These tools help financial professionals at each point in the value chain described above, for example, to develop an investor profile, to prepare proposals and sales materials, to develop an asset allocation or to recommend specific securities to an investor. Those recommendations may be for individual securities, a customized portfolio or a pre-packaged portfolio for investors with a given profile. In addition, digital tools can help develop recommendations to rebalance investors' portfolios on a periodic basis or to support tax-loss harvesting. The tools financial professionals use may be developed by their firms, acquired from third-party vendors by their firm or, in some cases, acquired by the financial professionals themselves.

In the late 1990s, the landscape of investment tools available directly to investors began to expand. Some firms started to make asset allocation tools available online. The landscape expanded further in 2005, when NASD Interpretative Material (IM) 2210-6 became effective, allowing broker-dealers to make “investment analysis tools” available to investors. FINRA defined an investment analysis tool to be an “interactive technological tool that produces simulations and statistical analyses that present the likelihood of various investment outcomes if certain investments are made or certain investment strategies or styles are undertaken.”<sup>5</sup>

Following the 2008 financial crisis, a number of new entrants began offering a wide range of digital financial tools directly to consumers, including investment advice tools. Many of these firms had their roots in the technology industry and brought new perspectives on the role of technology in financial services. The client-facing digital investment tools these firms developed offer aspects of the functionality previously only available to financial professionals. The degree of human involvement in client-facing tools varies substantially. Some firms rely on a purely digital interaction with clients while others provide optional or mandatory access to a financial professional.

In many cases, securities industry participants are responding with digital investment advice strategies of their own. Some participants are developing or acquiring client-facing investment advice tools while others are developing or acquiring financial professional-facing tools to enhance their ability to serve clients and compete more effectively. Some of these latter tools include advanced analytic tools—*e.g.*, to assess customer risk tolerance or portfolio risk—and in some cases presentation interfaces that enable the financial professional to present information to clients online. Vendors frequently position these tools as providing the basis for financial professionals to conduct more in-depth, sophisticated discussions with their client.

## Governance and Supervision

Governance and supervision of investment recommendations are recurring topics of FINRA guidance and are equally relevant to digital investment advice tools. We focus here on governance and supervision in two areas: 1) the algorithms that drive digital investment tools; and 2) the construction of client portfolios, including potential conflicts of interest that may arise in those portfolios.

### Algorithms

Algorithms are core components of digital investment advice tools. They use various financial models and assumptions to translate data inputs into suggested actions at each step of the advice value chain. The methodology by which the algorithm translates inputs into outputs should reflect a firm's approach to a particular task, *e.g.*, profiling an investor, rebalancing an account or performing tax-loss harvesting. If an algorithm is poorly designed for its task or not correctly coded, it may produce results that deviate systematically from the intended output and that adversely affect many investors.

For this reason, it is essential that firms effectively govern and supervise the algorithms they use in digital-advice tools. At the most basic level, firms should assess whether an algorithm is consistent with the firm's investment and analytic approaches. For example, a number of client-facing digital investment advice tools are based on precepts from Modern Portfolio Theory<sup>6</sup> and use a passive, index-based approach to investing based on the risk tolerance of the client, while others incorporate active management of investment portfolios. Not surprisingly, the outputs and investment advice from algorithms developed based on these approaches are likely to be different.

Even when client-facing digital advice tools take a similar approach to investing, implementation of methods for specific investing tasks, for example asset allocation, may produce very different results. Cerulli Associates compared the asset allocation for a notional 27-year-old investing for retirement across seven client-facing digital advice tools. Equity allocations ranged as high as 90 percent and as low as 51 percent; fixed income allocations ranged from 10 percent to 40 percent. (See Figure 2.) A *Wall Street Journal* analysis found similar disparities.<sup>7, 8</sup>



**Figure 2: Asset allocation model comparison<sup>9</sup>**

Asset Class	Digital Adviser A	Digital Adviser B	Digital Adviser C	Digital Adviser A	Digital Adviser D	Digital Adviser E	Digital Adviser F
Equity	90.1%	72.0%	51.0%	84.0%	60.0%	69.0%	72.2%
Domestic	42.1%	37.0%	26.0%	34.0%	30.0%	47.0%	28.9%
U.S. total stocks	16.2%	22.0%		34.0%		47.0%	13.0%
U.S. large-cap	16.2%		8.0%		19.0%		13.0%
U.S. mid-cap	5.2%						
U.S. small-cap	4.5%		18.0%		11.0%		2.9%
Dividend stocks		15.0%					
Foreign	48.0%	35.0%	25.0%	50.0%	30.0%	22.0%	43.3%
Emerging markets	10.5%	16.0%	13.0%	25.0%	9.0%	9.0%	17.0%
Developed markets	37.5%	19.0%	12.0%	25.0%	21.0%	13.0%	26.3%
Fixed income	10.1%	13.0%	40.0%	10.0%	21.5%	11.0%	15.0%
Developed markets bonds			15.0%		2.5%		4.1%
U.S. bonds	4.9%	6.0%	25.0%	10.0%	12.0%		10.9%
International bonds	3.6%						
Emerging markets bonds	1.6%	7.0%			7.0%		
Other	0.0%	15.0%	9.0%	6.0%	10.0%	16.0%	12.8%
Real estate		15.0%	9.0%	6.0%	5.0%		12.8%
Currencies						2.0%	
Gold & precious metals					5.0%		
Commodities						14.0%	
Cash					8.5%	4.0%	

**Asset Allocation Models for a 27-Year-Old Investing for Retirement, September 2015**

Source: Cerulli Associates

Note: Columns may not total to 100% due to rounding.

These examples highlight the importance of firms 1) understanding the methodological approaches embedded in the algorithms they use, including the assumptions underlying the potential scenarios on expected returns, and the biases or preferences that exist in those approaches and 2) assessing whether these methodological approaches reflect a firm's desired approach. These considerations apply both to the internal development of digital advice tools and third-party digital advice tools that firms acquire or private-label.

A look at two other areas of digital investment advice—customer risk tolerance assessment and portfolio analysis—reinforces the need for broker-dealers to establish and implement effective governance and supervision of their digital investment advice tools. FINRA reviewed several tools designed to help financial professionals understand investors' risk tolerance. In some cases, these tools also analyze the alignment of investors' portfolios with their risk tolerance and propose conforming changes to bring the portfolio into alignment. These tools vary considerably in approach to these tasks. (See *Observations on Practices* beginning on page 6 for a discussion of some of these approaches.) Good governance involves understanding if the approach to assessing customer risk tolerance is consistent with the firm's approach.

FINRA also reviewed tools to help financial professionals and their clients understand the impact of potential shocks to clients' portfolios, for example from an oil price fall, a global recession or a geo-political crisis. Careful governance would include understanding the analytic approaches that are used in these tools, including the assumptions that are made, about the impact of the shock events on the correlations in various asset price movements, among other things.

Developing an understanding of the algorithms a tool uses would also include understanding the circumstances in which their use may be inappropriate. For example, applying a tax-loss harvesting algorithm to one account of a married client where both spouses have multiple investment accounts may be detrimental. Without a full view of the couple's portfolio, the algorithm may generate unusable realized losses.

### Principles and Effective Practices: Governance and Supervision of Algorithms

Digital investment advice tools are dependent on the data and algorithms that produce the tools' output. Therefore, an effective governance and supervisory framework can be important to ensuring that the resulting advice is consistent with the securities laws and FINRA rules. Such a framework could include:

► **Initial reviews**

- assessing whether the methodology a tool uses, including any related assumptions, is well-suited to the task;
- understanding the data inputs that will be used; and
- testing the output to assess whether it conforms with a firm's expectations.

► **Ongoing reviews**

- assessing whether the models a tool uses remain appropriate as market and other conditions evolve;
- testing the output of the tool on a regular basis to ensure that it is performing as intended; and
- identifying individuals who are responsible for supervising the tool.

FINRA reinforces that a registered representative using a digital advice tool to help develop a recommendation must comply with requirements of the suitability rule and cannot rely on the tool as a substitute for the requisite knowledge about the securities or customer necessary to make a suitable recommendation.

Broker-dealers are required to supervise the types of business in which they engage. As a component of this supervision, broker-dealers should consider the nature of the advice provided, and to the extent this advice derives from digital investment advice tools, review of these tools would be useful.

In addition to the effective practices discussed above, firms should be able to address such other questions as: 1) Are the methodologies tested by independent third parties? 2) Can the firm explain to regulators how the tool works and how it complies with regulatory requirements? 3) Is there exception reporting to identify situations where a tool's output deviates from what might be expected and, if so, what are the parameters that trigger such reporting?

In the context of a financial professional-facing system, the following questions are also relevant: 1) What training or testing does the firm require before a financial professional may use the tool? 2) What discretion does the financial professional have regarding testing different scenarios and assumptions? 3) Does the firm review financial professionals' recommendations that are inconsistent with the tool's output?

## Observations on Practices

Based on FINRA's observations,<sup>10</sup> a number of entities use some form of an investment policy committee to 1) oversee the development and implementation of algorithms; 2) participate in the due diligence on third-party tools; or 3) evaluate scenarios used in firms' portfolio analysis tools. Depending on the entity, this group may be part of the broker-dealer or an affiliated entity.

For example, one firm allows registered representatives to use financial professional-facing digital advice tools, but requires all such tools to undergo an in-depth vetting and approval process. The result is that the firm permits most registered representatives to use only two firm-approved digital advice tools. The approval process for these tools includes a rigorous review by both compliance and technology staff. This review covers internal testing and vendor testing of the software to ensure that elements such as questionnaire scoring and results perform as expected. Also, these tools are incorporated into the firm's technology architecture and are protected by requirements for user entitlements and vetted to function within the firm's internal browser as added protection from cyberattacks. The tools are tested daily as part of the firm's "ready for business" testing.<sup>11</sup>

While some firms prohibit registered representatives from using digital investment advice tools without the firm's prior review and approval, others do not. We observed a firm that, in addition to allowing registered representatives to use certain pre-approved tools, also allows registered representatives to add tools that are not reviewed by the firm. The absence of a process to review such tools raises concerns about a firm's ability to adequately supervise the activities of registered representatives who use these tools, and is not consistent with the effective governance and supervision practices described above.

## Client Portfolio Construction and Monitoring, and Conflicts of Interest

In addition to their role with respect to algorithms, firms should also establish governance and supervision structures and processes for the portfolios digital investment tools may present to users. Many of these tools match investors to a pre-packaged portfolio of securities based on their profile, *i.e.*, investors with a conservative profile are placed in a conservative investment portfolio and investors with an aggressive profile are placed in an aggressive portfolio. Among the firms FINRA reviewed, most establish between five and eight investor profiles, although some firms have significantly more. In this context, the decision about the characteristics that make a portfolio suitable for a given investor profile is extremely important. (We discuss this in the *Investor Profiling* section beginning on page 8.)

The construction of portfolios may raise concerns about conflicts of interest. In the context of retail brokerage services, two categories of conflicts are particularly relevant to digital investment advice: employee vs. client and firm vs. client conflicts.<sup>12</sup> Purely digital client-facing tools eliminate the first of these conflicts because financial professionals are not involved in the advice process. Hybrid digital platforms—those that include a role for a financial professional in providing advice—may face these conflicts, depending on the incentive structure for the financial professional. Firm vs. client conflicts, however, may remain present for both financial professional- and client-facing digital advice tools, for example if a firm offers products or services from an affiliate or receives payments or other benefits from providers of the products or services.

## Principles and Effective Practices: Governance and Supervision of Portfolios and Conflicts of Interest

An effective practice for firms is to establish governance and supervisory mechanisms for the portfolios that a firm's digital investment advice tool may propose. This mechanism would:

- ▶ determine the characteristics—*e.g.*, return, diversification, credit risk and liquidity risk—of a portfolio for a given investor profile;
- ▶ establish criteria for including securities in the firm's portfolios (these can include, for example, fees, index tracking error, liquidity risk and credit risk);
- ▶ select the securities that are appropriate for each portfolio (or if this is done by an algorithm, oversee the development and implementation of that algorithm as discussed above);
- ▶ monitor pre-packaged portfolios to assess whether their performance and risk characteristics, such as volatility, are appropriate for the type of investors to which they are offered; and
- ▶ identify and mitigate conflicts of interest that may result from including particular securities in a portfolio.

The review mechanism should include staff who are independent of the business, and who can advise on both overall portfolio investment strategy and the selection of individual securities.

### Observations on Practices

As with the oversight of algorithms, the broker-dealers and other firms with which FINRA spoke typically use an investment policy committee, or equivalent body, to construct and review both the customer profiles and pre-packaged portfolios that may be offered to clients through digital investment advice tools. In some cases, the members of the committee sit in an affiliated legal entity while in others they sit within the entity. Many client-facing digital advice tools use Exchange-Traded Funds (ETFs) in creating their portfolios, and common criteria for their selection include cost, index tracking error, liquidity and bid-ask spreads.

Approaches to managing conflicts of interest that arise from security selection vary. Some financial services firms offering client-facing digital advice tools seek to avoid conflicts by not offering proprietary or affiliated funds or funds that provide revenue-sharing payments. Others follow a vet and disclose approach. Some of the principles that underlie FINRA Rule 2214 are applicable to conflicts that may arise in connection with a digital investment advice tool. Specifically, broker-dealers should disclose if the digital advice tool favors certain securities and, if so, explain the reason for the selectivity and state, if applicable, that other investments not considered may have characteristics, such as cost structure, similar or superior to those being analyzed.

## Investor Profiling

Understanding a customer's investment objectives and the specific facts and circumstances of the customer's finances—developing an investor profile—is essential to providing sound investment advice. FINRA believes that core principles regarding customer profiling apply regardless of whether that advice comes from a financial professional or an algorithm.

### Principles and Effective Practices: Customer Profiling

Customer profiling functionality is a critical component of digital advice tools because it drives recommendations to customers. Effective practices for customer profiling include:

- ▶ identifying the key elements of information necessary to profile a customer accurately;<sup>13</sup>
- ▶ assessing both a customers' risk capacity and risk willingness;<sup>14</sup>
- ▶ resolving contradictory or inconsistent responses in a customer profiling questionnaire;
- ▶ assessing whether investing (as opposed to saving or paying off debt) is appropriate for an individual;
- ▶ contacting customers periodically to determine if their profile has changed; and
- ▶ establishing appropriate governance and supervisory mechanisms for the customer profiling tool (addressed in the *Governance and Supervision* section beginning on page 3).

### Customer Profiling Information Requirements

A key question in developing a customer profile is: What information is necessary to build a customer profile with sufficient information to make a sound investment recommendation? FINRA has defined the necessary minimum body of information that broker-dealers are required to collect in its know your customer and suitability rules. FINRA Rule 2090 (Know Your Customer) requires broker-dealers to use reasonable diligence to know the essential facts concerning a customer at account opening and thereafter. When making a recommendation, FINRA Rule 2111 (Suitability) requires a broker-dealer to use reasonable diligence to obtain and analyze a customer's investment profile, which includes, but is not limited to, "the customer's age, other investments, financial situation and needs, tax status, investment objectives, investment experience, investment time horizon, liquidity needs, risk tolerance, and any other information the customer may disclose to the member or associated person in connection with such recommendation." The suitability rule also notes that "the level of importance of each factor may vary depending on the facts and circumstances of the particular case."

As a general matter, the financial professional-facing tools FINRA observed could be used to gather a broad range of information about a customer. Some tools enable the financial professional to include information about a customer's overall portfolio rather than a single account, information about a spouse's account, retirement income—e.g., Social Security and pension—and more detailed information about a client's financial condition, e.g., about expenses. Most fundamentally, though, financial professionals can ask the client questions to gather supplementary information and develop a nuanced understanding of the client's needs. The effectiveness is, of course, driven significantly by the skill of the financial professional.

By contrast, client-facing digital advice tools rely on a discrete set of questions to develop a customer profile. The tools FINRA reviewed seek answers to between four and twelve questions, generally falling into five broad categories: personal information, financial information, investment objective, time horizon and risk tolerance. (See Appendix for a sample of questions three client-facing digital advisers asked at the time of FINRA's review.)

### Customer-specific Suitability in a Digital Investment Advice Context

There are several areas of concern regarding digital advice tools, including whether they are designed to 1) collect and sufficiently analyze all of the required information about customers to make a suitability determination; 2) resolve conflicting responses to customer profile questionnaires; and 3) match customers' investment profiles to suitable securities or investment strategies. While many of these concerns can be resolved through interaction with a financial professional, the following questions may help assess whether a tool's output meets the customer-specific suitability obligation:

- ▶ Does the tool seek to obtain all of the required investment profile factors?
- ▶ If not, has the firm established a reasonable basis to believe that the particular factor is not necessary?
- ▶ How does the tool handle conflicting responses to customer profile questions?
- ▶ What are the criteria, assumptions and limitations for determining that a security or investment strategy is suitable for a customer?
- ▶ Does the tool favor any particular securities and, if yes, what is the basis for such treatment?
- ▶ Does the tool consider concentration levels and, if so, at what levels (*e.g.*, particular securities, class of securities, industry sector)?

### Assessing Risk Tolerance

Risk tolerance is an important consideration in developing a customer profile and an investment recommendation. Risk tolerance can be considered along at least two dimensions: risk capacity and risk willingness. FINRA-regulated broker-dealers are obligated to consider both in assessing a customer's risk tolerance.<sup>15</sup> Risk capacity measures an investor's ability to take risk or absorb loss. This can be a function of an investor's time horizon, liquidity needs, investment objectives and financial situation. For example, a 25-year-old customer opening an account for the purpose of retirement likely has a greater risk capacity than a 25-year-old investing to finance graduate school education in three years.

Separately, a customer's risk willingness measures the customer's attitude towards risk. For example, a customer who is willing to absorb a potential 20 percent loss over one year in return for a higher upside potential has a higher risk willingness than a customer focused on principal protection. Problems can arise when risk willingness exceeds risk capacity.

### Observations on Practices

FINRA observed firms taking a wide range of approaches to assessing a customer's risk tolerance. We focus here on two approaches: 1) those that seek to measure risk willingness and 2) those that measure risk in a portfolio in relation to the investor's risk tolerance.

There are a variety of approaches to assessing an investor's risk willingness. At the most basic level, some firms ask investors to self-assess by selecting from pre-set ratings, typically ranging from "conservative" to "aggressive."

Some approaches to assess risk willingness are scenario based and may draw on an investor's actual experience. For example, one client-facing digital advice tool asks the following questions: "Have you ever lost 20% or more of your investments in one year?" (Yes/No) followed by, for a yes answer, "In the year I lost 20% of my investments, I: a) sold everything; b) sold some; c) did nothing; d) reallocated my investments; or e) bought more."

Other approaches ask the investor to respond to hypothetical questions. One digital investment advice tool presents investors with questions regarding the amount of money they would be willing to risk to achieve a certain gain. Investors can use a slider bar to adjust the potential loss and gain to the level they are comfortable with. A different risk assessment tool asks the user to select a mix of two securities along a hypothetical budget line. The tool asks the user to make these selections multiple times for different budget lines and then aggregates the users' responses to assess various attributes of the user's risk tolerance.

Some of the vendors that offer risk tolerance assessment tools combine them with portfolio analysis tools. One vendor's tool, for example, evaluates the alignment between a customer's risk tolerance and the securities holdings in their portfolio.

Still other vendors offer tools that allow financial professionals to select from a variety of scenarios to perform "what if" risk analysis on their clients' accounts. Examples of these "what if" scenarios include emerging markets experiencing a hard landing, the Chinese economy slowing down or the U.S. credit rating being downgraded.

### Contradictory or Inconsistent Answers

In the course of answering customer profiling questions, a customer may provide contradictory responses, which firms should seek to reconcile. This can be done through discussions with the customer or, in a purely digital environment, by making a customer aware of contradictory responses and asking additional questions to resolve the inconsistency.

FINRA observed firms that averaged contradictory responses or that used the more conservative of the contradictory responses. Averaging is a poor practice, as it can result in a customer being placed in a portfolio that exceeds his or her risk tolerance. If a firm does not reconcile the customer response, taking the more conservative response is a better approach than averaging because it reduces the chance of unacceptable losses. However, even with this approach, the customer could end up with a portfolio that does not reflect their desired risk.

### Invest, Save or Pay Off Debt?

A threshold question for individuals considering opening an investment account is whether investing is an appropriate step. In some cases, they may be better served by paying off debt or saving.

An effective practice is for firms to develop a sufficient understanding of a client's financial situation to make clients aware when investing may not be appropriate for them, and FINRA observed some firms that do this. One of those firms serves a mass market client base with investable assets ranging between \$5,000 and \$100,000. This firm asks potential clients about their monthly net income—*i.e.*, income after expenses—to help determine if investing is an appropriate option. Another firm serves a generally more affluent client base and uses questions about investor time horizon and risk tolerance to determine if a client's profile is too conservative to invest. In addition, while not directly addressing the question of whether an individual should be investing, a third firm's frequently asked questions urge customers to maintain sufficient savings to cover at least six months' worth of expenses.

### Modifying Customer Profiles

FINRA-regulated broker-dealers are required to maintain essential information about their customers pursuant to FINRA Rule 2090. As firms develop their digital strategies, some may opt to allow customers to modify their profiles online. If investors frequently change their profile, an effective practice is for broker-dealers to contact the investor to understand why the investor is making these changes.

### Appropriateness of Digital Advice<sup>16</sup>

An effective practice is for firms to ask questions that would determine if an individual's advice needs cannot adequately be met solely through a digital approach. For example, a purely digital tool might not have the capability to provide a client who wishes to manage multiple investment accounts and multiple investment objectives on an integrated basis. In those instances, the client could be referred to a financial professional as part of the advice process.

### Rebalancing

Rebalancing an investment portfolio is necessary to maintain a target asset allocation over time. Rebalancing becomes necessary as the composition of an investment portfolio naturally drifts away from its intended target or when the target itself changes. Drift occurs when the constituent securities in a portfolio perform differently, which can lead to over or under weighting asset classes. This could arise, for example, through market volatility in a particular asset class or security.

#### Principles and Effective Practices: Rebalancing

Effective practices for automatic rebalancing include:

- ▶ explicitly establishing customer intent that the automatic rebalancing should occur;
- ▶ apprising the customer of the potential cost and tax implications of the rebalancing;
- ▶ disclosing to customers how the rebalancing works, including:
  - ▶ if the firm uses drift thresholds,<sup>17</sup> disclosing what the thresholds are and whether the thresholds vary by asset class;
  - ▶ if rebalancing is scheduled, disclosing whether rebalancing occurs monthly, quarterly or annually;
- ▶ developing policies and procedures that define how the tool will act in the event of a major market movement; and
- ▶ developing methods that minimize the tax impact of rebalancing.

One method to rebalance a portfolio uses customer cash flows. A digital advice tool may use multiple sources to rebalance a portfolio, including deposits, dividends, reinvestments or even withdrawals. Typically, a firm would use investment inflows and outflows to restore the target allocation of the investment portfolio; the firm uses customer contributions to purchase under-weighted asset classes and withdrawals from over-weighted asset classes. Generally, using dividends and reinvestments to rebalance a target allocation is effective when portfolio drift is minimal within an account since dividends and reinvestments would typically not be large relative to the size of the position.



In cases where cash inflows and outflows are insufficient to attain the target allocation, some digital advice tools may simply reallocate assets already within an account to achieve the targeted weightings. Reallocating assets invested in an account would typically involve the purchase and sale of assets, potentially exposing a customer to commissions and, in a taxable account, capital gains or losses.

The triggers for rebalancing vary among the client-facing tools FINRA reviewed. One firm uses a bright line threshold of 3 percent portfolio drift to initiate a rebalancing. Portfolio drift is monitored daily. By contrast, another firm's investment management committee determines the allowable drift on an *ad hoc* basis in response to market events. Similarly, two other firms monitor customer portfolios and periodically rebalance them as needed, but without stating specific drift parameters.

Depending on threshold limits and the frequency with which it conducts a rebalancing review, a digital tool could execute numerous rebalancing trades. The following questions may help assess rebalancing issues that could arise:

- ▶ Does the tool permit automatic rebalancing?
- ▶ What are the triggers for a portfolio rebalancing by the tool?
- ▶ How often does rebalancing occur?
- ▶ Does the rebalancing include the possibility of adding or removing a particular security, thereby requiring another customer-specific suitability analysis?
- ▶ Would the rebalancing result in excessive commissions or lead to adverse tax treatment?

## Training

Training and education are crucial for individuals who use digital investment advice tools. Some of the financial professional-facing tools FINRA observed can deliver sophisticated analytics, but using them effectively and communicating with clients about their output is dependent on the financial professional understanding the assumptions that go into the analytics and the potential limitations on the results.

### Principles and Effective Practices: Training

Effective practices include training financial professionals on:

- ▶ the permitted use of digital investment advice tools;
- ▶ the key assumptions and limitations of individual tools; and
- ▶ when use of a tool may not be appropriate for a client.

It is also an effective practice to assess the adequacy of any training by third-party vendors.

### Observations on Firm Practices

Most firms require financial professionals to participate in a training program before they are permitted to use a digital investment advice tool. This training varies from tool-specific training to training embedded in a firm's standard suitability training. In addition, some firms offer *ad hoc* training at the request of a financial professional.

Third-party vendors of digital investment advice tools often play a role in training staff on their tools. The vendors with which FINRA spoke typically offer one-on-one introductory training sessions with financial professionals to ensure they understand how to use the tool and how to position the output for customers. Some vendors also offer live training events once or twice a week for financial professionals, for example, to learn more about the methodology that supports a tool. In addition, some vendors offer *ad hoc* or follow-up training, although sometimes this is available only on a paid basis.

## Lessons for Investors

The use of digital investment advice tools adds nuances to the questions investors should ask and information investors should obtain and understand in opening and maintaining an investment account. We elaborate on some of those considerations here.

Sound investment advice rests on a robust understanding of an individual investor's particular needs and circumstances. Investors should evaluate whether their financial services firm gathers sufficient information and asks sufficient questions to understand their needs and risk tolerance, and whether these factors are reflected in the advice they receive. If an investor believes that relevant information is not being taken into consideration, the investor should raise this with the financial services firm before making investment decisions.

Investors should be aware that the advice they receive about allocating assets and building a portfolio depends significantly on the investment approach embodied in the algorithms and underlying assumptions used by a digital advice tool. To the degree possible, investors should familiarize themselves with the investment approach and key assumptions so that they understand how recommendations for securities and asset allocations are derived.

Since conflicts of interest may exist in the investment advice they receive, investors should evaluate whether those conflicts compromise the objectivity of that advice. Digital investment advice tools do not necessarily eliminate conflicts of interest. Conflicts could include, for example, commission payments and other incentives for a registered representative in a financial professional-facing context, and revenue sharing or sale of proprietary or affiliated products for a firm in a client-facing context.

As with any account, investors should understand the specific services they will receive and their cost. In this regard, investors should inquire about all costs associated with the services offered or provided, including costs generated from third parties, such as mutual fund management fees.

Since some accounts offer features such as rebalancing and tax-loss harvesting, investors should understand how these services will be performed. If an investor's account will be automatically rebalanced, investors should know whether this will occur based on a time schedule, *e.g.*, quarterly; based on a trigger such as portfolio drift, *e.g.*, if part of the account is more than five percent out of balance; or some other method. Investors should be aware of what safeguards, if any, exist if there are sudden, sharp market movements such as those that occurred during the May 2010 Flash Crash. Rebalancing may also generate expenses or tax liabilities, so investors should inquire into the financial consequences of this activity.

## Conclusion

Digital investment advice tools will likely play an increasingly important role in wealth management, and investor protection should be a paramount objective as firms develop their digital investment advice capabilities. Firms need to establish and maintain an investor protection foundation that accounts for the considerations raised by digital investment advice. One key element of that foundation is understanding customer needs. Another is using tools with sound methodological groundings, and a third is understanding those tools' limitations. FINRA trusts that the effective practices outlined in this document will help firms advance investor protection objectives in their use of digital investment advice tools.

## Appendix

### Comparison of Customer Profiling Questions at Three Client-Facing Digital Advisers<sup>18</sup>

Digital Advice   TOOL 1	Digital Advice   TOOL 2	Digital Advice   TOOL 3
<p><b>1. I'm saving in this account because</b></p> <ul style="list-style-type: none"><li>• I want to prepare for retirement.</li><li>• I'm saving for major upcoming expenses (education, health-bills, etc.).</li><li>• I'm saving for something special (vacation, new car, etc.).</li><li>• I need a rainy day fund for emergencies.</li><li>• I am retired or want income for expenses.</li><li>• I want to build long-term wealth.</li></ul>	<p><b>1. What are you looking for in a financial advisor?</b></p> <ul style="list-style-type: none"><li>• I'd like to create a diversified investment portfolio.</li><li>• I'd like to save money on my taxes.</li><li>• I'd like someone to completely manage my investments, so that I don't have to.</li><li>• I'd like to match or beat the performance of the markets.</li></ul>	<p><b>1. I am ____ years old and am <u>Not Retired/Retired</u>.</b></p>
<p><b>2. I have ____ understanding of stocks, bonds and ETFs.</b></p> <ul style="list-style-type: none"><li>• no</li><li>• some</li><li>• good</li><li>• extensive</li></ul>	<p><b>2. What is your current age?</b></p> <ul style="list-style-type: none"><li>• ____ years</li></ul>	<p><b>2. My annual income is ____.</b></p>

Digital Advice   TOOL 1	Digital Advice   TOOL 2	Digital Advice   TOOL 3
<p>3. When I hear “risk” related to my finances,</p> <p>_____</p> <ul style="list-style-type: none"> <li>• I worry I could be left with nothing.</li> <li>• I understand that it’s an inherent part of the investing process.</li> <li>• I see opportunity for great returns.</li> <li>• I think of the thrill of investing.</li> </ul>	<p>3. What is your annual pre-tax income?</p>	<p>3. I am not <u>new/new</u> to investing.</p>
<p>4. Have you ever lost 20% or more of your investments in one year?</p> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	<p>4. Which of the following best describes your household?</p> <ul style="list-style-type: none"> <li>• Single income, no dependents</li> <li>• Single income, at least one dependent</li> <li>• Dual income, no dependents</li> <li>• Dual income, at least one dependent</li> <li>• Retired or financially independent</li> </ul>	<p>4. Select your first goal to begin:</p> <ul style="list-style-type: none"> <li>• Safety Net</li> <li>• Retirement</li> <li>• General Investing</li> </ul>
<p>5. In the year I lost 20% of my investments, I _____</p> <ul style="list-style-type: none"> <li>• sold everything.</li> <li>• sold some.</li> <li>• did nothing.</li> <li>• reallocated my investments.</li> <li>• bought more.</li> </ul>	<p>5. What is the total value of your cash and liquid investments?</p>	

Digital Advice   TOOL 1	Digital Advice   TOOL 2	Digital Advice   TOOL 3
<p>6. When it comes to making important financial decision ...</p> <ul style="list-style-type: none"> <li>• I try to avoid making decisions.</li> <li>• I reluctantly make decisions.</li> <li>• I confidently make decisions and don't look back.</li> </ul>	<p>6. When deciding how to invest your money, which do you care about more?</p> <ul style="list-style-type: none"> <li>• Maximizing gains</li> <li>• Minimizing losses</li> <li>• Both equally</li> </ul>	
<p>7. I am ____ years old.</p>	<p>7. The global stock market is often volatile. If your entire investment portfolio lost 10% of its value in a month during a market decline, what would you do?</p> <ul style="list-style-type: none"> <li>• Sell all of your investments</li> <li>• Sell some</li> <li>• Keep all</li> <li>• Buy more</li> </ul>	
<p>8. My initial investment is ____.</p>		
<p>9. One year from now I would be comfortable with my initial investment fluctuating between ____ and ____.</p>		
<p>10. I plan to save an additional ____ per month.</p>		
<p>11. I need the money starting in ____ years for ____ years or rest of life.</p>		
<p>12. Which account type would you like to open?</p>		

## Endnotes

1. Many FINRA-registered broker-dealers are also registered as investment advisers.
2. The Aite Group projects that global spending on digital wealth management initiatives will triple, rising from \$4 billion in 2015 to \$12 billion by 2019. See Aite Group, *Wealth Management Incumbents' Digital Strategies*, Sophie Louvel Schmitt; November 2015; p. 4.
3. Tax-loss harvesting is a method to reduce capital gains tax exposure by selling one or more securities that can generate tax losses to offset capital gains. Typically, securities that are sold are replaced with securities that provide similar market exposure.
4. There is no standard definition of the activities that a “robo advisor” performs, but the tools FINRA reviewed performed these activities.
5. The material in IM 2210-6 has been substantially incorporated in FINRA Rule 2214. FINRA conditioned the offering of these tools on a firm making certain specified disclosures. See FINRA Rule 2214.
6. Modern Portfolio Theory was introduced by Professor Harry Markowitz in a March 1952 *The Journal of Finance* article titled “Portfolio Selection.”
7. See “Putting Robo Advisors to the Test,” *The Wall Street Journal*, April 24, 2015.
8. These examples relate to client-facing tools, but the same type of disparities could occur in financial professional-facing tools.
9. Cerulli’s analysis was completed in September 2015. Since then, firms may have changed their asset allocation models, added asset classes or subtracted asset classes. To make a side-by-side comparison, Cerulli grouped the investment vehicles recommended as closely as possible to the classes identified in the chart. For example, if the digital adviser uses a Real Estate Investment Trust (REIT) ETF, the percent allocated to that ETF will be represented in the Real Estate asset class. This does not mean other digital advisers do not have exposure to Real Estate: They may be obtaining their exposure through equity investment vehicles. Refer to *The Cerulli Report: Direct Firms and Digital Advice Providers* for a more detailed description of the methodology used to compare firms.
10. FINRA conducted its review in 2015. Firms’ practices may have changed since that time.
11. Ready-for-business testing refers to testing the firm does each morning to ensure that its systems are operating correctly.
12. Firm vs. client and employee vs. client conflicts exist when the incentive structures for the firm or employee may compromise the objectivity of recommendations clients receive. For further discussion see FINRA’s [Report on Conflicts of Interest](#).
13. This is an obligation for broker-dealers pursuant to FINRA Rule 2111.
14. This is an obligation for broker-dealers pursuant to FINRA Rule 2111.
15. See FINRA Rule 2111 (Suitability) and FINRA [Regulatory Notice 11-25](#), p. 4.
16. For a discussion about the application of a fiduciary standard to client-facing digital advice, see speech by SEC Commissioner Kara M. Stein, [Surfing the Wave: Technology, Innovation, and Competition](#), Remarks at Harvard Law School’s Fidelity Guest Lecture Series, November 9, 2015.
17. “Drift threshold” refers to the allowable divergence from an asset allocation. When the drift threshold is exceeded, the portfolio will be rebalanced to bring it back in line with the target asset allocation.
18. These questions may have changed since FINRA’s review.

Investor protection. Market integrity.

1735 K Street, NW  
Washington, DC 20006-1506

[www.finra.org](http://www.finra.org)  
© 2016 FINRA. All rights reserved.

16\_0106.1 –03/16

Tab 5



1 of 5 DOCUMENTS

*2016 SEC No-Act. LEXIS 280*

Investment Advisers Act of 1940 -- Section 206(3)

April 14, 2016

[\*1] J.P. Morgan Securities LLC

**TOTAL NUMBER OF LETTERS: 2**

**SEC-REPLY-1: SECURITIES AND EXCHANGE COMMISSION**  
WASHINGTON, D.C. 20549

Image of Letter

April 14, 2016

IM Ref. No. 20164111157

J.P. Morgan Securities LLC

In your letter dated April 14, 2016, you request assurance that the staff of the Division of Investment Management would not recommend enforcement action to the Securities and Exchange Commission under Section 206(3) of the Investment Advisers Act of 1940 (the "Advisers Act") if the Advisers (as defined below) and their affiliates that are registered with the Commission as broker-dealers ("broker-dealer affiliates") purchase fractional shares from certain advisory client accounts in the manner described in your letter.

Background

You State that J.P. Morgan Securities LLC and certain of its affiliates are registered with the Commission as investment advisers (collectively, the "Advisers") and that the Advisers exercise investment discretion over various client accounts through which client assets are invested in securities. You State that advisory clients who hold exchange-traded equity securities in their accounts may sometimes receive interests that represent [\*2] the right to receive the value of a fraction of a share ("fractional shares"). n1 You State further that such fractional shares are not issued by the issuer but rather are account entries meant to represent the portion of a whole share (held by a broker or another party) that an accountholder would be entitled to (including ongoing appreciation and depreciation) if fractional shares could be traded in the marketplace. n2

n1 With respect to fractional shares of investment companies, relief is requested only with respect to (i) open-end companies registered under the Investment Company Act of 1940 (the "Act") that operate as



exchange-traded funds and are not advised by an Adviser and (ii) closed-end companies that are either registered under the Act or have elected to be treated as business development companies under the Act and are not advised by an Adviser. Relief is not requested with respect to fractional shares of any other investment Company.

n2 You explain that fractional shares may occur as result of several types of events, including the transfer of an account from another investment adviser to an Adviser, or the division of an account into multiple accounts.

[\*3]

You propose that, if an Adviser determines to sell out of a client Position consisting of whole shares and fractional shares, the Adviser or a broker-dealer affiliate would purchase the fractional shares from the client on the same day and at the same price as the whole shares are sold. Alternatively, if the whole shares are transferred out of the client's account as a result of an event other than a sale, the Adviser or its broker-dealer affiliate would purchase the fractional shares from the client at that day's market closing price. n3 You State that, because fractional shares cannot be sold in the open market, there are limited, if any, alternatives to your proposed approach.

n3 You State that a transfer other than a sale may occur as a result of, for example, the closing of the account and transfer of the shares to a brokerage account or the Separation of an account into two accounts due to divorce. For a discussion of what constitutes a sale within the meaning of Section 206(3), *see* Goldman Sachs & Company, SEC Staff No-Action Letter (pub. avail. Feb. 22, 1999).

### Analysis

Section 206(3) of the Advisers Act makes it unlawful for any investment adviser, directly [\*4] or indirectly:

acting as principal for his own account, knowingly to sell any security to or purchase any security from a client... without disclosing to such client in writing before the completion of such transaction the capacity in which he is acting and obtaining the consent of the client to such transaction.

If the Adviser to a client, or another Adviser or broker-dealer affiliate that controls, is controlled by, or is under common control with that Adviser, purchases a fractional share as described above, such purchase could be considered to violate Section 206(3) unless the Adviser complies with that Section's disclosure and consent requirements. n4

n4 *See* In re Gintel Asset Mgmt, Investment Advisers Act Release No. 2079 (Nov. 8, 2002); In re Credit Suisse Asset Mgmt., Inc., Investment Advisers Act Release No. 1452 (Nov. 16, 1994); In re Concord Investment Co., Investment Advisers Act Release No. 1585 (Sept. 27, 1996); and Interplan Securities Corp., SEC Staff No-Action Letter (pub. avail. Feb. 23, 1978). *See also* Interpretation of Section 206(3) of the Investment Advisers Act of 1940, Investment Advisers Act Release No. 1732 (July 17, 1998) at n. 3 (Section 206(3) applies to certain principal or agency transactions engaged in, or effected by, a broker-dealer that controls, is controlled by, or is under common control with, an investment adviser).

[\*5]

Section 206(3) is intended to address the potential for self-dealing that can arise when an investment adviser acts as principal in a transaction with a client, such as through price manipulation. n5 In adopting Section 206(3), Congress chose not to prohibit advisers from engaging in principal transactions entirely but rather to impose disclosure and consent requirements. You State that the purchase of fractional shares as described in your letter does not present the price manipulation risk that Section 206(3) was designed to address because such purchases would be made at the market price for the corresponding whole shares. For this reason, you conclude that complying with the disclosure and consent requirements of Section 206(3) for these purchases would place a disproportionate burden on the Advisers and their clients. n6

n5 *See* Investment Trusts and Investment Companies: Hearings on S. 3580 Before the Subcomm. of the Comm. on Banking and Currency, 76th Cong., 3d Sess. 320-22 (1940). Section 206(3) is also intended to address the potential for the dumping of unwanted securities into a client's account. *Id.* Your proposal does not raise dumping concerns because clients would not be purchasing securities from the Advisers or their broker-dealer affiliates.

[\*6]

n6 You also observe that rules 152a and 236 under the Securities Act of 1933, which address registration under that Act for certain offerings related to fractional interests, reflect the Commission's recognition that fractional shares Warrant different treatment from whole shares under the federal securities laws.

### Conclusion

Based on the facts presented, we would not recommend enforcement action to the Commission under Section 206(3) of the Advisers Act if the Advisers and their broker-dealer affiliates purchase fractional shares from clients in the manner described in your letter. n7 In particular, our position is based on your representations that:

The value of the fractional shares would be immaterial (i) with respect to each applicable client and (ii) with respect to the Advisers and their broker-dealer affiliates. n8

In connection with a sale of the corresponding whole shares, the Adviser or its broker-dealer affiliate will purchase fractional shares on the same day and at same price as the whole shares. In connection with an event other than a sale, the Adviser or its broker-dealer affiliate will purchase fractional shares at that day's market closing price.

[\*7]

Neither the Advisers nor their broker-dealer affiliates will receive any commission or other compensation in connection with the purchase of fractional shares.

Because the purchase of fractional shares will always be connected to the ordinary course sale or transfer of the related whole shares held in the client's account, the Advisers will not separately determine the timing of the principal transaction.

The Adviser will disclose to clients in advance the practice of purchasing fractional shares either in a separate disclosure document, the advisory agreement or the Adviser's Form ADV. Such purchases will also be reflected on the clients' trade confirmation and account Statements, and will be identified as principal trades.

Any different facts or representations may require a different conclusion. This response expresses our position on enforcement action only and does not represent any legal conclusion on the issue presented.

n7 We note, however, that these transactions would be subject to the general antifraud provisions of Sections 206(1) and (2) of the Advisers Act.

n8 We note that fractional shares are not necessarily immaterial in value. For example, some individual securities trade with market prices in the thousands of dollars, and fractional interests in such securities may have substantial value. Our position, as described herein, would not extend to the purchase of fractional shares that have material value to the applicable client or, in the aggregate, to the Adviser or the broker-dealer affiliate purchasing the fractional shares.

[\*8]

David J. Marcinkus

Branch Chief

**INQUIRY-1:** Davis Polk & Wardwell LLP

450 Lexington Avenue  
New York, NY 10017

April 14, 2016

Mr. Douglas J. Scheidt  
Chief Counsel  
Office of Chief Counsel  
Division of Investment Management  
Securities and Exchange Commission  
100 F Street, N.E.  
Washington, D.C. 20549

Re: Request for no-action relief: Section 206(3) and fractional shares

Dear Mr. Scheidt:

On behalf of J.P. Morgan Securities LLC ("JPMS"), we respectfully request that the staff (the "Staff") of the Division of Investment Management of the Commission advise us that the Staff will not recommend Commission enforcement action under Section 206(3) of the Investment Advisers Act of 1940, as amended (the "Advisers Act"), against JPMS or certain of its affiliates that are broker-dealers registered with the Commission ("broker-dealer affiliates"), if JPMS and the broker-dealer affiliates purchase fractional shares (as defined below) from advisory client accounts as described below.

1. Factual Background

JPMS is a wholly-owned subsidiary of JPMorgan Chase & Co., a publicly-held financial Services holding Company. JPMS is registered with the Commission as both a broker-dealer and investment [\*9] adviser. Certain JPMS affiliates are also registered as investment advisers with the Commission (together with JPMS, each an "Adviser" and together the "Advisers"). The Advisers' investment advisory Services include managing and exercising investment discretion over client accounts, through which the assets of their Clients are invested in individual securities (as well as other instruments such as mutual funds and ETFs).

During the ordinary course of the Advisers' advisory Services, their clients who hold exchange-traded equity securities in their accounts may sometimes receive interests which represent the right to receive the value of a fraction of a share (*i.e.* less than one full share) of equity ownership (such interests, "fractional shares" or "fractional interests"). n1 Fractional shares are not issued by the issuer but rather are account entries meant to represent the portion of a whole share (held by a broker or another party) that an accountholder would be entitled to (including ongoing appreciation and depreciation) if fractional shares existed and could be traded in the marketplace. Fractional shares might occur as result of a transfer of an account with a fractional [\*10] interest from a third party adviser, division of an account into multiple accounts (*e.g.* due to divorce) or where an Adviser is Sponsor of a wrap program and a third party manager in the program deposits a fractional share into the wrap account. When it is time to sell the fractional share the Advisers must find an appropriate way to monetize the fractional share on behalf of the client in light of the fact that fractional shares are not supported in the market (*i.e.* fractional shares cannot be sold in the open market).

n1 With respect to fractional shares of Investment companies, relief is requested only with respect to (i)

open-end companies registered under the Investment Company Act of 1940 (the "Act") that operate as exchange-traded funds and are not advised by an Adviser and (ii) closed-end companies that are either registered under the Act or have elected to be treated as business development companies under the Act and are not advised by an Adviser. Relief is not requested with respect to fractional shares of any other investment Company.

If the Adviser or one of its broker-dealer affiliates as an accommodation to a client purchases fractional shares from the [\*11] client, the purchase from the client could be considered to violate Section 206(3) unless written disclosure is made and client consent is obtained on a transaction-by-transaction basis. However, given how irregularly fractional interests are received, how immaterial the monetary value of such interests is compared to a client's Overall holdings, and that there is no potential for abuse and no risk of price manipulation for such principal sale transactions, transaction-by-transaction disclosure and consent appears unnecessary and is impractical and would place a disproportionate burden on the Advisers and their clients. n2

n2 Application of Section 206(3) assumes that a fractional share is a security.

## 2. Request for Relief

The Advisers propose that, as an accommodation to clients, when an account holds a fractional share and the Adviser decides to sell out of a position consisting of whole shares and fractional shares, the fractional shares will be purchased from the client by the Adviser or its broker-dealer affiliate on the same day and at the same price as the whole shares and if the whole shares are transferred out of the account via journal as a result of a non-sale [\*12] event (*e.g.* closing of the managed account and transferring the shares to a brokerage account or the Separation of an account into two accounts due to divorce), the fractional share will be sold to the Adviser or its broker-dealer affiliate using the same day's market closing price.

The Adviser will Charge no commission or other compensation in connection with the purchase and the Adviser will disclose to Clients the practice of purchasing fractional shares from Clients (either via a separate disclosure document or in their advisory agreement or Form ADV).

## 3. Analysis

Section 206(3) of the Advisers Act prohibits an investment adviser from "acting as principal for his own account, knowingly to sell any security to or purchase any security from a client, or acting as broker for a person other than such client, knowingly to effect any sale or purchase of any security for the account of such client, without disclosing to such client in writing before the completion of such transaction the capacity in which he is acting and obtaining the consent of the client to such transaction." Section 206(3) imposes a prior written consent requirement on any investment adviser that acts [\*13] as principal in a transaction with a client, and is intended to address the potential for conflicts between the interests of the adviser and the client and the risk of self-dealing by the adviser. n3

n3 *See* Interpretation of Section 206(3) of the Investment Advisers Act of 1940, Advisers Act Release No. 1732 (July 17, 1998).

We believe that the purchase of fractional interests in the manner described above will not raise the conflicts of interests and self-dealing issue that Section 206(3) was meant to address. We note in that regard that (i) the price of the fractional interests will be determined by the market; (ii) the value of fractional interests received are expected to be immaterial with respect to each applicable client and with respect to the Advisers and their broker-dealer affiliates; (iii) the

purchases of fractional interests are being done as an accommodation to clients and as part of the Advisers' ordinary-course advisory Services; (iv) because the purchase of fractional shares will always be connected to the ordinary-course sale or transfer of the related whole shares in the client's account, the Advisers and their broker-dealer affiliates will not separately [\*14] determine the timing of the principal transaction; (v) there are limited, if any, alternatives to the Advisers or their broker-dealer affiliates buying the fractional interests due to the illiquid nature of fractional interests; (vi) clients will be provided clear disclosure about the arrangements with respect to fractional interests; (vii) the Advisers and their broker-dealer affiliates will not benefit from purchase transactions involving fractional interests because the price paid for fractional interests will be equivalent to the market price of the respective full interests and the Advisers and their broker-dealer affiliates will not receive any transaction-based compensation in connection with the purchase; and (viii) such transactions and the principal sale nature of such transactions will be reflected on the trade confirmation and on each applicable client's account Statement.

We believe that the proposed arrangement of providing prior written disclosure to investment advisory clients about the treatment of fractional shares together with the protective conditions outlined above, does not present the potential for conflicts of interests and risk of self-dealing that Section [\*15] 206(3) was intended to address, is consistent with the Advisers' fiduciary duty and with the best interests of their clients, and meets the investor protection objectives and satisfies the purposes of Section 206(3) of the Advisers Act. We also note that Rule 152a and Rule 236 n4 under the Securities Act of 1933, as amended, exclude fractional shares from registration requirements and appear to indicate the Commission's recognition that fractional shares Warrant different treatment than whole shares under the Federal securities laws.

n4 Rule 152a provides a safe harbor for offers or sales of fractional interests to fall within the exemption from registration by Section 4(a)(1) of the Securities Act. Rule 236 also provides an exemption from Securities Act registration for aggregation of fractional shares in connection with certain transactions.

For the foregoing reasons, we respectfully request that the Staff advise us that the Staff will not recommend Commission enforcement action against the Advisers or their broker-dealer affiliates if it proceeds as described above.

Thank you for your help with this matter. Please do not hesitate to call me at (212) 450-4684 if you need [\*16] more Information or have questions concerning this request.

Very truly yours,

Nora M. Jordan

#### **Legal Topics:**

For related research and practice materials, see the following legal topics:

Securities LawInitial Public Offerings & the Securities Act of 1933Registration of SecuritiesGeneral  
OverviewSecurities LawInvestment AdvisersGeneral OverviewSecurities LawInvestment CompaniesUnregistered  
Company Transactions

0EVA2016041801

04/25/2016

04/25/2016

Tab 6

**ROBO-ADVISERS**

Automated advisers, which are often colloquially referred to as “robo-advisers,” represent a fast-growing trend within the investment advisory industry, and have the potential to give retail investors more affordable access to investment advisory services as well as change the competitive landscape in the market for investment advice.<sup>1</sup> While many robo-advisers were initially geared towards millennials, their popularity has been expanding among all age groups and classes of investors.<sup>2</sup> Robo-advisers, which are typically registered investment advisers, use innovative technologies to provide discretionary asset management services to their clients<sup>3</sup> through online algorithmic-based programs.<sup>4</sup> A client that wishes to utilize a robo-adviser enters personal information and other data into an interactive, digital platform (e.g., a website and/or mobile application). Based on such information, the robo-adviser generates a portfolio for the client and subsequently manages the client’s account.

Robo-advisers operate under a wide variety of business models and provide a range of advisory services. For example, robo-advisers offer varying levels of human interaction to their clients. Some robo-advisers provide investment advice directly to the client with limited, if any, direct human interaction between the client and investment advisory personnel. For other robo-advisers, advice is provided by investment advisory personnel using the interactive platform to generate an investment plan that is discussed and refined with the client. Robo-advisers may also use a range of methods to collect information from their clients. For example, many robo-advisers rely solely on questionnaires of varying lengths to obtain information from their clients. Other robo-advisers obtain additional information through direct client contact or by allowing clients to provide information with regard to their other accounts.<sup>5</sup>

The Staff of the Division of Investment Management, in coordination with the Staff of the Office of Compliance Inspections and Examinations, has been monitoring and engaging with robo-advisers to evaluate how these advisers meet their obligations under the Investment Advisers Act of 1940 (the “Advisers Act”), given the unique



challenges and opportunities presented by these programs. In addition, on November 14, 2016, the Commission held a Fintech Forum that included an informative panel on these programs.<sup>6</sup> Based on input at the Forum and the Staff's observations, the Staff believes that, depending on their business models and operations, robo-advisers should keep in mind certain unique considerations as they seek to meet their legal obligations under the Advisers Act. This Staff guidance offers suggestions for how robo-advisers may address some of these issues. The Staff recognizes that there may be a variety of means for a robo-adviser to meet its obligations to its clients under the Advisers Act, and that not all of the issues addressed in this guidance will be applicable to every robo-adviser.

This Staff guidance focuses on robo-advisers that provide services directly to clients over the internet. This guidance, however, may be helpful for other types of robo-advisers as well as other registered investment advisers.<sup>7</sup>

#### **Potential Considerations under the Advisers Act**

Robo-advisers, like all registered investment advisers, are subject to the substantive and fiduciary obligations of the Advisers Act.<sup>8</sup> Because robo-advisers rely on algorithms, provide advisory services over the internet, and may offer limited, if any, direct human interaction to their clients, their unique business models may raise certain considerations when seeking to comply with the Advisers Act. This guidance focuses on three distinct areas identified by the Staff, listed below, and provides suggestions on how robo-advisers may address them:

1. The substance and presentation of disclosures to clients about the robo-adviser and the investment advisory services it offers;
2. The obligation to obtain information from clients to support the robo-adviser's duty to provide suitable advice; and
3. The adoption and implementation of effective compliance programs reasonably designed to address particular concerns relevant to providing automated advice.

While this guidance focuses on the obligations of robo-advisers under the Advisers Act, robo-advisers should consider whether the organization and operation of their programs raise any issues under the other federal securities laws, including the Investment Company Act of 1940 (the "Investment Company Act"), and in particular Rule 3a-4 under that Act.<sup>9</sup> To the extent that a robo-adviser believes that its organization and operation raise unique facts or circumstances not addressed by Rule 3a-4, such adviser may wish to consider contacting the Staff for further guidance.



## 1. Substance and Presentation of Disclosures

The information a client receives from an investment adviser is critical to his or her ability to make informed decisions about engaging, and then managing the relationship with, the investment adviser.<sup>10</sup> As a fiduciary, an investment adviser has a duty to make full and fair disclosure of all material facts to, and to employ reasonable care to avoid misleading, clients.<sup>11</sup> The information provided must be sufficiently specific so that a client is able to understand the investment adviser's business practices and conflicts of interests.<sup>12</sup> Such information must be presented in a manner that clients are likely to read (if in writing) and understand.<sup>13</sup>

Particularly because client relationships with robo-advisers may occur with limited, if any, human interaction, robo-advisers should be mindful that the ability of a client to make an informed decision about whether to enter into, or continue, an investment advisory relationship may be dependent solely on a robo-adviser's electronic disclosures made via email, websites, mobile applications, and/or other electronic media.<sup>14</sup> Furthermore, given the unique aspects of their business models, including their reliance on algorithms and the internet as a means of providing advisory services, robo-advisers may wish to consider the most effective way to communicate to their clients the limitations, risks, and operational aspects of their advisory services. Accordingly, as discussed below, when designing its disclosures, it may be useful for a robo-adviser to consider how it explains its business model and the scope of the investment advisory services it provides, as well as how it presents material information to clients.

### *Explanation of Business Model*

To address potential gaps in a client's understanding of how a robo-adviser provides its investment advice, the robo-adviser (like all registered investment advisers) should disclose, in addition to other required information,<sup>15</sup> information regarding its particular business practices and related risks.<sup>16</sup> Information a robo-adviser should consider providing includes:

- A statement that an algorithm is used to manage individual client accounts;
- A description of the algorithmic functions used to manage client accounts (e.g., that the algorithm generates recommended portfolios; that individual client accounts are invested and rebalanced by the algorithm);
- A description of the assumptions and limitations of the algorithm used to manage client accounts (e.g., if the algorithm is based on modern portfolio theory, a description of the assumptions behind and the limitations of that theory);

- A description of the particular risks inherent in the use of an algorithm to manage client accounts (e.g., that the algorithm might rebalance client accounts without regard to market conditions or on a more frequent basis than the client might expect; that the algorithm may not address prolonged changes in market conditions);
- A description of any circumstances that might cause the robo-adviser to override the algorithm used to manage client accounts (e.g., that the robo-adviser might halt trading or take other temporary defensive measures in stressed market conditions);
- A description of any involvement by a third party in the development, management, or ownership of the algorithm used to manage client accounts, including an explanation of any conflicts of interest such an arrangement may create (e.g., if the third party offers the algorithm to the robo-adviser at a discount, but the algorithm directs clients into products from which the third party earns a fee);
- An explanation of any fees the client will be charged directly by the robo-adviser, and of any other costs that the client may bear either directly or indirectly (e.g., fees or expenses clients may pay in connection with the advisory services provided, such as custodian or mutual fund expenses; brokerage and other transaction costs);
- An explanation of the degree of human involvement in the oversight and management of individual client accounts (e.g., that investment advisory personnel oversee the algorithm but may not monitor each client's account);
- A description of how the robo-adviser uses the information gathered from a client to generate a recommended portfolio and any limitations (e.g., if a questionnaire is used, that the responses to the questionnaire may be the sole basis for the robo-adviser's advice; if the robo-adviser has access to other client information or accounts, whether, and if so, how, that information is used in generating investment advice); and
- An explanation of how and when a client should update information he or she has provided to the robo-adviser.

### *Scope of Advisory Services*

Robo-advisers, like all registered investment advisers, should consider the clarity of the descriptions of the investment advisory services they offer and use reasonable care to avoid creating a false implication or sense about the scope of those services which may materially mislead clients.<sup>17</sup> Robo-advisers should be careful not to mislead clients by implying, for example, that:

- The robo-adviser is providing a comprehensive financial plan if it is not in fact doing so (e.g., if the robo-adviser does not take into consideration a client's tax situation or debt obligations, or if the investment advice is only targeted to meet a specific goal—such as paying for a large purchase or college tuition—without regard to the client's broader financial situation);
- A tax-loss harvesting service also provides comprehensive tax advice; or
- Information other than that collected by the questionnaire (e.g., information concerning other client accounts held with the robo-adviser, its affiliates or third parties; information supplementally submitted by the client) is considered when generating investment recommendations if such information is not in fact considered.

### *Presentation of Disclosures*

Robo-advisers may or may not make investment advisory personnel available to clients to highlight and explain important concepts. Clients may also be unlikely to read or understand disclosures that are dense and that are not in plain English. After reviewing the websites and disclosures of a number of robo-advisers, we have observed that robo-advisers utilize a variety of practices in providing important information to their clients. Because of robo-advisers' reliance on online disclosures to provide such information, there may be unique issues that arise when communicating key information, risks, and disclaimers.<sup>18</sup> We therefore remind robo-advisers to carefully consider whether their written disclosures are designed to be effective (e.g., are not buried<sup>19</sup> or incomprehensible<sup>20</sup>). In particular, in presenting their disclosures, robo-advisers may wish to consider:

- Whether key disclosures are presented prior to the sign-up process so that information necessary to make an informed investment decision is available to clients before they engage, and make any investment with, the robo-adviser;
- Whether key disclosures are specially emphasized (e.g., through design features such as pop-up boxes);

- Whether some disclosures should be accompanied by interactive text (e.g., through design features such as tooltips<sup>21</sup>) or other means to provide additional details to clients who are seeking more information (e.g., through a “Frequently Asked Questions” section); and
- Whether the presentation and formatting of disclosure made available on a mobile platform have been appropriately adapted for that platform.

## 2. Provision of Suitable Advice

An investment adviser’s fiduciary duty includes an obligation to act in the best interests of its clients and to provide only suitable investment advice.<sup>22</sup> Consistent with these obligations, an investment adviser must make a reasonable determination that the investment advice provided is suitable for the client based on the client’s financial situation and investment objectives.<sup>23</sup>

### *Reliance on Questionnaires to Gather Client Information*

We have observed that robo-advisers may provide investment advice based primarily, if not solely, on client responses to online questionnaires. The questionnaires we have reviewed have varied with respect to length and the types of information requested. For example, some robo-advisers generate a recommended portfolio based upon a client’s age, income and financial goals. Other robo-advisers may obtain through their questionnaires different or additional information such as investment horizon, risk tolerance, and/or living and other expenses when generating a recommended portfolio. We have also observed that some of these questionnaires are not designed to provide a client with the opportunity to give additional information or context concerning the client’s selected responses. In addition, robo-advisers may not be designed so that advisory personnel may ask follow-up or clarifying questions about a client’s responses, address inconsistencies in client responses, or provide a client with help when filling out the questionnaire. Given this limited interaction, when considering whether its questionnaire is designed to elicit sufficient information to support its suitability obligation, a robo-adviser may wish to consider factors such as:

- Whether the questions elicit sufficient information to allow the robo-adviser to conclude that its initial recommendations and ongoing investment advice are suitable and appropriate for that client based on his or her financial situation and investment objectives;<sup>24</sup>
- Whether the questions in the questionnaire are sufficiently clear and/or whether the questionnaire is designed to provide additional clarification or examples to clients when necessary (e.g., through the use of design features, such as tool-tips or pop-up boxes); and

- Whether steps have been taken to address inconsistent client responses, such as:
  - Incorporating into the questionnaire design features to alert a client when his or her responses appear internally inconsistent and suggest that the client may wish to reconsider such responses; or
  - Implementing systems to automatically flag apparently inconsistent information provided by a client for review or follow-up by the robo-adviser.<sup>25</sup>

### *Client-Directed Changes in Investment Strategy*

Many robo-advisers give clients the opportunity to select portfolios other than those that they have recommended.<sup>26</sup> Some robo-advisers do not, however, give a client the opportunity to consult with investment advisory personnel about how the client-selected portfolio relates to the client's stated investment objective and risk profile, and its suitability for that client. This may result in a client selecting a portfolio that the robo-adviser believes is not suitable for the investment objective and risk profile the robo-adviser has generated for the client based on his or her questionnaire responses. Thus, consistent with its obligation to act in its client's best interests, a robo-adviser should consider providing commentary as to why it believes particular portfolios may be more appropriate for a given investment objective and risk profile. In this regard, a robo-adviser may wish to consider whether pop-up boxes or other design features would be useful to alert a client of potential inconsistencies between the client's stated objective and the selected portfolio.

### **3. Effective Compliance Programs**

Rule 206(4)-7 under the Advisers Act requires each registered investment adviser to establish an internal compliance program that addresses the adviser's performance of its fiduciary and substantive obligations under that Act. To comply with the rule, a registered investment adviser must adopt, implement, and annually review written policies and procedures that are reasonably designed to prevent violations of the Advisers Act and the rules thereunder, and that take into consideration the nature of the firm's operations and the risk exposures created by such operations.<sup>27</sup> A registered investment adviser must also designate a chief compliance officer who is competent and knowledgeable about the Advisers Act to be responsible for administering the written policies and procedures adopted.<sup>28</sup>

In developing its compliance program, a robo-adviser should be mindful of the unique aspects of its business model. For example, a robo-adviser's reliance on algorithms, the limited, if any, human interaction with clients, and the provision of advisory services over the internet may create or accentuate risk exposures for the robo-adviser that should

be addressed through written policies and procedures.<sup>29</sup> Thus, in addition to adopting and implementing written policies and procedures that address issues relevant to traditional investment advisers,<sup>30</sup> robo-advisers should consider whether to adopt and implement written policies and procedures that address areas such as:

- The development, testing, and backtesting of the algorithmic code and the post-implementation monitoring of its performance<sup>31</sup> (e.g., to ensure that the code is adequately tested before, and periodically after, it is integrated into the robo-advisers' platform; the code performs as represented;<sup>32</sup> and any modifications to the code would not adversely affect client accounts);
- The questionnaire eliciting sufficient information to allow the robo-adviser to conclude that its initial recommendations and ongoing investment advice are suitable and appropriate for that client based on his or her financial situation and investment objectives;
- The disclosure to clients of changes to the algorithmic code that may materially affect their portfolios;
- The appropriate oversight of any third party that develops, owns, or manages the algorithmic code or software modules utilized by the robo-adviser;
- The prevention and detection of, and response to, cybersecurity threats;<sup>33</sup>
- The use of social and other forms of electronic media in connection with the marketing of advisory services (e.g., websites; Twitter; compensation of bloggers to publicize services; "refer-a-friend" programs);<sup>34</sup> and
- The protection of client accounts<sup>35</sup> and key advisory systems.<sup>36</sup>

## Conclusion

Robo-advisers represent a fast-growing trend within the investment advisory industry, and have the potential to give retail investors more affordable access to investment advisory services. As registered investment advisers, robo-advisers should be mindful that they are subject to the fiduciary and other substantive requirements of the Advisers Act. This guidance is intended to provide suggestions to such advisers as they seek to meet their obligations under that Act. As the investment advisory industry continues to innovate and develop new ways to provide advisory services to clients, the Staff will monitor these innovations and implement safeguards, as necessary, to help facilitate such developments and protect investors.

## Endnotes

- 1 See, e.g., Andrew Meola, *The Fintech Report 2016: Financial Industry Trends and Investment*, Business Insider (Dec. 14, 2016), available at: <http://www.businessinsider.com/the-fintech-report-2016-financial-industry-trends-and-investment-2016-12?r=UK&IR=T>; Marlene Y. Satter, Robo-Advisors Will Disrupt Market: Study, Benefitspro.com (Aug. 8, 2016), available at: <http://www.benefitspro.com/2016/08/08/robo-advisors-will-disrupt-market-study>; Sarah Kocianski, *Robo-Advisor Report: Market Share, Returns and Key Growth Drivers*, Business Insider (June 9, 2016), available at: <http://www.businessinsider.com/the-robo-advising-report-market-forecasts-key-growth-drivers-and-how-automated-asset-management-will-change-the-advisory-industry-2016-6>.
- 2 See, e.g., Richard Eisenberg, *Robo-Advisers: Not Just for Millennials Anymore?* (Dec. 6, 2016), available at: <http://www.forbes.com/sites/nextavenue/2016/12/06/robo-advisers-not-just-for-millennials-anymore/>.
- 3 For purposes of this guidance, the term “client” also includes “prospective client.”
- 4 For purposes of this guidance, the term “robo-adviser” includes both the registered investment adviser and any automated investment advisory program it offers.
- 5 We also note that some robo-advisers operate as stand-alone companies, while others are business units of larger, traditional investment advisers. Furthermore, some robo-advisers enable clients to access their services directly. Other robo-advisers are offered as digital portfolio management tools by traditional advisers that view these programs as components of their existing advisory practices.
- 6 See generally Fintech Forum, SEC (Nov. 14, 2016), available at: <https://www.sec.gov/spotlight/fintech> (“Fintech Forum”). An unofficial transcript of the November 14, 2016 Fintech Forum is available at: <https://www.sec.gov/spotlight/fintech/transcript-111416.pdf> (“Forum Transcript”).

The increasing use of digital advice tools has also been the focus of other regulators and certain international bodies. See, e.g., *Update to the Report on the IOSCO Automated Advice Tools Survey*, International Organization of the Securities Commissions (Dec. 2016), available at: <http://www.iosco.org/library/pubdocs/pdf/IOSCOPD552.pdf>; Report on Digital Investment Advice, FINRA (March, 2016), available at: <http://www.finra.org/sites/default/files/digital-investment-advice-report.pdf>; *Regulating Digital Financial Product Advice*, Australian Securities

& Investments Commission (March 21, 2016), *available at*: <http://asic.gov.au/regulatory-resources/find-a-document/consultation-papers/cp-254-regulating-digital-financial-product-advice/>.

- 7 See *generally* Forum Transcript, *supra* note 6, at 38 (Bo Lu, Co-Founder and CEO of Future Advisor at Blackrock) (“Digital advice actually underpins a whole spectrum of delivery models. And there will be places where . . . you’ll have an almost exclusively digital relationship, and places where you’ll have what appears to the end user an almost exclusively human-based relationship, underpinned by digital [advice] that the client never knew about.”).
- 8 As SEC-registered investment advisers, robo-advisers are subject to all of the requirements of the Advisers Act, including the requirement that they provide advice consistent with the fiduciary duty they owe to their clients. A general overview of the regulatory requirements of the Advisers Act can be found at <https://www.sec.gov/divisions/investment/advoverview.htm>. This guidance focuses on certain issues that robo-advisers should consider due to the nature of their business model.
- 9 See Rule 3a-4 under the Investment Company Act (creating a non-exclusive safe-harbor from the definition of “investment company” for advisory programs that meet Rule 3a-4’s requirements). See *also* Status of Investment Advisory Programs under the Investment Company Act of 1940, Investment Company Act Release No. 21260 (July 27, 1995) (discussing circumstances in which an investment advisory program may be considered an investment company).
- 10 See Amendments to Form ADV, Advisers Act Release No. 3060 (July 28, 2010) (“Amendments to Form ADV Adopting Release”). See *also* Advisers Act Rule 204-3(b) (requiring delivery of a brochure before or at the time an adviser enters into an investment advisory contract with a client). An adviser’s disclosure responsibilities are broad and delivery of the adviser’s brochure alone may not fully satisfy the adviser’s disclosure obligations. See Instruction 3 of General Instructions for Part 2 of Form ADV; Advisers Act Rule 204-3(f) (delivery of a brochure or brochure supplement does not relieve an adviser of any other disclosure obligations it has to its advisory clients).
- 11 See SEC v. Capital Gains Research Bureau, Inc., et al., 375 U.S. 180, 186, 194 (1963). See *also* H. R. Rep. No. 85, 73d Cong., 1st Sess. 2; General Instruction 3 to Part 2 of Form ADV.



- 12 See Amendments to Form ADV Adopting Release, *supra* note 10, at n. 28. See also Staff of the U.S. Securities and Exchange Commission, Study on Investment Advisers and Broker-Dealers As Required by Section 913 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, n. 531 (Jan. 2011) (the “Study”), available at: [www.sec.gov/news/studies/2011/913studyfinal.pdf](http://www.sec.gov/news/studies/2011/913studyfinal.pdf); Instruction 3 of General Instructions for Part 2 of Form ADV.
- 13 Amendments to Form ADV Adopting Release, *supra* note 10. See also In the Matter of Arlene W. Hughes d/b/a E. W. Hughes & Company, Securities Exchange Act Release No. 4048 (Feb. 18, 1947).
- 14 Robo-advisers should also be mindful to make disclosures in plain English. See generally Instruction 2 of General Instructions for Part 2 of Form ADV (providing guidance on drafting in plain English); Amendments to Form ADV Adopting Release, *supra* note 10. See also A Plain English Handbook, SEC Office of Investor Education and Assistance (August 1998), available at: <https://www.sec.gov/pdf/handbook.pdf>.
- 15 See *supra* note 10.
- 16 See Amendments to Form ADV Adopting Release, *supra* note 10 (“To allow clients and prospective clients to evaluate the risks associated with a particular investment adviser, its business practices, and its investment strategies, it is essential that clients and prospective clients have clear disclosure that they are likely to read and understand”). See generally Forum Transcript, *supra* note 6, at 71 (Mark Goines, Vice Chairman of Personal Capital) (“[T]he other area that I think is really important for us. . . [is] making sure . . . that the accountability to the clients is clear and that that’s fully disclosed.”).
- 17 See, e.g., In the Matter of T. Rowe Price and Associates, Inc., Advisers Act Release No. 658 (Jan. 16, 1979) (settled action) (a registered investment adviser “willfully violated Section 206 of the Investment Advisers Act of 1940 in that it failed to adequately and accurately disclose in certain promotional literature and otherwise to actual and prospective . . . clients the amount of individualized treatment provided to each . . . account and the extent to which investment decisions for . . . accounts would be made and implemented based upon ‘model portfolios.’”).

- 18 In other contexts, the Staff has taken the position that a relevant factor to consider when determining if potentially confusing disclosures are misleading is whether such disclosures are individually highlighted and explained during an in-person meeting. See, e.g., Heitman Capital Management, LLC, SEC Staff No-Action Letter (Feb. 12, 2007) (addressing the use of certain hedge clauses in certain advisory contracts).
- 19 Under the “buried facts” doctrine, a court would consider disclosure to be false and misleading if its overall significance is obscured because material information is “buried,” for example in a footnote or appendix. See Commission Guidance on the Use of Company Web Sites, Investment Company Act Release No. 28351 (Aug. 1, 2008) at n. 68.
- 20 See generally *id.*
- 21 A tooltip allows additional information to be shown in a text box when a mouse cursor hovers over a particular item on a web page.
- 22 Status of Investment Advisory Programs under the Investment Company Act of 1940, Investment Company Act Release No. 22579 (Mar. 24, 1997) at text accompanying n.32 (“Investment advisers under the Advisers Act owe their clients the duty to provide only suitable investment advice, whether or not the advice is provided to clients through an investment advisory program. To fulfill this suitability obligation, an investment adviser must make a reasonable determination that the investment advice provided is suitable for the client based on the client’s financial situation and investment objectives.”) (“Rule 3a-4 Adopting Release”), *citing to* Suitability of Investment Advice Provided by Investment Advisers, Advisers Act Release No. 1406 (Mar. 16, 1994) (“Suitability Rule Proposing Release”) (proposing a rule under Section 206(4) of the Advisers Act that would expressly require advisers to give clients only suitable advice; the rule would have codified existing suitability obligations of advisers). See also The Study, *supra* note 12, at 22, 27. We note that the Commission has brought a number of enforcement actions against investment advisers for failing to provide suitable investment advice. See, e.g., In re David A. King and King Capital Corp., Advisers Act Release No. 1391 (Nov. 9, 1993) (investment adviser recommended investments in a risky pool of first, second and third mortgages to retirees and others of limited means); In re George Sein Lin, Advisers Act Release No. 1174 (June 19, 1989) (investment adviser with discretionary investment authority invested funds of clients desiring low-risk investments in uncovered option contracts and utilized margin brokerage accounts); In re

Westmark Financial Services, Corp., Advisers Act Release No. 1117 (May 16, 1988) (financial planner recommended speculative equipment leasing partnerships to unsophisticated investors with modest incomes); *In re Shearson, Hammill & Co.*, 42 SEC 811 (1965) (sections 206(1) and (2) violated when adviser recommended investments unsuitable to child and widow).

- 23 See Rule 3a-4 Adopting Release, *supra* note 22, at text accompanying n.32. See also *The Study*, *supra* note 12, at 27; Suitability Rule Proposing Release, *supra* note 22.
- 24 See generally Forum Transcript, *supra* note 6, at 66 (Mark Goines, Vice Chairman of Personal Capital) (“[Does the robo-adviser] have enough of an understanding of the client to be able to apply the algorithm, or is the algorithm actually collecting enough data to actually apply its applied rules effectively? . . . We have to be very careful that the algorithms are very good but that the inputs are robust, so that we really truly understand the client before we apply it. . . . [A]lgorithms with minimal input run the risk of not fully understanding the client.”).
- 25 For example, a client could indicate that he or she wants a conservative strategy, but would like to invest primarily in high-yield bonds. Similarly, an elderly client may indicate a long-term investment time horizon.
- 26 For example, some robo-advisers allow a client to adjust his or her portfolio away from the strategy the adviser has recommended — including by allowing the client to adjust a slider or risk score to select a portfolio that is more or less aggressive than the portfolio recommended by the robo-adviser.
- 27 Compliance Programs of Investment Companies and Investment Advisers, Advisers Act Release No. 2204 (Dec. 17, 2003) at n.10 and n. 17 and accompanying text (“Adopting Release to Rule 206(4)-7”) (“Each adviser, in designing its policies and procedures, should first identify conflicts and other compliance factors creating risk exposure for the firm and its clients in light of the firm’s particular operations, and then design policies and procedures that address those risks”). The Commission has generally stated that these policies and procedures should cover at a minimum (to the extent they are applicable to the adviser), such areas as portfolio management processes, trading practices, proprietary trading, personal trading activities of supervised persons, disclosure requirements, custody, maintenance of books and records, marketing and cash solicitation activities, valuation, privacy concerns and business continuity plans. See *id.* at nn.17-22 and accompanying text (setting forth a detailed list of areas where the Commission expects registered investment advisers to adopt policies and procedures).

- 28 *Id.* at n.73 and accompanying text.
- 29 *See supra* note 27 and accompanying text.
- 30 *See id.*
- 31 *See generally* Forum Transcript, *supra* note 6, at 59 (Jim Allen, Head of Capital Markets Policy Group, CFA Institute) (“[Many CFA Institute members believe] the biggest risk in the Fintech space is . . . flaws in the algorithms behind these technologies.”).
- 32 *See, e.g.,* In the Matter of AXA Rosenberg Group, LLC, et al., Advisers Act Release No. 3149 (Feb. 3, 2011) (settled action) (In a settled administrative proceeding, the Commission found that two affiliated investment advisers that used a quantitative investment model in managing client accounts breached their fiduciary obligations to their clients by concealing and delaying to fix a material error in the model. One of the investment advisers was also found to have failed to adopt and implement policies and procedures reasonably designed to ensure that it did not make false and misleading statements to clients and investors, including failing to ensure that the model performed as represented, in violation of antifraud provisions of the Advisers Act).
- 33 *See, e.g.,* Cybersecurity Guidance, IM Guidance Update No. 2015-02, April 2015. *See also* Adviser Business Continuity and Transition Plans, Advisers Act Release No. 4439 (June 28, 2016) at n. 77 and accompanying text (“An adviser generally should consider and address as relevant the operational and other risks related to cyber-attacks”).
- 34 *See, e.g.,* Advisers Act Rule 206(4)-1 (addressing advertisements by investment advisers and prohibiting client testimonials); Advisers Act Rule 206(4)-3 (making cash payments to solicitors by registered investment advisers unlawful unless certain conditions are met); Guidance on the Testimonial Rule and Social Media, IM Guidance Update No. 2014-04, March 2014.
- 35 *See, e.g.,* Advisers Act Rule 206(4)-2 (addressing custody of funds or securities of clients by investment advisers). *See also* Staff Responses to Questions About the Custody Rule, Question II.6. (Sept. 1, 2013) available at: [http://www.sec.gov/divisions/investment/custody\\_faq\\_030510.htm](http://www.sec.gov/divisions/investment/custody_faq_030510.htm) (an investment adviser is deemed

to have custody of client assets if the adviser is provided password access to an account and such access provides the adviser with the ability to withdraw funds or securities or transfer them to an account not in the client's name at a qualified custodian).

- 36 See, e.g., Adopting Release to Rule 206(4)-7, *supra* note 27, at n. 22 (“We believe that an adviser’s fiduciary obligation to its clients includes the obligation to take steps to protect the clients’ interests from being placed at risk as a result of the adviser’s inability to provide advisory services.”).

*IM Guidance Updates are recurring publications that summarize the staff’s views regarding various requirements of the federal securities laws. The Division generally issues IM Guidance Updates as a result of emerging asset management industry trends, discussions with industry participants, reviews of registrant disclosures, and no-action and interpretive requests.*

*The statements in this IM Guidance Update represent the views of the Division of Investment Management. This guidance is not a rule, regulation or statement of the Securities and Exchange Commission. Further, the Commission has neither approved nor disapproved its content. Future changes in rules, regulations, and/or staff no-action and interpretive positions may supersede some or all of the guidance in a particular IM Guidance Update.*

The mission of the Securities and Exchange Commission is to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation.

---

**If you have any questions about this IM Guidance Update, please contact:**

ROCHELLE KAUFFMAN PLESSET  
ROBERT H. SHAPIRO  
CHIEF COUNSEL’S OFFICE  
PHONE: 202.551.6825  
EMAIL: IMOCC@SEC.GOV

Tab 7

## Investor Alerts and Bulletins

---

# Investor Bulletin: Robo-Advisers

**Feb. 23, 2017**

*The last few years have seen the growth in availability and popularity of automated digital investment advisory programs (often called “robo-advisers”). These programs allow individual investors to create and manage their investment accounts through a web portal or mobile application, sometimes with little or no interaction with a human being with the potential benefit of lower costs than traditional investment advisory programs. The SEC’s Office of Investor Education and Advocacy is issuing this Investor Bulletin to educate investors about these programs, and to help investors using robo-advisers to make informed decisions in meeting their investment goals.*

### **What is a Robo-Adviser?**

The term “robo-adviser” generally refers to an automated digital investment advisory program. In most cases, the robo-adviser collects information regarding your financial goals, investment horizon, income and other assets, and risk tolerance by asking you to complete an online questionnaire. Based on that information, it creates and manages an investment portfolio for you. Robo-advisers often seek to offer investment advice for lower costs and fees than traditional advisory programs, and in some cases require lower account minimums than traditional investment advisers. The services provided, approaches to investing, and features of robo-advisers vary widely. You can find information about these topics in the adviser’s [Form ADV Part 1 and Part 2 brochure](#).

While robo-advisers have similarities to traditional investment advisory programs, there are also differences. Before making a decision about whether to invest through a robo-adviser, or in deciding which robo-adviser might be best for you, you should do your own research. Make sure the robo-adviser and the investment portfolio it puts together for you are a good match for your investment needs and goals, and that you understand the potential costs, risks, and benefits of using that particular robo-adviser. Below we’ve highlighted some issues you may want to consider in making these important decisions.

### **What Level of Interaction with a Person is Important to You?**

The amount of human interaction available to you may vary from one robo-adviser to another. Some robo-advisers may offer the opportunity to contact an investment professional to discuss your investment needs (this hybrid of both automated and personal advice is sometimes referred to as “bionic” advice). Other robo-advisers may only make technical support staff available, which will limit you to relying on the information on their websites or other sources you find to address your questions about investing.

If a robo-adviser does make an investment professional available to you, the format and amount of the interaction may also vary. For example, a person may be available by email but not by phone, or available only for a limited number of in-person meetings. In some cases, a robo-adviser may offer access to a person only for accounts that meet a certain minimum account size. Still other robo-advisers may offer limited, if any, involvement of an investment professional in the creation and management of a client’s account.

Unlike a traditional investment adviser, there may be no initial or subsequent conversation with a person to gather information about you and your personal financial needs. However, the robo-adviser may be able to offer you lower costs and fees by limiting the expense associated with a human adviser’s time.

As with any adviser, it is very important you take the time to learn about the robo-adviser's services, including the level of interaction with a person, and find out answers to any questions you may have. Here are a few questions to consider:

- *How much human interaction is important to you? Would you like to be able to ask a person questions about your investments, the investment strategy being used, and potential risks? Would you like to be able to speak with a person during market events, such as periods of exceptional volatility or downturns? Do you prefer being able to talk in person or on a phone, or is electronic communication fine with you?*
- *What is your level of financial literacy, especially when it comes to investing? Your ability to ask a person questions about investing (for example, about the robo-adviser's investment strategy) may be limited and you may need to rely almost entirely on the robo-adviser's online disclosures or other sources of information that you find on your own. Are you comfortable using online resources?*
- *As with a traditional adviser, you may be interested in how often you will have contact with the robo-adviser. For example, how often does the robo-adviser follow-up with clients to confirm any changes that would affect their investment choices? Would you have to contact the robo-adviser with any updates to your financial situation?*

### ***What Information is the Robo-Adviser Using to Create a Recommendation?***

A robo-adviser uses information you provide to create a recommendation. As a result, a robo-adviser's recommendation is limited by the information it requests and receives from you, typically through an online questionnaire. It is important to keep in mind that some robo-advisers may obtain and consider only limited information about you. In addition, as with traditional advisers, in many cases the burden to update this information will fall on you. Here are a few questions to consider:

- *Would you use the robo-adviser for a specific financial goal (for example, retirement, buying a home, or investing for your children's education), or to meet your overall financial needs more broadly? Does the robo-adviser's recommendation take into account your purpose in using the robo-adviser?*
- *Does the robo-adviser's recommendation take into account relevant personal financial information, given your goal? For example, does the robo-adviser ask for information about high interest credit card debt or student loans you may have? Does it take into account your bank and savings accounts? Does it take into account your real estate holdings, such as your home, or other investments such as retirement accounts? Does it take into account other assets that you have?*
- *How does the robo-adviser take into account your tolerance for risk? How you respond to the robo-adviser's questions about risk can affect what portfolio the robo-adviser recommends. In addition to the initial makeup of your portfolio, how does your risk tolerance impact how the robo-adviser might rebalance your portfolio (for example, in the event of a market decline)?*

### ***What is the Robo-Adviser's Approach to Investing?***

Different robo-advisers have different approaches to investing, including different investment styles and different products offered. Some have several pre-determined portfolios of investments that they will recommend for you that you may or may not be able to customize. Some robo-advisers focus solely on a limited range of investment products, such as broad-based exchange-traded funds, or ETFs.





**Exchange-Traded Funds**

Many robo-advisers utilize ETFs. ETFs have unique characteristics that may make them more suitable for certain investors and less suitable for others. To learn more about ETFs, including how they differ from mutual funds, read our [Investor Bulletin: Exchange-Traded Funds \(ETFs\)](#). Also, certain robo-advisers may use hypothetical performance for newer ETFs in their marketing materials. To learn more about performance claims, read our [Investor Bulletin: Performance Claims](#)

Some robo-advisers may recommend emerging market funds or invest in smaller companies, which could be more volatile or potentially less [liquid](#). The investment style of the robo-adviser can make a big difference in the asset allocation of your portfolio. In addition, some robo-advisers have additional features that can affect returns on your investment. Also, in some cases robo-advisers may not have been tested under stressed market conditions.

You should take the time to understand how the robo-adviser develops a portfolio recommendation, and what pieces of information it uses – or does not use – in developing the portfolio. Here are a few questions to consider:

- Does the robo-adviser offer a limited range of investment products, such as only ETFs? Are the investment products utilized by the robo-adviser appropriate for your goals?
- Does the robo-adviser only offer certain limited portfolios within those investment products? How many different portfolios could your money possibly be invested in? What portfolio does the robo-adviser recommend for you and why?
- What type of accounts does the robo-adviser manage? For example, does the robo-adviser manage [individual retirement accounts \(IRAs\)](#)? Taxable accounts? [401\(k\) accounts](#) or [college savings plans](#)?
- How does the robo-adviser handle volatility? For example, does the robo-adviser have the ability to freeze sales (not let you sell your investments for cash for a certain period of time)?
- How often is your account rebalanced? Rebalancing can have tax implications, depending on the type of account. What would trigger a change in the asset allocation or investment categories of your portfolio?

**Tax Loss Harvesting**

Does the robo-adviser utilize tax loss harvesting? Tax loss harvesting involves selling investments that have experienced losses in your account, which may result in tax implications. The value of tax loss harvesting can depend on your particular tax situation in a given year. It also may implicate rules against [wash sales](#). Make sure you understand the tax implications of any sales, and consider whether you may wish to consult a tax adviser. For more information about wash sales, read [IRS Publication 550, Investment Income and Expenses \(Including Capital Gains and Losses\)](#).

**What Fees and Costs Will the Robo-Adviser Charge?**

[Fees and other costs](#) can greatly impact your return on investment. One of the main benefits of a robo-adviser can be lower fees and costs – so it is very important that you understand what you would be charged. A robo-adviser may offer lower-cost investment advice, but if the robo-adviser utilizes investment products with high costs, your total overall costs could still be high. It's important to understand your *total* costs.

Also, in some cases, a robo-adviser may offer services that are not significantly different from services you could obtain through a traditional investment advisory program or through investing in a product such as a [target date retirement fund](#). It is worth considering whether one product or service can offer what you need at a lower overall cost than another. Here are a few questions to consider:

- *What fees would you be charged directly by the robo-adviser? Are there any other costs (e.g., brokerage fees, management fees for ETFs purchased for your account) that you would pay directly or indirectly?*
- *How is the robo-adviser compensated? Does the way it is compensated create any conflicts of interest with you, the investor? For example, is the robo-adviser paid to offer particular products or does it offer only products with which it is affiliated (e.g., mutual funds sponsored by the robo-adviser or its affiliates)?*
- *Are there penalties or fees if you want to withdraw your investment, or transfer or close your account? Liquidating an account may have tax implications for you as well.*
- *Does the amount you are charged depend on how much money you invest?*
- *Can the costs and fees change over time?*
- *Does the robo-adviser pay a referral or marketing fee, or other incentives for finding new clients? Robo-advisers may use different marketing techniques, such as paying money to others or providing discounted fees for making client referrals. You should understand if a robo-adviser has that kind of feature, even if you are not paying a fee yourself.*

### **Licensing and Registration – How Do You Find More Information?**

Firms that provide advisory services in the U.S. are typically [registered](#) as investment advisers with either the SEC or one or more state securities authorities. Although the services that they provide are automated, robo-advisers in the U.S. must comply with the securities laws applicable to SEC or state-registered investment advisers. Use the SEC's [Investment Adviser Public Disclosure \(IAPD\)](#) database, which is available on [Investor.gov](#), to research the background, including registration or license status and disciplinary history, of any individual or firm recommending an investment. In addition, a firm that provides robo-adviser services may be affiliated with a [broker](#) that can execute the robo-adviser's recommendations by buying and selling specific securities for your account. You can research that broker using the [Investment Adviser Public Disclosure \(IAPD\)](#) database as well, which is again available on [Investor.gov](#).

Finally, like traditional investment advisers, robo-advisers are also required to file a [Form ADV](#). Robo-advisers may also offer certain information about their advisory business on their websites or in communications with clients. Check the robo-adviser's website regularly to see if there is any updated information.

### **Additional Information**

[Investor Alert: Automated Investment Tools](#)

[Ask a question or report a problem](#) concerning your investments, your investment account or a financial professional. Report [possible securities fraud](#).

Visit [Investor.gov](#), the SEC's website for individual investors.

Receive Investor Alerts and Bulletins from the Office of Investor Education and Advocacy ("OIEA") by [email](#) or [RSS feed](#). Follow OIEA on [Twitter @SEC\\_Investor\\_Ed](#). Like OIEA on [Facebook](#) at [facebook.com/secinvestoreducation](#).

The Office of Investor Education and Advocacy has provided this information as a service to investors. It is neither a legal interpretation nor a statement of SEC policy. If you have questions concerning the meaning or application of a particular law or rule, please consult with an attorney who specializes in securities law.

*Modified: March 2, 2017*

# Tab 8



# NATIONAL EXAM PROGRAM

## RISK ALERT

*By the Office of Compliance Inspections and Examinations (“OCIE”)*<sup>1</sup>

**Volume VI, Issue 5**

**August 7, 2017**

*This Risk Alert provides a summary of observations from OCIE’s examinations of registered broker-dealers, investment advisers, and investment companies conducted pursuant to the Cybersecurity Examination Initiative announced on September 15, 2015.*

## OBSERVATIONS FROM CYBERSECURITY EXAMINATIONS

### I. Introduction

In OCIE’s Cybersecurity 2 Initiative, National Examination Program staff examined 75 firms, including broker-dealers, investment advisers, and investment companies (“funds”) registered with the SEC to assess industry practices and legal and compliance issues associated with cybersecurity preparedness.<sup>2</sup> The Cybersecurity 2 Initiative built upon prior cybersecurity examinations, particularly OCIE’s 2014 Cybersecurity 1 Initiative.<sup>3</sup> However, the Cybersecurity 2 Initiative examinations involved more validation and testing of procedures and controls surrounding cybersecurity preparedness than was previously performed.

The examinations focused on the firms’ written policies and procedures regarding cybersecurity, including validating and testing that such policies and procedures were implemented and followed. In addition, the staff sought to better understand how firms managed their cybersecurity preparedness by focusing on the following areas: (1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response.

In general, the staff observed increased cybersecurity preparedness since our 2014 Cybersecurity 1 Initiative. However, the staff also observed areas where compliance and oversight could be improved. This Risk Alert provides a summary of the staff’s observations from the Cybersecurity 2 Initiative

<sup>1</sup> The views expressed herein are those of the staff of OCIE, in coordination with other staff of the Securities and Exchange Commission (“SEC” or “Commission”). The Commission has expressed no view on the contents of this Risk Alert. This document was prepared by the SEC staff and is not legal advice.

<sup>2</sup> See OCIE, [Examination Priorities for 2015](#) (January 13, 2015) and [National Exam Program Risk Alert, OCIE’s 2015 Cybersecurity Examination Initiative](#) (September 15, 2015). A few of the staff’s observations discussed herein were previously discussed in a recent [National Exam Program Risk Alert, Cybersecurity: Ransomware Alert](#) (May 17, 2017).

<sup>3</sup> See OCIE, [OCIE Cybersecurity Initiative](#) (April 15, 2014) and [National Exam Program Risk Alert, Cybersecurity Examination Sweep Summary](#) (February 3, 2015). The staff examined a different population of firms in the Cybersecurity 2 Initiative than those that were examined in the Cybersecurity 1 Initiative.

examinations and highlights certain issues observed as well as certain policies and procedures that the staff believes may be effective.<sup>4</sup>

## II. Summary of Examination Observations

Among the 75 firms examined, the staff noted an overall improvement in firms' awareness of cyber-related risks and the implementation of certain cybersecurity practices since the Cybersecurity 1 Initiative. Most notably, all broker-dealers, all funds, and nearly all advisers examined maintained cybersecurity-related written policies and procedures addressing the protection of customer/shareholder records and information. This contrasts with the staff's observations in the Cybersecurity 1 Initiative, in which comparatively fewer broker-dealers and advisers had adopted this type of written policies and procedures.

In the examinations, the staff observed:

- Nearly all broker-dealers and the vast majority of advisers and funds conducted periodic risk assessments of critical systems to identify cybersecurity threats, vulnerabilities, and the potential business consequences of a cyber incident.
- Nearly all broker-dealers and almost half of the advisers and funds conducted penetration tests and vulnerability scans on systems that the firms considered to be critical, although a number of firms did not appear to fully remediate some of the high risk observations that they discovered from these tests and scans during the review period.
- All firms utilized some form of system, utility, or tool to prevent, detect, and monitor data loss as it relates to personally identifiable information.
- All broker-dealers and nearly all advisers and funds had a process in place for ensuring regular system maintenance, including the installation of software patches to address security vulnerabilities. However, the staff observed that a few of the firms had a significant number of system patches that, according to the firms, included critical security updates that had not yet been installed.
- Information protection programs at the firms typically included relevant cyber-related topics, such as:
  - *Policies and procedures.* Nearly all firms' policies and procedures addressed cyber-related business continuity planning and Regulation S-P.<sup>5</sup> In addition, nearly all broker-dealers and

---

<sup>4</sup> The examinations were conducted between September 2015 and June 2016 and generally covered the review period October 1, 2014 through September 30, 2015.

<sup>5</sup> See 17 C.F.R. Part 248, Subpart A—[\*Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information\*](#). See also [\*Disposal of Consumer Report Information\*](#), Securities Exchange Act of 1934 ("Exchange Act") Release No. 50781, Investment Advisers Act of 1940 ("Advisers Act") Release No. 2332, Investment Company Act of 1940 ("Investment Company Act") Release No. 26685 (December 2, 2004), 69 Fed. Reg. 71321 (December 8, 2004) and [\*Privacy of Consumer Financial Information \(Regulation S-P\)\*](#), Exchange Act Release No. 42974, Investment Company Act Release No. 24543, Advisers Act Release No. 1883 (June 22, 2000), 65 Fed. Reg. 40334 (June 29, 2000).

most advisers and funds had specific cybersecurity and Regulation S-ID<sup>6</sup> policies and procedures.

- *Response plans.* Nearly all of the firms had plans for addressing access incidents. In addition, the vast majority of firms had plans for denial of service incidents and unauthorized intrusions. However, while the vast majority of broker-dealers maintained plans for data breach incidents and most had plans for notifying customers of material events, less than two-thirds of the advisers and funds appeared to maintain such plans.
- All broker-dealers and a large majority of advisers and funds maintained cybersecurity organizational charts and/or identified and described cybersecurity roles and responsibilities for the firms' workforce.
- The vast majority of broker-dealers and nearly two-thirds of the advisers and funds had authority from customers/shareholders to transfer funds to third party accounts.
  - Some of the broker-dealers did not appear to memorialize their processes into written supervisory procedures. Rather, these broker-dealers appeared to have informal practices for verifying customers' identities in order to proceed with requests to transfer funds.
  - All of the advisers and funds maintained policies, procedures, and standards related to verifying the authenticity of a customer/shareholder who was requesting to transfer funds.
- Almost all firms either conducted vendor risk assessments or required that vendors provide the firms with risk management and performance reports (i.e., internal and/or external audit reports) and security reviews or certification reports. While vendor risk assessments are typically conducted at the outset of a relationship, over half of the firms also required updating such risk assessments on at least an annual basis.

### III. Issues Observed

The staff observed one or more issues in the vast majority of the Cybersecurity 2 Initiative examinations. Highlighted below are issues the staff believes firms would benefit from considering in order to assess and improve their policies, procedures, and practices.

- While, as noted above, all broker-dealers and funds, and nearly all advisers maintained written policies and procedures addressing cyber-related protection of customer/shareholder records and information, a majority of the firms' information protection policies and procedures appeared to have issues. Examples included:
  - *Policies and procedures were not reasonably tailored* because they provided employees with only general guidance, identified limited examples of safeguards for employees to consider, were very narrowly scoped, or were vague, as they did not articulate procedures for implementing the policies.

---

<sup>6</sup> See 17 C.F.R. Part 248, Subpart C—[Regulation S-ID: Identity Theft Red Flags](#). See also [Identity Theft Red Flags Rules](#), Exchange Act Release No. 69359, Advisers Act Release No. 3582, Investment Company Act Release No. 30456 (April 10, 2013), 78 Fed. Reg. 23637 (April 19, 2013).

- *Firms did not appear to adhere to or enforce policies and procedures, or the policies and procedures did not reflect the firms' actual practices*, such as when the policies:
  - Required annual customer protection reviews; however, in practice, they were conducted less frequently.
  - Required ongoing reviews to determine whether supplemental security protocols were appropriate; however, such reviews were performed only annually, or not at all.
  - Created contradictory or confusing instructions for employees, such as policies regarding remote customer access that appeared to be inconsistent with those for investor fund transfers, making it unclear to employees whether certain activity was permissible.
  - Required all employees to complete cybersecurity awareness training; however, firms did not appear to ensure this occurred and take action concerning employees who did not complete the required training.
- The staff also observed Regulation S-P-related issues among firms that did not appear to adequately conduct system maintenance, such as the installation of software patches to address security vulnerabilities and other operational safeguards to protect customer records and information. Examples included:
  - *Stale Risk Assessments*. Using outdated operating systems that were no longer supported by security patches.
  - *Lack of Remediation Efforts*. High-risk findings from penetration tests or vulnerability scans that did not appear to be fully remediated in a timely manner.

#### **IV. Elements of Robust Policies and Procedures<sup>7</sup>**

During these examinations, the staff observed several elements that were included in the policies and procedures of firms that the staff believes had implemented robust controls. Firms may wish to consider the following elements as they could be useful in the implementation of cybersecurity-related policies and procedures.<sup>8</sup>

- *Maintenance of an inventory of data, information, and vendors*. Policies and procedures included a complete inventory of data and information, along with classifications of the risks,

---

<sup>7</sup> This is not intended to be a comprehensive list of the elements of robust cybersecurity policies and procedures. The adequacy of supervisory, compliance, and other risk management policies and procedures can be determined only with reference to the profile of each specific firm and other facts and circumstances.

<sup>8</sup> Firms may also wish to consider the guidance and information issued by the SEC's Division of Investment Management and the cybersecurity issues discussed in Commission orders in settled enforcement proceedings. See, e.g., [IM Guidance Update: Cybersecurity Guidance](#) (April 2015), [In re Morgan Stanley Smith Barney LLC](#), Exchange Act Release No. 78021, Advisers Act Release No. 4415 (June 8, 2016), [In re R.T. Jones Capital Equities Management Inc.](#), Advisers Act Release No. 4204 (September 22, 2015), and [In re Craig Scott Capital LLC](#), Exchange Act Release No. 77595 (April 12, 2016).



vulnerabilities, data, business consequences, and information regarding each service provider and vendor, if applicable.

- *Detailed cybersecurity-related instructions.* Examples included:
  - Penetration tests – policies and procedures included specific information to review the effectiveness of security solutions.
  - Security monitoring and system auditing – policies and procedures regarding the firm’s information security framework included details related to the appropriate testing methodologies.
  - Access rights – requests for access were tracked, and policies and procedures specifically addressed modification of access rights, such as for employee on-boarding, changing positions or responsibilities, or terminating employment.
  - Reporting – policies and procedures specified actions to undertake, including who to contact, if sensitive information was lost, stolen, or unintentionally disclosed/misdirected.
- *Maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities.* Examples included:
  - Vulnerability scans of core IT infrastructure were required to aid in identifying potential weaknesses in a firm’s key systems, with prioritized action items for any concerns identified.
  - Patch management policies that included, among other things, the beta testing of a patch with a small number of users and servers before deploying it across the firm, an analysis of the problem the patch was designed to fix, the potential risk in applying the patch, and the method to use in applying the patch.
- *Established and enforced controls to access data and systems.* For example, the firms:
  - Implemented detailed “acceptable use” policies that specified employees’ obligations when using the firm’s networks and equipment.
  - Required and enforced restrictions and controls for mobile devices that connected to the firms’ systems, such as passwords and software that encrypted communications.
  - Required third-party vendors to periodically provide logs of their activity on the firms’ networks.
  - Required immediate termination of access for terminated employees and very prompt (typically same day) termination of access for employees that left voluntarily.
- *Mandatory employee training.* Information security training was mandatory for all employees at on-boarding and periodically thereafter, and firms instituted policies and procedures to ensure that employees completed the mandatory training.
- *Engaged senior management.* The policies and procedures were vetted and approved by senior management.

## V. Conclusion

Cybersecurity remains one of the top compliance risks for financial firms.<sup>9</sup> As noted in OCIE's 2017 priorities, OCIE will continue to examine for cybersecurity compliance procedures and controls, including testing the implementation of those procedures and controls at firms.<sup>10</sup>

---

*This Risk Alert is intended to highlight for firms the risks and issues that the staff identified during examinations of broker-dealers, investment advisers, and investment companies regarding cybersecurity preparedness. In addition, this Risk Alert describes factors that firms may consider to (1) assess their supervisory, compliance and/or other risk management systems related to cybersecurity risks, and (2) make any changes, as may be appropriate, to address or strengthen such systems. These factors are not exhaustive, nor will they constitute a safe harbor. Factors other than those described in this Risk Alert may be appropriate to consider, and some of the factors may not be applicable to a particular firm's business. While some of the factors discussed in this Risk Alert reflect existing regulatory requirements, they are not intended to alter such requirements. Moreover, future changes in laws or regulations may supersede some of the factors or issues raised herein. The adequacy of supervisory, compliance, and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.*

---

<sup>9</sup> See, e.g., Investment Adviser Association, ACA Compliance Group, and OMAM, [2016 Investment Management Compliance Testing Survey](#) (June 23, 2016), which synthesizes 730 adviser compliance professionals' responses to 94 compliance-related questions. Q94: 88% of advisers view cybersecurity, privacy, and identity theft as the hottest compliance topic for 2016.

<sup>10</sup> OCIE, [Examination Priorities for 2017](#) (January 12, 2017).

Tab 9

**SEC Electronic Investment Advice Initiative**  
**Redacted Information Request**  
(September 2017)

**General Background**

1. For the Examination Period, a list of all employees, contractors, interns, third-party consultants, senior advisers, partners, officers and/or directors and their respective titles, group or functional area (e.g., portfolio management, trading, information technology, software development, accounting), office location, and hire date. Also provide an organization chart of each group or functional area within the Adviser illustrating the reporting structure.
2. All versions of any Terms of Use applicable to the Adviser's website/mobile application that were in effect during the Examination Period.
3. A list of any sub-advisers. If applicable, copies of agreements with such sub-advisers.
4. Names and locations of all affiliated and unaffiliated service providers and the services they perform. Include agreements underlying these arrangements. For this item, the Adviser may exclude basic clerical support services.
5. Names of all platforms used by the Adviser to provide electronic investment advice ("robo-advisory services"). For each, indicate:
  - (a) proprietary or non-proprietary (e.g., White-Label)
  - (b) accessible via website, mobile application, or both
  - (c) whether users/clients must complete a questionnaire
  - (d) whether it employs cognitive computing (e.g., artificial intelligence, machine learning)
  - (e) whether it includes human communication (e.g., financial planner)
  - (f) whether it employs gamification and, if so, for what purpose
  - (g) if non-proprietary: adviser-facing, client/user-facing, or both
  - (h) if non-proprietary: manufacturer's name
  - (i) if non-proprietary: whether the Adviser also uses turnkey services offered by the platform
6. Names of all FinTech/robo-advisory tools used by the Adviser, excluding platforms disclosed in response to Item 5 (e.g., for account aggregation, data aggregation, data analytics/business intelligence). Also include the manufacturer's name and the tool's purpose.
7. Provide the information below for all robo-advisory client accounts as of [DATE]. The preferred format for this information is in Excel.
  - (a) inception date, account number, client name and address, and market value;
  - (b) client's date of birth;
  - (c) whether the client is a related person, affiliated person, or a proprietary account;
  - (d) type of account (e.g., individual, joint, IRA, 401(k), trust);

- (e) platform used;
  - (f) account custodian and location;
  - (g) whether or not the Adviser has discretionary authority;
  - (h) whether the Adviser, an officer, an employee, or an affiliate acts as trustee, co-trustee, or successor trustee or has full power of attorney for the account;
  - (i) client risk tolerance level or code;
  - (j) current net worth and income of the client;
  - (k) account portfolio manager(s), if applicable;
  - (l) whether the client pays a performance fee; and
  - (m) for clients obtained during the Examination Period, provide name(s) of person(s) who solicited or otherwise helped to obtain the client, if any.
8. To the extent the Adviser provides robo-advisory services to accounts not included in response to Item 7, please provide for those accounts, the same information that is requested in Item 7.
9. If applicable, a list of clients that utilized the Adviser's automated platform and subsequently converted their accounts to traditional (non-automated) advised accounts at the Adviser.
10. If applicable, a list of clients that have traditional/non-automated advised accounts at the Adviser and also have one or more accounts that are managed by the Adviser's automated platform.
11. Provide the information below for all advisory clients' accounts that closed during the Examination Period. The preferred format for this information is in Excel.
- (a) inception date
  - (b) closing date
  - (c) account number
  - (d) client's name
  - (e) client's date of birth
  - (f) whether the client is a related person, affiliated person, or a proprietary account;
  - (g) type of account (e.g., individual, joint, IRA, 401(k), trust);
  - (h) platform used
  - (i) whether or not the Adviser had discretionary authority;
  - (j) client risk tolerance level or code; and
  - (k) client address.

### **Compliance Oversight**

12. All compliance policies and procedures that currently are in effect for the Adviser. In responding to this request, the Adviser also should include any procedures related to the development, testing, maintenance, and monitoring of any systems and algorithms. If material amendments were made to the policies and procedures during the Examination Period, provide details on the amendments and when they became effective. Please note that subsequent items in this Request Letter may ask for policies and procedures that are covered by the documents produced in response to this item. For those items, you may refer back to this request item and specify where the information can be found.
13. List any third-party resources used to support the Adviser's compliance function. Provide copies of any reports or reviews conducted by external compliance consultants during the Examination Period.
14. An explanation of the role of compliance in connection with the testing and monitoring of risk assessment models and investment/asset allocation algorithms. Indicate whether compliance is engaged at the onset of system design, and describe compliance's role on an ongoing basis, as well as note whether compliance has representation on any committees or design groups that are responsible for investment models or investment/allocation algorithms. In connection with this request item, provide a flow chart that illustrates the Adviser's software development lifecycle, and indicate the various points where compliance interacts with the process.
15. An organizational chart(s) illustrating any software development teams and stating the specific roles and responsibilities of the participants on such teams. In connection with this item, identify the project leaders and provide a brief description of their respective projects. List software development areas/projects that do not collaborate with the compliance department.
16. Documentation regarding any reviews conducted of the Adviser's policies and procedures, including annual and interim reports, internal control analyses, and forensic or transactional tests. As part of your response, provide any reports/documentation to evidence the Adviser's annual compliance reviews performed pursuant to Rule 206(4)-7 of the Advisers Act for the Examination Period. If included in the Adviser's annual review process, provide a copy of the most recent risk matrix evidencing the assessment and categorization of various risks identified by the compliance function. The Adviser's response also should address any corrective or remedial actions undertaken with respect to any findings.
17. A list and description of automated reports, including any exception reports, used in connection with the compliance function's monitoring of any algorithms employed in providing the Advisor's investment services.
18. A log and description of any tests conducted by the Adviser during the Examination Period to determine how systems performed or would have performed under various operating environments (e.g., periods of market volatility, high volumes of client driven activity). Include any policies and procedures that support such testing. Indicate any tests results that were escalated for further assessment.
19. A log of any instances when the Adviser suspended trading. Include any instances when the Adviser breached its internal trading thresholds/limits/parameters, established clearing firm limits, or both.
20. A list of any internal audits, including the subject and the date of each review, conducted during the Examination Period. Include a summary of each audit's scope and any related findings.
21. A list of trade errors made during the Examination Period. The Adviser's response to this item should include any trading, portfolio management or algorithmic-based errors and should briefly state how each error was made and resolved.
22. Policies and procedures addressing how compliance evaluates the suitability of specific investments or allocations relative to information provided by the client. Any compliance reviews conducted to evaluate various criteria used by the Adviser in its selection of specific securities/investment products. Any exception reports used by the Adviser to track drift in actual investment allocations from expected allocations **relative** to an account's assigned risk score.

23. Any policies and procedures (e.g., compliance manual, standard operating procedures) that address the Adviser's use of social media. Indicate whether such policies/procedures address the activities of existing clients to the extent that the Adviser has incentivized such clients to attract new clients.
24. Indicate whether the Adviser or any of its affiliates or supervised persons has access to the logins and/or passwords of any of its clients' or prospective clients' ("users") brokerage accounts or other financial accounts, or had access to such information at any time during the client onboarding process. If so, provide a list of such accounts, as well as any policies and procedures and supporting internal controls relating to this practice.
25. A list of client and user complaints received during the Examination Period. Also, the Adviser's operating definition of a client and/or user complaint, as well as any supporting policies and procedures governing the receipt, monitoring and disposition of client/user correspondence and/or complaints.
26. Any correspondence with the staff of the Commission or other regulatory agencies, including foreign agencies/governments.

### **Portfolio Management and Brokerage Practices**

27. A list of any proprietary securities or products of affiliates that are or were used or recommended by the Adviser in connection with its investment advisory services. Also, indicate the amount of compensation received by the Adviser and/or affiliates in connection with the use of these securities and products. Provide copies of any agreements related to these arrangements.
28. A list of any investment products or services offered by an unaffiliated entity that are or were used or recommended by the Adviser and for which the Adviser receives or received compensation other than its advisory fee, whether directly or indirectly. Describe the investment product and nature of the compensation. Also, provide copies of any written agreements relating to these arrangements.
29. A list of investment portfolio model(s) offered by the Adviser. For each model, include a description of the model relating to the strategy employed, the type and number of securities included, the general range of asset class/security weightings, the risk level assigned to the model, and any other significant characteristics that distinguish the model. If applicable, indicate the index against which the model is benchmarked.
30. For each of the investment strategies/portfolio models offered by the Adviser, provide copies of any research or analysis performed by the Adviser in order to determine the type of client (as defined by factors such as risk tolerance and investment objective) that is best suited for it.
31. A list of the data fields that must be completed during the onboarding process to become an advisory client. Specifically, identify any data fields that are used to assess and determine client risk tolerances, financial goals/objectives, and the initial investment recommendation. If amendments were made to such data fields during the Examination Period, describe the changes and indicate when they became effective and the extent to which compliance was involved in the process. If applicable, identify the data fields that provide clients with the option to select from pre-populated responses, and list those responses accordingly.
32. A copy of the model/formula used to determine the risk rating/tolerance for each client account.
33. Indicate whether clients are permitted to transfer into their accounts shares of securities that they currently own and/or whether they may impose account restrictions, including those related to the selection of recommended investment products. If applicable, indicate the types of transfers and/or restrictions that are permitted.
34. A list of the data fields that a client may update (once onboarded) that could result in changes to client risk tolerances, financial goals, and/or investment recommendations. Also, indicate how frequently clients are able to make such changes, how the Adviser is made aware of any such changes, when any changes would become effective/be implemented, and whether the Adviser may prompt clients to initiate these updates. If

the Adviser may prompt clients to initiate updates, indicate the general frequency of such prompts (e.g., ad hoc, based on client-specific events, periodically, annually). In connection with monitoring a client's objective, include any procedures of the Adviser that address stale or incomplete account information.

35. In addition to client data referenced above, list or identify any non-client specific key assumptions and/or factors that are included in the Adviser's investment model(s) for the purpose of determining client risk tolerances, financial goals, and investment recommendations (e.g., short or long term interest rates, relevant index returns, income tax rates).
36. A list of any data fields used in generating exception reports designed to identify circumstances when data fields completed by clients/users may be inconsistent with one another or a specific model selection (e.g., client/user indicates a low risk tolerance with an aggressive investment strategy). Indicate whether these exceptions are communicated to the client/user automatically through the Adviser's system (e.g., via an alert, confirm, or prompt box; an email; a text message), or if advisory personnel are prompted to evaluate and initiate corrective action.
37. If not already provided in response to an earlier item, a list and sample copies of any reports, including exception reports, used to review client portfolios for consistency with portfolio investment restrictions and objectives, risk tolerances, and investment model parameters.
38. If not already provided in response to an earlier item, a list and sample copies of any reports, including exception reports that the Adviser generates to evaluate the adequacy of its investment models or to otherwise ensure that the models are functioning in a manner consistent with representations made to clients/users.
39. A list of online questions users/clients must answer so that the Adviser can make its initial and/or on-going suitability assessment(s). If only a subset of the questions that users/clients are asked to answer is required to make such assessments, also provide a list of all questions posed to users/clients.
40. Sample copies of user/client reports and/or output screens generated for each step of the investment process. This item should include, for example, reports/screens pertaining to client risk tolerances, financial goal/objectives, investment recommendations, portfolio transactions, portfolio holdings including asset allocation, performance returns, and client billing, among others. Specify the frequency with which these are provided to clients. During fieldwork, the staff may request a demonstration of and/or "experiential access" to the user/client interface supporting these processes (i.e., website and/or mobile application).
41. With respect to the platform(s) employed by the Adviser for assessing user/client risk and implementing and managing a client's investment program, briefly describe any production code changes effected during the Examination Period for risk modeling and portfolio management (e.g., rebalancing, tax loss harvesting, target allocation weights).
42. Copies of any policies and procedures in effect during the Examination Period relating to the Adviser's use of a tax loss harvesting strategy.
43. Copies of any policies and procedures in effect during the Examination Period relating to the rebalancing of client portfolios, including the frequency of and factors that may trigger it.
44. Copies of any policies and procedures, scripts and/or talking points in effect during the Examination Period that pertain to client communications by advisory or client servicing personnel regarding the management of accounts. This request item relates to communications by phone, email, instant messaging, chats, etc.
45. Copies of any specific policies and procedures that address steps taken in the event of various types of market dislocations/events (e.g., Brexit, Flash Crash, Prevailing SRO Circuit Breakers and Trading Halts). Include any protocols that outline instances where the Adviser would suspend trading on behalf of client accounts, as well as how such suspension would be communicated to clients. This response should address any gates imposed by the Adviser that could impact a client's ability to effect withdrawals from or



liquidations of his/her account(s). If any suspensions have ever occurred, provide details regarding each such suspension.

46. Description of methodologies and systems used to calculate account performance and how such performance is communicated to the client.
47. Describe how clients are notified of any wash sales or capital losses in their accounts.
48. A list of any wrap-fee platforms used or sponsored by the Adviser. If applicable, provide any agreements and disclosure documents relating to these programs.

### **Marketing & Advertising**

49. A list of all advertising mechanisms (e.g., websites, mobile applications, podcasts, search engine advertisements, mainstream media) used to solicit or inform users or clients, including blogs and social media sites (e.g., Facebook, Twitter, LinkedIn). If applicable, describe any compensation arrangements with third-parties.
50. List and describe any marketing programs in place that compensate individuals or entities for client referrals. The Adviser's response should address, among other items, programs that compensate: (a) clients or users with gifts, products, or fee discounts; (b) solicitors, as defined by the cash solicitation rule under the Advisers Act; and (c) bloggers or other entities, whether or not pursuant to an affiliate marketing or co-registration program.
51. If not available on the Adviser's website/mobile application, all pitch books, pamphlets, brochures, videos and any other promotional and/or marketing materials furnished to clients and/or users regarding the Adviser's robo-advisory services.
52. If the Adviser's website/mobile application includes a section for users, clients, investors, or advisory representatives that only is accessible with a username and password, please establish a temporary username and password for the staff's use during the examination and include them with your response.

### **Cybersecurity**

53. A copy of the Adviser's policies and procedures addressing the protection of customer/client/user records and information, including those that are designed to secure customer/client/user documents and information; protect against anticipated threats to customer/client/user information; and protect against unauthorized access to customer/client/user accounts or information for the Examination Period. Please note that subsequent items in this Request Letter may ask for policies and procedures that are covered by the documents produced in response to this item. For those items, you may refer back to this request item and specify where the information can be found.
54. A copy of the Adviser's policies, procedures, and standards that are designed to ensure that unauthorized persons do not access the Adviser's network resources and devices or to restrict access according to job functions (e.g., access control policy, acceptable use policy, administrative management of systems, corporate information security policy). If applicable, provide a copy of the Adviser's last internal audit that covered access rights and controls.
55. A copy of the Adviser's policies, procedures, and standards related to login attempts, failures, lockouts, and unlocks or resets for each perimeter-facing system. Please indicate how these policies are enforced.
56. A list of any instances during the Examination Period when system users had access to systems in contravention of the Adviser's policies or practices (e.g., employees changing roles within or leaving the Adviser). Please include the date(s) and a brief description of the instance(s) and any remediation efforts undertaken in response.

57. A copy of the Adviser's policies, procedures, and standards related to verification of the authenticity of a customer/client request to transfer funds externally. If no such written policies, procedures, or standards exist, describe the process the Adviser follows to verify the authenticity of fund transfer requests and list the individuals and/or departments involved in the approval process.
58. A list of all third-party vendors that facilitated the mitigation of cybersecurity risks by means related to access controls, data loss prevention, and management of Personally Identifiable Information ("PII") during the Examination Period. Include a brief description of the services each vendor provided to the Adviser.
59. A copy of the Adviser's policies, procedures, and standards relating to the selection and supervision of third-party vendors, including protocols ensuring that such vendors only have access to those systems specified in any governing agreement.
60. A copy of the Adviser's written business continuity of operations plan that addresses mitigation of the effects of a cybersecurity incident and/or recovery from such an incident, if such a plan exists. If the Adviser maintains a separate written cybersecurity incident response policy, provide a copy of the policy and indicate the date it most recently was updated.
61. A list of all cyber incidents. Identify the amount of actual client losses associated with each cyber incident, including the amount reimbursed by the Adviser.

**In addition to the documents noted above, please have the following documents available for review at the onset of the fieldwork portion of the examination:**

62. A list of all cybersecurity assessments conducted during the Examination Period, including penetration testing and vulnerability scans, conducted by the Adviser or on behalf of the Adviser by third-parties. Also provide a copy of the results of the most recent tests and scans.
63. Separate lists of the systems or applications for which the Adviser uses or does not use multi-factor authentication for employee and customer/client access. Provide any policies and procedures that address the Adviser's deployment and management of multi-factor authentication processes.
64. A copy of the Adviser's policies and procedures related to enterprise data loss prevention. Also, provide a list of the systems, utilities, and tools used to prevent, detect, and monitor data loss as it relates to PII and access to customer/client accounts. Indicate whether the systems are proprietary, managed by a third party, or commercial off-the-shelf products.
65. A copy of the Adviser's policies and procedures relating to monitoring data exfiltration (i.e., unauthorized copying/transfer/distribution/retrieval of sensitive information), including PII, either internally or externally through email, physical media, hard copy, web-based file transfer programs, or via other electronic means. If the Adviser maintains documentation of this monitoring, include a copy of the most recent report. Also, include any policies that address how these incidents are reported internally or externally.
66. A list of all third-party vendors with access to the Adviser's network or data. Include a brief description of the service (or type of service) the vendor provides to the Adviser.

Tab 10



*October 18, 2017*

**Consumer Protection Principles:**  
**Consumer-Authorized Financial Data Sharing and Aggregation**

In the Dodd-Frank Act, Congress instructed the Bureau to implement and enforce consumer financial law “for the purpose of ensuring that all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive.”<sup>1</sup> Congress further instructed the Bureau to exercise its authorities so that “markets for consumer financial products and services operate transparently and efficiently to facilitate access and innovation.”<sup>2</sup>

For some time, a range of companies—many of them “fintech” companies—have been accessing consumer account data with consumers’ authorization and providing services to consumers using data from the consumers’ various financial accounts. Such “data aggregation”-based services include the provision of financial advice or financial management tools, the verification of accounts and transactions, the facilitation of underwriting or fraud-screening, and a range of other functions. This type of consumer-authorized data access and aggregation holds the promise of improved and innovative consumer financial products and services, enhanced control for consumers over their financial lives, and increased competition in the provision of financial services to consumers.

There are many significant consumer protection challenges to be considered—particularly with respect to data privacy and security—as these technologies and practices continue to develop. In part through a November 2016 public Request for Information, the Bureau is aware that a range of industry stakeholders are working, through a variety of individual arrangements as well as broader industry initiatives, on agreements, systems, and standards for data access, aggregation, use, redistribution, and disposal. The Bureau believes that consumer interests must be the priority of all stakeholders as the aggregation services-related market develops. A common understanding of consumer interests is essential so that effective consumer protections can be integrated consistently into this market.

As a result, the Bureau today is releasing a set of Consumer Protection Principles intended to reiterate the importance of consumer interests to all stakeholders in the developing market for services based on the consumer-authorized use of financial data. The Principles express the Bureau’s vision for realizing a robust, safe, and workable data aggregation market that gives consumers protection, usefulness, and value.

---

<sup>1</sup> 12 U.S.C. 5511(a).

<sup>2</sup> 12 U.S.C. 5511(b)(5).

The Bureau recognizes that many consumer protections apply to this market under existing statutes and regulations. These Principles are not intended to alter, interpret, or otherwise provide guidance on—although they may accord with—the scope of those existing protections. Thus, the Principles do not themselves establish binding requirements or obligations relevant to the Bureau’s exercise of its rulemaking, supervisory, or enforcement authority. In addition, the Principles are not intended as a statement of the Bureau’s future enforcement or supervisory priorities.

The Bureau will continue to monitor closely developments in this market. The Bureau will also continue to assess how the Principles set forth below may best be realized in the design and delivery of consumer financial products and services. The Bureau stands ready to facilitate constructive efforts or to take other appropriate action to protect consumers.

**Consumer Protection Principles:**  
**Consumer-Authorized Financial Data Sharing and Aggregation**

*Consumer-authorized access and use of consumer financial account data may enable the development of innovative and improved financial products and services, increase competition in financial markets, and empower consumers to take greater control of their financial lives. To accomplish these objectives, however, such access and use must be designed and implemented to serve and protect consumers. The Bureau intends for the following Consumer Protection Principles to help safeguard consumer interests as the consumer-authorized aggregation services market develops. The Principles are intended to be read together. They are not intended to alter, interpret, or otherwise provide guidance on—although they may accord with—existing statutes and regulations that apply in this market.*

**1) Access**

Consumers are able, upon request, to obtain information about their ownership or use of a financial product or service from their product or service provider. Such information is made available in a timely manner. Consumers are generally able to authorize trusted third parties to obtain such information from account providers to use on behalf of consumers, for consumer benefit, and in a safe manner.

Financial account agreements and terms support safe, consumer-authorized access, promote consumer interests, and do not seek to deter consumers from accessing or granting access to their account information. Access does not require consumers to share their account credentials with third parties.

**2) Data Scope and Usability**

Financial data subject to consumer and consumer-authorized access may include any transaction, series of transactions, or other aspect of consumer usage; the terms of any account, such as a fee schedule; realized consumer costs, such as fees or interest paid; and realized consumer benefits, such as interest earned or rewards. Information is made available in forms that are readily usable by consumers and consumer-authorized third parties. Third parties with authorized access only access the data necessary to provide the product(s) or service(s) selected by the consumer and only maintain such data as long as necessary.

**3) Control and Informed Consent**

Consumers can enhance their financial lives when they control information regarding their accounts or use of financial services. Authorized terms of access, storage, use, and disposal are fully and effectively disclosed to the consumer, understood by the consumer, not overly broad, and consistent with the consumer's reasonable expectations in light of the product(s) or service(s) selected by the consumer. Terms of data access include access frequency, data scope, and retention period. Consumers are not coerced into granting third-party access. Consumers understand data sharing revocation terms and can readily and simply revoke authorizations to access, use, or store data. Revocations are implemented by providers in a timely and effective manner, and at the discretion of the consumer, provide for third parties to delete personally identifiable information.

4) **Authorizing Payments**

Authorized data access, in and of itself, is not payment authorization. Product or service providers that access information and initiate payments obtain separate and distinct consumer authorizations for these separate activities. Providers that access information and initiate payments may reasonably require consumers to supply both forms of authorization to obtain services.

5) **Security**

Consumer data are accessed, stored, used, and distributed securely. Consumer data are maintained in a manner and in formats that deter and protect against security breaches and prevent harm to consumers. Access credentials are similarly secured. All parties that access, store, transmit, or dispose of data use strong protections and effective processes to mitigate the risks of, detect, promptly respond to, and resolve and remedy data breaches, transmission errors, unauthorized access, and fraud, and transmit data only to third parties that also have such protections and processes. Security practices adapt effectively to new threats.

6) **Access Transparency**

Consumers are informed of, or can readily ascertain, which third parties that they have authorized are accessing or using information regarding the consumers' accounts or other consumer use of financial services. The identity and security of each such party, the data they access, their use of such data, and the frequency at which they access the data is reasonably ascertainable to the consumer throughout the period that the data are accessed, used, or stored.

7) **Accuracy**

Consumers can expect the data they access or authorize others to access or use to be accurate and current. Consumers have reasonable means to dispute and resolve data inaccuracies, regardless of how or where inaccuracies arise.

8) **Ability to Dispute and Resolve Unauthorized Access**

Consumers have reasonable and practical means to dispute and resolve instances of unauthorized access and data sharing, unauthorized payments conducted in connection with or as a result of either authorized or unauthorized data sharing access, and failures to comply with other obligations, including the terms of consumer authorizations. Consumers are not required to identify the party or parties who gained or enabled unauthorized access to receive appropriate remediation. Parties responsible for unauthorized access are held accountable for the consequences of such access.

9) **Efficient and Effective Accountability Mechanisms**

The goals and incentives of parties that grant access to, access, use, store, redistribute, and dispose of consumer data align to enable safe consumer access and deter misuse. Commercial participants are accountable for the risks, harms, and costs they introduce to consumers. Commercial participants are likewise incentivized and empowered effectively to prevent, detect, and resolve unauthorized access and data sharing, unauthorized payments conducted in connection with or as a result of either authorized or unauthorized

data sharing access, data inaccuracies, insecurity of data, and failures to comply with other obligations, including the terms of consumer authorizations.



Tab 11

U.S. SECURITIES AND EXCHANGE COMMISSION

# 2018 NATIONAL EXAM PROGRAM EXAMINATION PRIORITIES

Office of Compliance  
Inspections and Examinations

**Disclaimer**

This document was prepared by SEC staff, and the views expressed herein are those of OCIE. The Commission has expressed no view on this document's contents. It is not legal advice; it is not intended to, and does not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal.

# CONTENTS

<b>Message from OCIE's Leadership Team .....</b>	<b>1</b>
<b>Introduction .....</b>	<b>4</b>
<b>Retail Investors, Including Seniors and Those Saving for Retirement.....</b>	<b>4</b>
Disclosure of the Costs of Investing .....	4
Electronic Investment Advice .....	5
Wrap Fee Programs .....	5
Never-Before-Examined Investment Advisers .....	5
Senior Investors and Retirement Accounts and Products .....	6
Mutual Funds and Exchange Traded Funds (ETFs) .....	6
Municipal Advisors and Underwriters .....	6
Fixed Income Order Execution .....	7
Cryptocurrency, Initial Coin Offerings (ICOs), Secondary Market Trading, and Blockchain.....	7
<b>Compliance and Risks in Critical Market Infrastructure .....</b>	<b>7</b>
Clearing Agencies .....	7
National Securities Exchanges .....	8
Transfer Agents .....	8
Regulation Systems Compliance and Integrity (SCI) Entities.....	8
<b>Focus on FINRA and MSRB.....</b>	<b>9</b>
FINRA.....	9
MSRB .....	9
<b>Cybersecurity.....</b>	<b>9</b>
<b>Anti-Money Laundering Programs.....</b>	<b>10</b>
<b>Conclusion .....</b>	<b>10</b>



## MESSAGE FROM OCIE'S LEADERSHIP TEAM

It is our privilege to share with you the 2018 examination priorities of the Office of Compliance Inspections and Examinations (OCIE) of the U.S. Securities and Exchange Commission (SEC or Commission).

This year we will continue to prioritize our commitment to protect retail investors, including seniors and those saving for retirement. We will especially be looking closely at products and services offered to retail investors, as well as the disclosures they receive about those investments. We intend to do this by conducting examinations targeting circumstances in which retail investors may have been harmed and reviewing whether financial service professionals have met their legal obligations.

Compliance with the securities laws overseen by the SEC has helped make our markets the safest and most vibrant in the world. Our National Exam Program (NEP) fosters compliance and helps fulfill the SEC's mission of protecting investors, maintaining fair, orderly and efficient markets, and facilitating capital formation. We do this through a variety of risk-focused strategies, including conducting compliance examinations of entities regulated by the SEC, publishing Risk Alerts, holding outreach events, and speaking to investors and market participants.

Our work stands on four “pillars”: promoting compliance, preventing fraud, identifying and monitoring risk, and informing policy. This is the sixth year we have published our examination priorities. It is our hope that this publication provides transparency into our thinking on issues and areas that we believe constitute an appropriate focus for us in the upcoming year and which entail the most effective use of examination resources in fulfilling our mission.

### DID YOU KNOW?

Our work stands on four “pillars”: promoting compliance, preventing fraud, identifying and monitoring risk, and informing policy.

Determining our priorities is a collaborative effort. We consult with our examination staff, as well as key constituencies outside the program. OCIE examiners are in discussions daily with financial professionals, market participants, compliance professionals, accountants, and attorneys regarding new products, recent trends, compliance challenges, and high risk areas. In addition, examiners see firsthand how firms are, or are not, complying with the federal securities laws. As a result, examiners are uniquely positioned to identify the practices, products, and services that may pose significant risk to investors or the financial markets.

In formulating priorities, we also seek the advice of the Chairman and Commissioners, staff from other SEC Divisions and Offices, the SEC's Investor Advocate, and our fellow regulators. Throughout the year we will add priorities—beyond those published here—as we identify emerging risks and trends and respond to tips, complaints, and referrals. Our regional offices also initiate exams based on their local assessment of risk and knowledge of their registrant population.

In executing on these priorities, we abide by the following principles:

**Principle 1: We are risk-based.**

The sheer size and continued growth of the securities industry prevents us from conducting regular comprehensive examinations of each registered firm. In order to effectively oversee all of the varying market participants within our jurisdiction, and given our limited resources, we utilize a risk-based strategy. A central part of this effort is ongoing analysis of root causes of harm to investors and markets and the identification of the greatest risks. The analysis flows into a number of aspects of our program, including our process for setting priorities, the criteria we use to select potential examination candidates, and determining the appropriate scope of our exams, as well as resource allocation more generally. We recognize that the choices we make in this regard imply foregone attention on other areas and firms, but such hard decisions are necessary in order to maximize our impact.

**Principle 2: We are data-driven.**

Our use of data is integral to the program and complements our risk-based exam approach and utilization of technology. We use data in areas such as risk assessment and exam scoping, planning, and execution. For example, we are rapidly advancing in our capacity to use data to analyze regulatory filings and trading activity. Among other things, this has included development by our Quantitative Analytics Unit (QAU) of the National Exam Analytics Tool (NEAT) to facilitate the analysis of trading blotters. The QAU is comprised of financial engineers who, in addition to developing tools, directly assist exam teams with quantitative analysis. Our sophistication in using data analytics to identify potential non-compliance with the securities laws, including possible fraudulent behavior, is ever growing. We also use data to better identify high-risk exam candidates and to more efficiently analyze information during examinations. We continuously look for ways to employ technology and data analytics to enhance our effectiveness in every aspect of the examination program.

**Principle 3: We are transparent.**

Transparency is an important tool for us. We believe that publicly sharing certain information about our examination program—particularly our priorities, common findings, and what we believe to be the highest risk areas—will ultimately benefit investors by assisting the work of legal, compliance, and risk staff at registered entities as they work within their organizations to achieve compliance with the securities laws. To this end, we have been publishing more information about what we are doing, why we are doing it, and what we have found and learned in the process.

**DID YOU KNOW?**

The NEP published six Risk Alerts to the industry in FY 2017.

Risk Alerts, in particular, have become a valuable tool, and we have made a concerted effort to publish them more frequently. The ultimate goal of these Risk Alerts is to promote compliance. Recent topics in our Risk Alerts include the most frequently-cited deficiencies from various examination initiatives, as well as observations

of industry practices and compliance issues from cybersecurity examinations. We believe sharing this information helps registered firms—particularly those that have not been examined recently—sharpen their identification and correction of deficient practices, maximizing the impact of the examination program and resulting in better protection for investors.

**Principle 4: We strive to put our resources to their highest and best use.**

We rely heavily on our talented and experienced staff, many of whom are subject matter experts in key risk areas. We also increasingly leverage technology and data in our risk assessment and examination processes. Resources, however, are limited. We continually assess our resource deployment and ask: Are we using our resources in way that maximizes the benefit to investors? The decisions we make come with tradeoffs, but top of mind is always effectively advancing investor protection and fulfilling the SEC's mission.

**DID YOU KNOW?**

In Fiscal Year 2017, the National Exam Program completed over 2,870 examinations—representing an 18 percent increase over FY 2016.

**Principle 5: We embrace innovation and new technology, both as a means to do more with less and as a necessary focal point of our analytic efforts.**

We recognize that technology in the financial markets often spurs innovation in ways that are beneficial to investors. It has the potential, for example, to help drive down costs to investors and provide new ways for people to access our financial markets, investment information, and financial advice. Where technological advances lead to new business models, we seek to assess their potential impact on the financial markets, identify ways investors may be harmed, if any, and work with our colleagues to share critical observations that may assist the Commission in adapting to emerging risks and concerns. We also seek to keep pace with advancing technology, to monitor for cybersecurity risks, to engage with industry in efforts to help combat cybersecurity attacks, and to prevent investor harm.

We hope you find publication of our examination priorities valuable in your efforts to promote compliance and protect investors. Please know also that we are always interested in hearing more about new and emerging risk areas and products as well as how OCIE can be more effective in its mission. Our contact information can be found at: <https://www.sec.gov/contact-information/sec-directory>.



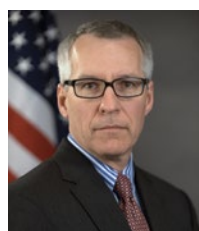
**Peter B. Driscoll**  
Director



**Jane E. Jarcho**  
Deputy Director and  
Co-National Investment  
Adviser/Investment  
Company Director



**Keith E. Cassidy**  
National Technology  
Controls Program  
Director



**Kevin W. Goodman**  
National FINRA and  
Securities Industry  
Oversight Director



**Daniel R. Gregus**  
Acting Clearing Agency  
Director



**Daniel S. Kahl**  
Chief Counsel



**John S. Polise**  
National Broker Dealer  
and Exchange Director



**James R. Reese**  
Acting Chief Risk Officer



**Kristin A. Snyder**  
Co-National Investment  
Adviser/Investment  
Company Director



## INTRODUCTION

This document presents OCIE’s 2018 examination priorities.<sup>1</sup> In general, the priorities reflect certain practices, products, and services that OCIE believes may present potentially heightened risk to investors and/or the integrity of the U.S. capital markets. Our 2018 priorities are organized around five themes:

1. Matters of importance to retail investors, including seniors and those saving for retirement;
2. Compliance and risks in critical market infrastructure;
3. Financial Industry Regulatory Authority (FINRA) and Municipal Securities Rulemaking Board (MSRB);
4. Cybersecurity; and
5. Anti-Money laundering programs.

### DID YOU KNOW?

In FY 2017, the NEP held four regional investment adviser/investment company compliance outreach programs, a national broker-dealer compliance outreach program and participated in hundreds of other outreach events in order to promote and improve industry compliance.

While we believe these areas are critical, this list is not comprehensive; OCIE remains flexible in order to cover emerging and exigent risks to investors and the marketplace as they arise. Rapid institutional and technological change in the market landscape demands a responsive approach. While the change is fast and perhaps accelerating, we keep both our analytic efforts and our examinations firmly grounded in our four pillars: promoting compliance, preventing fraud, identifying and monitoring risk, and informing policy.

## RETAIL INVESTORS, INCLUDING SENIORS AND THOSE SAVING FOR RETIREMENT

The protection of retail investors is embedded in the SEC’s mission and likewise in OCIE’s organizational culture. This year, we will continue to prioritize protecting retail investors, particularly seniors and those saving for retirement, and pursue examinations of firms that provide products and services directly to them. We will also focus on higher risk products as well as recent technological changes in how investment advice is delivered. We will particularly focus on the following areas:

### Disclosure of the Costs of Investing

When a retail investor hires a financial professional, some of the most important information they receive relates to the fees charged and other compensation the financial professional may receive, such as compensation from transactions involving affiliates of the financial professional. Every dollar an investor pays in fees and expenses is a dollar not invested for his or her benefit. Therefore, the proper disclosure and calculation of fees, expenses, and other charges investors pay is critically important. It is also important for financial professionals to inform investors of any

<sup>1</sup> This document was prepared by SEC staff, and the views expressed herein are those of OCIE. The Commission has expressed no view on this document’s contents. It is not legal advice; it is not intended to, and does not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal.

conflicts of interest that might provide incentives for the financial professionals to recommend certain types of products or services to investors, including any higher cost or riskier products. Examiners will review, among other things, whether fees and expenses are calculated and charged in accordance with the disclosures provided to investors. Examiners will also review fees charged to advisory accounts, particularly where the fee is dependent on the value of the account, to assess whether assets are valued in accordance with investor agreements, disclosures, and the firm's policies and procedures.

We will also focus on firms that have practices or business models that may create increased risks that investors will pay inadequately disclosed fees, expenses, or other charges. These practices or business models include:

- certain advisory personnel that may receive financial incentives to recommend that investors invest, or remain invested, in particular share classes of mutual funds where the investors may pay higher sales loads or distribution fees and the conflict of interest may not be disclosed to investors;
- accounts where investment advisory representatives have departed from the firms, and the accounts have not been assigned a new representative to properly oversee them;
- advisers that changed the manner in which fees are charged from a commission on executed trades to a percentage of client assets under management; and
- private fund advisers that manage funds with a high concentration of investors investing for the benefit of retail clients, including non-profit organizations and pension plans.

### **Electronic Investment Advice**

We will continue to examine investment advisers and broker-dealers that offer investment advice through automated or digital platforms. This includes “robo-advisers” and other firms that interact primarily with clients online. Examinations will focus on registrants' compliance programs, including the oversight of computer program algorithms that generate recommendations, marketing materials, investor data protection, and disclosure of conflicts of interest.

### **Wrap Fee Programs**

We will continue to examine registered investment advisers and broker-dealers associated with wrap fee programs, which charge investors a single bundled (wrapped) fee based on a percentage of assets for investment advisory and brokerage services. We will review whether investment advisers are acting in a manner consistent with their fiduciary duty and whether they are meeting their contractual obligations to clients. Areas of interest will include whether (i) the recommendations to invest in a wrap fee program and to continue in the program are reasonable, (ii) conflicts of interests are disclosed in compliance with applicable regulatory requirements, and (iii) investment advisers are obtaining best execution and disclosing costs associated with executing trades through another broker-dealer.

### **Never-Before-Examined Investment Advisers**

Given the percentage of investment advisers that are either newly registered or that have not been examined in some time, we will continue to make risk-based assessments and select those investment advisers for examination that have elevated risk profiles.

#### **DID YOU KNOW?**

In FY 2017, the SEC achieved examination coverage of approximately 15 percent of all investment advisers, up from 8 percent just five years ago.

## Senior Investors and Retirement Accounts and Products

Seniors and those saving for retirement are increasingly reliant on returns from their investments. We will review how broker-dealers oversee their interactions with senior investors, including the ability of firms to identify financial exploitation of seniors. We will also focus on internal controls at firms designed to supervise their representatives, particularly relating to sales of products and services directed at senior investors.

### DID YOU KNOW?

The NEP completed more than 2,100 exams of investment advisers in FY 2017, which is an increase of approximately 46 percent over FY 2016.

We will continue to conduct examinations of investment advisers and broker-dealers that offer services and products to investors with retirement accounts. These examinations will focus on, among other things, investment recommendations, sales of variable insurance products, and sales and management of target date funds. In addition, we will examine investment adviser and broker-dealer facilitation and involvement in retirement vehicles that primarily serve state and local government employees and non-profit employees, including 403(b) and 457 plans.

## Mutual Funds and Exchange Traded Funds (ETFs)

Mutual funds and ETFs are the primary investment vehicles for many retail investors. We will focus on mutual funds (i) that have experienced poor performance or liquidity in terms of their subscriptions and redemptions relative to their peer groups, (ii) that are managed by advisers with little experience managing registered investment companies, or (iii) that hold securities which are potentially difficult to value during times of market stress, including securitized auto, student, or consumer loans, or collateralized mortgage-backed securities. We will also focus on ETFs and mutual funds that seek to track custom-built indexes to review for any conflicts the adviser may have with the index provider and the adviser's role with respect to the selection and weighting of index components.

With respect to ETFs, our focus will be on funds that have little secondary market trading volume and that face the risk of being delisted from an exchange and having to liquidate assets. When this happens, the value of the ETF has the potential to rapidly decline and investors may pay the cost to liquidate the funds' assets. The focus of these examinations will include analyzing whether investment risks are adequately disclosed to investors.

## Municipal Advisors and Underwriters

Municipal advisors provide advice to, or on behalf of, a municipal entity or obligated person about the issuance of bonds and other financial products. We will continue to examine municipal advisors to evaluate their compliance with registration, recordkeeping, and supervision requirements, particularly those municipal advisors that are not registered as broker-dealers. Examinations will also review for compliance with MSRB rules regarding professional qualification requirements, continuing education requirements, and core standards of conduct and duties of municipal advisors when engaging in municipal advisory activities.

State and local governments and other municipal entities often rely on broker-dealer and municipal advisors, among other financial professionals, to raise money for essential infrastructure such as hospitals, schools, and utilities through the issuance of fixed income securities. We will continue to examine municipal underwriters for their compliance with MSRB and SEC rules.

### **Fixed Income Order Execution**

One of the key investor protection requirements in the fixed income secondary market is the best execution of customer orders. We will conduct examinations to assess whether broker-dealers have implemented best execution policies and procedures, consistent with regulatory requirements, for both municipal bond and corporate bond transactions.

### **Cryptocurrency, Initial Coin Offerings (ICOs), Secondary Market Trading, and Blockchain**

The cryptocurrency and ICO markets have grown rapidly and present a number of risks for retail investors. Along with the growth of these products and markets, the number of broker-dealers and investment advisers engaged in this space continues to grow as well. We will continue to monitor the sale of these products, and where the products are securities, examine for regulatory compliance. Areas of focus will include, among other things, whether financial professionals maintain adequate controls and safeguards to protect these assets from theft or misappropriation, and whether financial professionals are providing investors with disclosure about the risks associated with these investments, including the risk of investment losses, liquidity risks, price volatility, and potential fraud.

## **COMPLIANCE AND RISKS IN CRITICAL MARKET INFRASTRUCTURE**

### **Clearing Agencies**

Clearing agencies perform a variety of services that help ensure that trades settle on time and at the agreed upon terms. For example, clearing agencies compare transaction information, calculate settlement obligations, collect margin, and may serve as a depository to hold securities as certificates or in electronic form to facilitate automated settlement. We will continue to conduct annual examinations of clearing agencies that the Financial Stability Oversight Council has designated as systemically important and for which the Commission is the supervisory agency. Examinations will focus on compliance with the Commission's Standards for Covered Clearing Agencies,<sup>2</sup> whether clearing agencies have taken timely corrective action in response to prior examinations, and other areas identified in collaboration with our colleagues in the Division of Trading and Markets and with other regulators, as applicable.

#### **DID YOU KNOW?**

Clearing agencies perform a variety of services that help ensure that trades settle on time and at the agreed upon terms.

<sup>2</sup> See Standards for Covered Clearing Agencies, Release No. 34-78961 (adopted Sept. 28, 2016), <https://www.sec.gov/rules/final/2016/34-78961.pdf> (compliance date April 11, 2017).

## National Securities Exchanges

With over 20 national securities exchanges facilitating transactions in the marketplace, OCIE will focus on, among other things, the internal audits conducted by the exchanges, the fees paid under Exchange Act Section 31, and the governance and operation of certain National Market System (NMS) plans. Specific to NMS plans, OCIE, in coordination with our colleagues in the Division of Trading and Markets, will conduct examinations of the equities and options consolidated market data plans, with a focus on governance, revenue and expense generation, and revenue and expense allocation procedures.

## Transfer Agents

Transfer agents stand between the companies that issue securities and the individuals and entities that own those securities and perform four main functions: (i) track, record, and maintain an issuer's security holder records, (ii) cancel and issue certificates, (iii) facilitate communications between issuers and security holders, and (iv) make distributions to security holders. Efficient transfer agent operations are critical to secondary securities markets. Our examinations will focus on transfers, recordkeeping, and the safeguarding of funds and securities. Examination candidates will include transfer agents that serve as paying agents or that service microcap or crowdfunding issuers.

## Regulation Systems Compliance and Integrity (SCI) Entities

Regulation SCI was adopted by the Commission to strengthen the technology infrastructure of the U.S. securities markets.<sup>3</sup> Among other things, it requires SCI entities, which include, national securities exchanges, clearing agencies, and certain alternative trading systems, to establish, maintain, and enforce policies and procedures for their systems' capacity, integrity, resiliency, availability, and security. If certain SCI events occur, these entities are required to take corrective action as soon as reasonably practical and immediately notify the SEC of the occurrence. We will continue to examine SCI entities to evaluate whether they have effectively implemented such written policies and procedures. OCIE will also review, among other things, controls relating to how systems record the time of transactions or events and how they synchronize with other systems. Examinations will also assess entities' readiness and business continuity plan effectiveness, vendor risk management, particularly in cloud environments, and enterprise risk management, including whether these programs cover appropriate business units, subsidiaries, and related interconnected infrastructure.

---

<sup>3</sup> See Regulation Systems Compliance and Integrity, Release No. 34-37639, (November 19, 2014), <http://www.sec.gov/rules/final/2014/34-73639.pdf>.

## FOCUS ON FINRA AND MSRB

### FINRA

FINRA is a registered national securities association and a primary regulator of the vast majority of SEC-registered broker-dealers. As an SRO, FINRA adopts and enforces rules governing the conduct of its members. FINRA oversees approximately 3,700 brokerage firms, 156,000 branch offices, and 630,000 registered representatives through examinations, enforcement, and surveillance. In addition, FINRA, among other things, provides a forum for securities arbitration and mediation, conducts market regulation by contract for numerous exchanges, reviews broker-dealer advertisements, administers the testing and licensing of registered persons, and operates industry utilities such as Trade Reporting Facilities. Our examinations of FINRA will focus on FINRA's operations and regulatory programs and the quality of FINRA's examinations of broker-dealers and municipal advisors that are also registered as broker-dealers.

### MSRB

MSRB regulates the activities of broker-dealers that buy, sell, and underwrite municipal securities. MSRB also regulates municipal advisors. MSRB establishes rules for municipal securities dealers and municipal advisors, supports market transparency by making municipal securities trade data and disclosure documents available, and conducts education and outreach regarding the municipal securities market. Given the responsibility of the MSRB to regulate municipal securities firms, examination staff will examine the MSRB to evaluate the effectiveness of select operational and internal policies, procedures, and controls.

#### DID YOU KNOW?

FINRA oversees approximately 3,700 brokerage firms, 156,000 branch offices, and 630,000 registered representatives through examinations, enforcement, and surveillance.

## CYBERSECURITY

Cybersecurity protection is critical to the operation of our markets. The scope and severity of risks that cyber threats present have increased dramatically. The impact of a successful cyber attack may have consequences that extend beyond the firm compromised to other market participants and retail investors, who may not be well informed of these risks and consequences. We are focused on working with firms to identify and manage cybersecurity risks and to encourage market participants to actively and effectively engage in this effort.

We will continue to prioritize cybersecurity in each of our examination programs. Our examinations have and will continue to focus on, among other things, governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.

## ANTI-MONEY LAUNDERING PROGRAMS

Certain financial institutions are required by regulations adopted under the Bank Secrecy Act to establish anti-money laundering programs. These “AML program” rules require institutions (including the securities firms we regulate such as broker-dealers and investment companies) to, among other things, establish written programs to identify their customers, perform customer due diligence, and monitor accounts for suspicious activity. Where suspicious activity is noted, institutions have an obligation to file Suspicious Activity Reports (SARs) with the Financial Crimes Enforcement Network. These SARs have been used by the SEC and various law enforcement agencies to detect and combat terrorist financing, organized crime, public corruption, and a variety of other fraudulent behavior. As a result, ensuring financial institutions meet their AML program obligations is an important and critical task for financial regulators.

### DID YOU KNOW?

Certain financial institutions are required by regulations adopted under the Bank Secrecy Act to establish anti-money laundering programs.

In 2018, we will continue to focus a portion of our resources on examining whether the entities we regulate are appropriately adapting their AML programs to address their obligations. Our reviews will cover, for example, the customer due diligence requirement and will look to determine whether these entities are taking reasonable steps to understand the nature and purpose of customer relationships and to properly address risks. We will also assess whether these entities are

filing timely, complete, and accurate SARs. Last, we will take steps to evaluate whether these entities are conducting robust and timely independent tests of their AML programs.

## CONCLUSION

This description of OCIE priorities is not exhaustive. While we expect to allocate significant resources throughout 2018 to the examination issues described herein, our staff will also conduct examinations focused on risks, issues, and policy matters that arise from market and regulatory developments, new information learned from examinations, or other sources, including tips, complaints, and referrals, and coordination with other regulators. OCIE welcomes comments and suggestions regarding how we can better fulfill our mission to promote compliance, prevent fraud, identify and monitor risk, and inform SEC policy. If you suspect or observe activity that may violate the federal securities laws or otherwise operates to harm investors, please notify SEC Staff at <https://www.sec.gov/tcr>.







U.S. Securities and  
Exchange Commission  
100 F Street NE  
Washington, DC 20549  
[www.sec.gov](http://www.sec.gov)

Tab 12



March 2018

# FINANCIAL TECHNOLOGY

## Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight

# GAO Highlights

Highlights of [GAO-18-254](#), a report to congressional requesters

## Why GAO Did This Study

Advances in technology and the widespread use of the Internet and mobile communication devices have helped fuel the rise of traditional financial services provided by non-traditional technology-enabled providers, often referred to as fintech.

GAO was asked to provide information on various aspects of fintech activities. This report addresses fintech payment, lending, wealth management, and other products. GAO assesses 1) fintech benefits, risks, and protections for users; 2) regulatory oversight of fintech firms; 3) regulatory challenges for fintech firms; and 4) the steps taken by domestic and other countries' regulators to encourage financial innovation within their countries. GAO reviewed available data, literature, and agency documents; analyzed relevant laws and regulations; and conducted interviews with over 120 federal and state regulators, market participants, and observers, and regulators in 4 countries with active fintech sectors and varying regulatory approaches.

## What GAO Recommends

GAO is making numerous recommendations related to improving interagency coordination on fintech, addressing competing concerns on financial account aggregation, and evaluating whether it would be feasible and beneficial to adopt regulatory approaches similar to those undertaken by regulators in jurisdictions outside of the United States. In written comments on a draft of this report, the agencies stated that they concurred with GAO's recommendations and would take responsive steps.

View [GAO-18-254](#). For more information, contact Lawrence L. Evans, Jr. at (202) 512-8678 or [Evansl@gao.gov](mailto:Evansl@gao.gov).

March 2018

## FINANCIAL TECHNOLOGY

### Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight

## What GAO Found

Fintech products—including payments, lending, wealth management, and others—generally provide benefits to consumers, such as convenience and lower costs. For example, fintech robo-advisers offer low cost investment advice provided solely by algorithms instead of humans. Fintech products pose similar risks as traditional products, but their risks may not always be sufficiently addressed by existing laws and regulations. Also, regulators and others noted that fintech activities create data security and privacy concerns and could potentially impact overall financial stability as fintech grows.

The extent to which fintech firms are subject to federal oversight of their compliance with applicable laws varies. Securities regulators can oversee fintech investment advisers in the same ways as traditional investment advisers. Federal regulators may review some activities of fintech lenders or payment firms as part of overseeing risks arising from these firms' partnerships with banks or credit unions. In other cases, state regulators primarily oversee fintech firms, but federal regulators could take enforcement actions. Regulators have published consumer complaints against fintech firms, but indications of widespread consumer harm appear limited.

The U.S. regulatory structure poses challenges to fintech firms. With numerous regulators, fintech firms noted that identifying the applicable laws and how their activities will be regulated can be difficult. Although regulators have issued some guidance, fintech payment and lending firms say complying with fragmented state requirements is costly and time-consuming. Regulators are collaborating in various ways, including engaging in discussions on financial protections for customers that may experience harm when their accounts are aggregated by a fintech firm and unauthorized transactions occur. Market participants disagree over reimbursement for such consumers, and key regulators are reluctant to act prematurely. Given their mandated consumer protection missions, regulators could act collaboratively to better ensure that consumers avoid financial harm and continue to benefit from these services. GAO has identified leading practices for interagency collaboration, including defining agency roles and responsibilities and defining outcomes. Implementing these practices could increase the effectiveness of regulators' efforts to help resolve this conflict.

Regulators abroad have taken various approaches to encourage fintech innovation. These include establishing innovation offices to help fintech firms understand applicable regulations and foster regulatory interactions. Some use "regulatory sandboxes" that allow fintech firms to offer products on a limited scale and provide valuable knowledge about products and risks to both firms and regulators. Regulators abroad also established various mechanisms to coordinate with other agencies on financial innovation. While some U.S. regulators have taken similar steps, others have not due to concerns of favoring certain competitors or perceived lack of authority. While these constraints may limit regulators' ability to take such steps, considering these approaches could result in better interactions between U.S. regulators and fintech firms and help regulators increase their understanding of fintech products. This would be consistent with GAO's framework calling for regulatory systems to be flexible and forward looking to help regulators adapt to market innovations.

---

# Contents

---

Letter		1
	Background	3
	Fintech Activities Can Provide Benefits and Pose Risks to Consumers and the Broader Financial System	12
	Fintech Firms' Compliance with Applicable Laws Is Subject to Varied Federal Oversight	30
	The U.S. Regulatory Environment Poses Various Challenges to Fintech Firms	40
	Consideration of Regulatory Approaches Abroad Could Benefit Fintech Regulation and Innovation	59
	Conclusions	72
	Recommendations for Executive Action	74
	Agency Comments and Our Response	76
Appendix I	Objectives, Scope, and Methodology	81
Appendix II	Interagency Collaborative Efforts That Have Addressed Fintech Issues	85
Appendix III	Regulatory Sandbox Examples	90
Appendix IV	Comments from the Consumer Financial Protection Bureau	94
Appendix V	Comments from the Commodity Futures Trading Commission	96
Appendix VI	Comments from the Conference of State Bank Supervisors	98
Appendix VII	Comments from the Federal Communications Commission	113

Appendix VIII	Comments from the Federal Deposit Insurance Corporation	114
Appendix IX	Comments from the Board of Governors of the Federal Reserve System	117
Appendix X	Comments from the National Credit Union Administration	121
Appendix XI	Comments from the Office of the Comptroller of the Currency	122
Appendix XII	Comments from the Securities and Exchange Commission	124
Appendix XIII	GAO Contact and Staff Acknowledgments	126

## Tables

Table 1: Agencies with Regulatory Responsibilities Related to Financial Technology Activities	11
Table 2: Domestic Interagency Fintech Collaboration Efforts	86
Table 3: International Interagency Fintech Collaboration Efforts	88

## Figures

Figure 1: How Mobile Wallets Work	5
Figure 2: Illustration of a Direct Lender Model	6
Figure 3: Illustration of a Lender Partnered with a Depository Institution Model	7
Figure 4: Illustration of a Fintech Wealth Management Interaction	8
Figure 5: Select Interaction-Building Initiatives among U.S. Federal and Other Jurisdictions' Regulators	62
Figure 6: Select Knowledge-Building Initiatives among U.S. Federal and Other Jurisdictions' Regulators	64
Figure 7: Select Regulatory Coordination Initiatives among U.S. Federal and Other Jurisdictions' Regulators	70

---

---

## Abbreviations

AML	Anti-money laundering
Apps	Applications
CFPB	Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
CSBS	Conference of State Bank Supervisors
CTF	Counter-terrorist financing
DLT	Distributed ledger technology
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FCC	Federal Communications Commission
FDIC	Federal Deposit Insurance Corporation
Federal Reserve	Board of Governors of the Federal Reserve System
FFIEC	Federal Financial Institutions Examination Council
FinCEN	Treasury Financial Crimes Enforcement Network
FINRA	Financial Industry Regulatory Authority
Fintech	Financial technology
FTC	Federal Trade Commission
GLBA	Gramm-Leach-Bliley Act
GPS	Global Positioning System
HKMA	Hong Kong Monetary Authority
ICURN	International Credit Union Regulators Network
ILC	Industrial Loan Corporation
IOSCO	International Organization of Securities Commissions
MAS	Monetary Authority of Singapore
MSB	Money services business
NCUA	National Credit Union Administration
OCC	Office of the Comptroller of the Currency
SEC	Securities and Exchange Commission
TFCC	Task Force on Consumer Compliance
TFFT	Task Force on Financial Technology
TFOS	Task Force on Supervision
Treasury	Department of the Treasury
UK	United Kingdom

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



March 22, 2018

## Congressional Requesters

Advances in technology and the widespread use of the Internet and mobile communication devices have helped fuel the rise of financial services provided by nonfinancial firms, including large and small technology firms. Often referred to as fintech, these firms are offering payment services, loans to consumers and businesses, advice on investments or other financial activities, and other services.<sup>1</sup> While typically offering their services through mobile devices or the Internet with little or no face-to-face interaction, these fintech firms also often incorporate the use of traditional financial products, such as debit or credit cards, or partner with existing financial institutions to provide their services.

The products and services offered by fintech firms provide benefits to consumers and businesses but also can present risks. The extent to which some fintech firms or their activities are regulated can also vary. While some fintech products and services are being offered by U.S. firms, fintech activities are also occurring in other places, including in the United Kingdom and Asia. In April 2017, we issued a report providing an overview of fintech activities and their oversight.<sup>2</sup>

You asked us to provide information on the various aspects of fintech activities. This report addresses four types of fintech activities, payments, lending, wealth and financial advice, and distributed ledger technologies—some of which are known as blockchain—that are being used to track financial asset ownership or other purposes. Specifically for these four fintech sectors, we report on (1) their benefits, risks, and extent of legal or regulatory protections for users; (2) the efforts by U.S. regulators to oversee fintech activities; (3) challenges that the regulatory environment poses to fintech firms; and (4) the steps taken by domestic

---

<sup>1</sup>In some cases, traditional financial firms, such as banks or investment advisers, are also offering products through mobile devices or the Internet that are similar to those offered by fintech firms, but this report primarily focuses on those offered by non-financial firms to consumers because of the potential differences in regulatory oversight of fintech firms as compared to traditional financial institutions.

<sup>2</sup>GAO, *Financial Technology: Information on Subsectors and Regulatory Oversight*, [GAO-17-361](#) (Washington, D.C.: Apr. 19, 2017).



---

and other countries' regulators to encourage financial innovation within their countries.

To address these objectives, we reviewed available data on transaction volumes; prior GAO reports; and academic papers, reports, and studies by other organizations on fintech activities. We analyzed relevant financial laws and regulations to determine the extent to which fintech activities were covered by their protections. We also reviewed guidance, final rulemakings, initiatives, and enforcement actions from agencies.

We conducted over 120 interviews with representatives of relevant organizations, including fintech providers; financial institutions; related trade associations; law firms; and consumer groups. These interviews also included federal financial regulators in the United States, including staff from the federal depository institution prudential regulators: the Federal Deposit Insurance Corporation (FDIC); the Board of Governors of the Federal Reserve System (Federal Reserve); the Office of the Comptroller of the Currency (OCC); and the National Credit Union Administration (NCUA); as well as staff from the Commodity Futures Trading Commission (CFTC); the Consumer Financial Protection Bureau (CFPB); the Department of the Treasury (Treasury); the Federal Communications Commission (FCC); the Federal Trade Commission (FTC); the Financial Industry Regulatory Authority (FINRA); the Securities and Exchange Commission (SEC); and the Small Business Administration.

To obtain state-level perspectives, we interviewed representatives of associations representing state attorneys general and state regulators for banks, credit unions, money transmitters, and securities entities as well as staff from relevant state regulatory agencies in three states with active fintech firms and regulatory activities—California, Illinois, and New York. We also interviewed representatives of fintech providers, trade associations, and regulators in other jurisdictions with active fintech sectors and that were pursuing various potentially innovative regulatory activities, which included Canada; Hong Kong; Singapore; and the United Kingdom. (See app. I for a more detailed discussion of our scope and methodology for this report.)

We conducted this performance audit from August 2016 to March 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that

---

the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

## Background

Fintech—originally short for financial technology—refers to the use of technology and innovation to provide financial products and services. For purposes of this report, fintech firms are nontraditional technology-enabled providers, such as start-ups or more established technology firms, such as Apple or Google, that are offering traditional financial products or services to consumers. Fintech products or services are typically provided—sometimes exclusively—through the Internet or via mobile devices, such as smartphones, rather than being provided through face-to-face visits to financial institution branches.

The products and services that fintech firms offer include:

- payments between individuals, and between individuals and businesses;
- loans to consumers and businesses;
- advice on wealth management or general financial activities; and
- distributed ledger technology used to make payments, record and track asset ownership, and other purposes.

---

## Fintech Payments

Various fintech firms offer ways for individuals to make payments and transfer value, including for purchasing goods or services or for transferring money to individuals domestically or internationally. The payments offered by these providers are often conducted using applications (apps) on smartphones or other mobile devices. Often these fintech payments involve the use of accounts linked to existing debit or credit cards and are processed through the existing networks and channels for these types of payments. In some cases, fintech providers may also route their payments through the Automated Clearing House networks, which have traditionally been used to facilitate automatic bill paying to utilities or other merchants or funds transfers between banks. Fintech payments can also be made by charging a consumer's phone bill. For example, consumers can send charity contributions via text or charge in-app purchases to their mobile phone bill.

One common fintech payment method involves mobile wallets, or electronic versions of consumers' wallets, which offer consumers the convenience of conducting transactions without having to enter credit or

---

debit card information for each transaction. Using a mobile wallet, consumers can store payment card information and other information on their mobile devices that is often needed to complete a purchase.<sup>3</sup> Generally, mobile wallets replace sensitive information with random values—a process called tokenization—to provide greater security when making a payment, and transmit this information using existing credit and debit card networks.<sup>4</sup> A variety of fintech firms provide mobile wallets, including Apple, Google, and Samsung.<sup>5</sup>

Consumers may use mobile wallets to make payments to other consumers or to businesses; in mobile applications; through mobile browsers; or in-person at a store's point-of-sale terminal. Some providers, such as Paypal and Venmo, allow individuals to create accounts on mobile devices to make payments funded by debit or credit cards, as well receive and store funds sent to the account owner that can be used to make payments to others or buy goods from merchants. Figure 1 illustrates how a mobile wallet enables the payment information to be transferred by allowing compatible devices to exchange data when placed in very close proximity to each other using various technologies, such as wireless communication.<sup>6</sup>

---

<sup>3</sup>In a mobile wallet, consumers can enter payment information from debit and credit cards, gift cards, and prepaid cards. Consumers can also store other information often needed to complete a transaction, such as shipping address, e-mail, and phone number.

<sup>4</sup>Tokenization is the process of replacing sensitive credit or debit card information—such as bank account and credit or debit card numbers— with randomly generated numbers. Tokenization can reduce the financial impact resulting from data compromise, theft, or unintended disclosure during disposal because the randomly generated numbers can be specific to each transaction. For more information, see Susan Pandey and Marianne Crowe, *Mobile Payments Industry Workgroup Meeting Discussion on Tokenization Landscape in the U.S.* (Washington, D.C.: September 2014) and also Marianne Crowe, Susan Pandey, David Lott, and Steve Mott, *Is Payment Tokenization Ready for Primetime? Perspectives from Industry Stakeholders on the Tokenization Landscape*, Federal Reserve Bank of Atlanta and Federal Reserve Bank of Boston, June 11, 2015.

<sup>5</sup>Mobile wallets are also offered by other merchants, such as Starbucks, Walmart, and CVS, as well as traditional financial institutions such as JP Morgan Chase & Co. and Citibank.

<sup>6</sup>Wireless communication technologies include Near Field Communications technology, a standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart, among others.

**Figure 1: How Mobile Wallets Work**



Source: GAO. | GAO-18-254

Regarding the total volume of payments by fintech providers, the association representing state banking supervisors estimated that fintech payment firms were likely used to facilitate payments or currency exchanges of up to \$189 billion in the first 2 quarters of 2017. In a 2016 report on consumers' use of mobile financial services, the Federal Reserve's survey of more than 2,220 respondents found that over 30 percent of consumers aged 18-44 had made payments using mobile phones sometime during 2015.<sup>7</sup> According to a report by the Smart Payment Association, 200,000 locations accepted Apple Pay when it was

<sup>7</sup>Board of Governors of the Federal Reserve, *Consumers and Mobile Financial Services 2016* (Washington, D.C.: March 2016).

---

launched in September 2014, but by February 2016, this number had reached 2 million.<sup>8</sup> According to Paypal, it had 218 million active customer accounts at the end of the third quarter of 2017 and processed over 6 billion payments valued at more than \$354 billion in 2016.

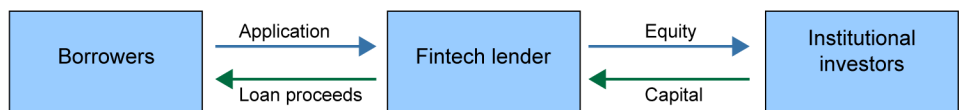
---

## Fintech Lending

Fintech lenders—often referred to as marketplace lenders and which operate almost exclusively online—offer a variety of loan types and may use different sources of funds than traditional lenders. The types of loans offered by fintech providers include consumer and small business loans. While these lenders may use traditional means of assessing borrowers' creditworthiness, such as credit scores, they also may analyze large amounts of additional or alternative sources of data on other aspects of borrower characteristics, such as information from bank accounts, to determine creditworthiness.

Fintech lenders can follow various models. For example, some conduct person-to-person lending in which loans are financed by individual investors. In other cases, the funds for these loans can come from institutional investors such as hedge funds, financial institutions, or from notes sold to individual investors. In some cases, funding for loans is obtained by securitizing previously-made loans and selling securities backed by the cashflows from the underlying loans. The fintech lenders that use external capital are referred to as direct lenders and include such firms as SoFi and Earnest. Figure 2 below shows the flow of funds for typical direct lenders.

**Figure 2: Illustration of a Direct Lender Model**



Sources: GAO analysis of Congressional Research Service and Department of the Treasury information. | GAO-18-254

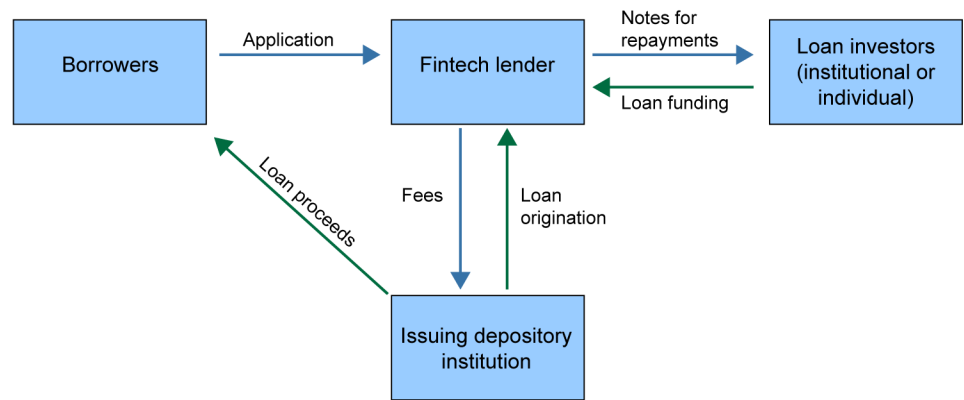
Other fintech lenders include lenders that partner with depository institutions—including banks or credit unions—to originate loans that are then purchased by the lender or by another investor. Examples of lenders partnered with depository institutions include LendingClub Corporation,

---

<sup>8</sup>Smart Payment Association, *An Overview of Contactless Payment Benefits and Worldwide Deployments*, April 2016.

Prosper, and Upstart. Figure 3 shows the flow of funds for such lenders. Some lenders, such as OnDeck, have now developed hybrid models, selling some whole loans to institutional investors while retaining servicing responsibilities.

**Figure 3: Illustration of a Lender Partnered with a Depository Institution Model**



Sources: GAO analysis of Congressional Research Service and Department of the Treasury information. | GAO-18-254

One firm that tracks fintech activities reported that the volume of lending by 13 of the most significant lenders had reached about \$61 billion as of the end of September 2016,<sup>9</sup> and other market monitors estimate that fintech lending volumes could grow to as much as \$90 billion to \$122 billion by 2020.<sup>10</sup>

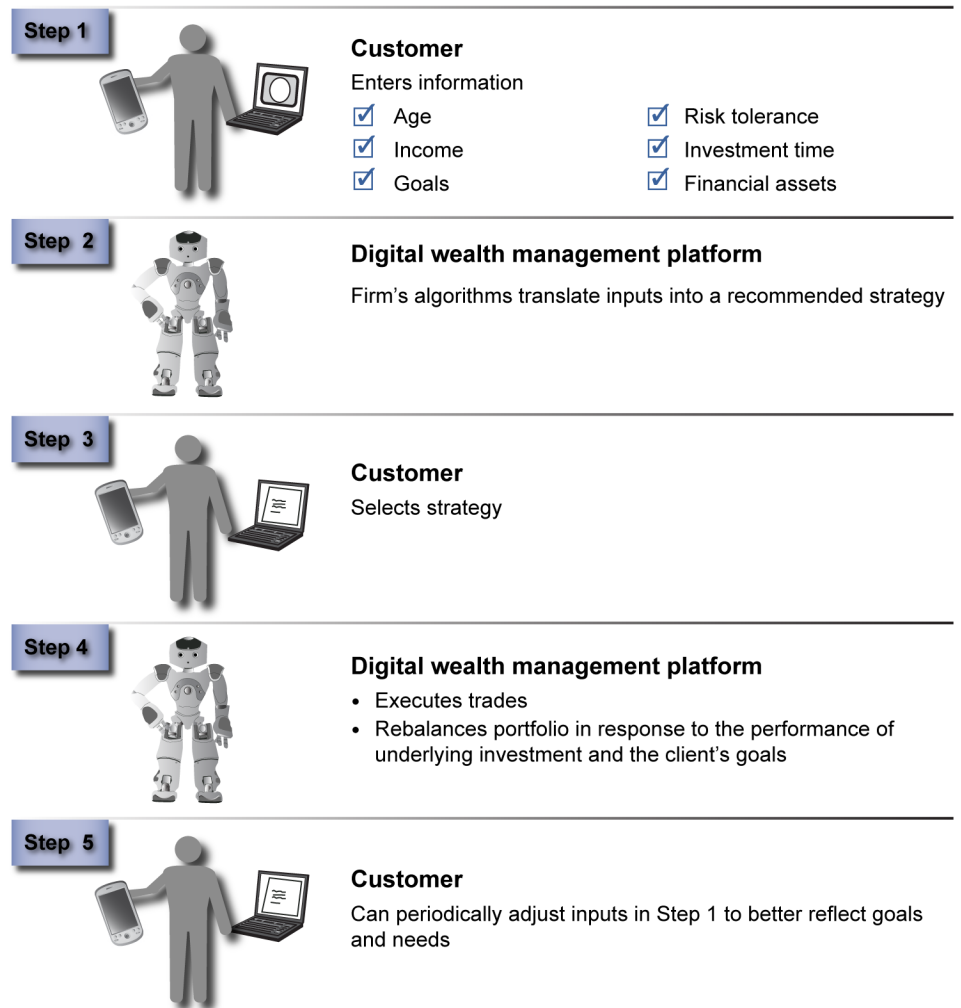
## Fintech Wealth Management and Financial Advice

Fintech firms are also offering wealth management or other financial advice, some with minimal or no human interaction. For example, new firms called robo-advisers are offering investors advice using algorithms based on these investors' data and risk preferences to provide advice on recommended asset holdings and allocations. Fintech firms offering these advice services include Betterment, Personal Capital, and Wealthfront. Figure 4 illustrates a typical case of a consumer using a fintech wealth management adviser.

<sup>9</sup>See S&P Global Market Intelligence December 2016 *U.S. Digital Lending Landscape* (Charlottesville, Va: December 2016).

<sup>10</sup>See S&P Global Market Intelligence *An Introduction to Fintech: Key Sectors and Trends* (October 2016) and FinXtech, *Fintech Intelligence Report: Marketplace Lending*.

**Figure 4: Illustration of a Fintech Wealth Management Interaction**



Source: GAO analysis. | GAO-18-254

One research firm estimated in July 2017 that robo-adviser firms would have as much as \$1 trillion in assets under management by 2020 and as much as \$4 trillion by 2022.<sup>11</sup>

In addition, some fintech firms—referred to as financial account aggregators—allow consumers to aggregate the information from their

<sup>11</sup>Business Insider Intelligence, *Evolution of Robo Advising*, June 2017.

---

various financial accounts, including their assets in bank accounts and brokerage accounts, to enable them to better see their financial health and receive advice on alternative ways to save money or manage their finances. Consumers can access this combined information either online or on mobile devices. Account aggregator firms offering this type of advice on savings and other activities include Mint and HelloWallet.

---

## Distributed Ledger Technologies

Distributed ledger technology (DLT) is a secured way of conducting transfers of digital assets in a near real-time basis potentially without the need for a central authority. DLT involves a distributed database maintained over a network of connected computers that allows network participants to share and retain identical cryptographically secured records. Such networks can consist of individuals, financial entities, or other businesses.

Blockchain is one type of DLT. A blockchain is a shared digital ledger that records transactions in a public or private network. Distributed to all members in the network, the ledger permanently records, in a sequential chain of cryptographically secured blocks, the history of transactions that take place among the participants in the network. DLT products can have different types of access control. For example, some may be “unpermissioned” (public) ledgers that are open to everyone to contribute data to the ledger and have no central control, while others may be “permissioned” (private) ledgers that allow only certain participants to add records and verify the contents of the ledger.

The financial services industry has identified various potential uses for DLT. These include tracking international money transfers<sup>12</sup> or tracking the changes of ownership of various financial assets, such as or securities like bonds or stocks or derivatives like swaps contracts. In addition, DLT is being used to track ownership of bitcoin, a virtual currency, specifically using a blockchain.<sup>13</sup>

Some companies are using DLT to raise funds. According to a recent bulletin by U.S. securities regulators, these virtual coins or tokens are

---

<sup>12</sup>See [GAO-14-496](#). As we previously reported, virtual currencies can be used to make payments and transfer funds.

<sup>13</sup>See GAO, *Virtual Currencies: Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges*, [GAO-14-496](#) (Washington, D.C.: May 29, 2014).



---

being created and then disseminated using DLT as part of offerings known as token sales or initial coin offerings.<sup>14</sup> As part of these token sales, purchasers may use fiat currency (e.g., U.S. dollars) or virtual currencies to buy these virtual coins or tokens. Currently, the capital raised from the sales may be used to fund development of a digital platform, software, or other project; or, the virtual tokens or coins may be used to access the platform, use the software, or otherwise participate in the project. After they are issued, in some cases the virtual coins or tokens may be resold to others in a secondary market on virtual currency exchanges or other platforms.

---

## Various Regulators May Oversee Fintech Activities

A variety of federal and state regulatory bodies may oversee fintech firms or their activities to the extent these firms provide a regulated payment; lending; wealth management; or distributed ledger technology service or activity. Table 1 explains the basic functions of the relevant federal regulators.

---

<sup>14</sup>Securities and Exchange Commission, *Investor Bulletin: Initial Coin Offerings*, (July 25, 2017).

**Table 1: Agencies with Regulatory Responsibilities Related to Financial Technology Activities**

Regulator	Basic function
Board of Governors of the Federal Reserve System	Supervises state-chartered banks that opt to be members of the Federal Reserve System, bank and thrift holding companies, and the nondepository institution subsidiaries of those institutions; and nonbank financial companies and financial market utilities designated as systemically important by the Financial Stability Oversight Council for consolidated supervision and enhanced prudential standards. Supervises state-licensed branches and agencies of foreign banks and regulates the U.S. nonbanking activities of foreign banking organizations.
Federal Deposit Insurance Corporation	Insures the deposits of all banks and thrifts approved for federal deposit insurance; supervises insured state-chartered banks that are not members of the Federal Reserve System, as well as insured state savings associations and insured state chartered branches of foreign banks; resolves all failed insured banks and thrifts; and may be appointed to resolve large bank holding companies and nonbank financial companies supervised by the Federal Reserve. Also, has backup supervisory responsibility for all federally insured depository institutions.
National Credit Union Administration	Charters and supervises federally chartered credit unions and insures savings in federal and most state-chartered credit unions.
Office of the Comptroller of the Currency	Charters and supervises national banks, federal savings associations, and federally licensed branches and agencies of foreign banks.
Consumer Financial Protection Bureau	Regulates the offering and provision of consumer financial products or services under the federal consumer financial laws. Has exclusive examination authority as well as primary enforcement authority for the federal consumer financial laws for insured depository institutions with over \$10 billion in assets and their affiliates. Supervises certain nondepository financial entities and their service providers and enforces the federal consumer financial laws. Enforces prohibitions on unfair, deceptive, or abusive acts or practices and other requirements of the federal consumer financial laws for persons under its jurisdiction.
Department of the Treasury Financial Crimes Enforcement Network	Administers the Bank Secrecy Act, which with its implementing regulations, generally requires financial institutions, among others, to collect and retain various records of customer transactions, verify customers' identities in certain situations, maintain anti-money laundering programs, and report suspicious and large cash transactions. Collects, analyzes, and disseminates financial intelligence information from institutions. It generally relies on financial regulators and other entities to conduct routine examinations of U.S. financial institutions across a variety of financial sectors to determine compliance with these regulations.
Federal Communications Commission	Regulates interstate and international communications by radio; wire; satellite; and cable.
Federal Trade Commission	Maintains competition and has consumer protection enforcement authority over nonbank financial entities, including certain kinds of mortgage market participants; payment processors; private student lenders; and payday loan lenders, for the purposes of enforcing the consumer financial protection laws. Has investigative and law enforcement authority to protect consumers from unfair or deceptive acts or practices in most sectors of the economy.
Securities and Exchange Commission	Regulates securities markets, including offers and sales of securities and regulation of securities activities of certain participants such as securities exchanges; broker-dealers; investment companies; clearing agencies; transfer agents; and certain investment advisers and municipal advisers. Oversees self-regulatory organizations, such as the Financial Industry Regulatory Authority (FINRA). FINRA seeks to promote investor protection and market integrity by developing rules, examining securities firms for compliance, and taking actions against violators.
Commodity Futures Trading Commission	Regulates derivatives markets and seeks to protect market users and the public from fraud; manipulation; abusive practices; and systemic risk related to derivatives subject to the Commodity Exchange Act. Also seeks to foster open, competitive, and financially sound futures markets.

Source: GAO analysis of relevant laws and agency documents. | GAO-18-254

---

In addition to the federal regulators above, various state entities also conduct regulatory activities over fintech firms operating within their jurisdictions. According to the association representing state regulators, state financial services regulators license and supervise activities, such as money transmission, consumer lending, and debt collection, irrespective of technology deployed. Nonbank financial service providers that offer services directly to consumers are likely subject to state oversight. In addition to state financial services regulators, state securities regulators, state entities that oversee corporate activities, and state attorneys general have jurisdiction over certain fintech firms. In general, these entities may have authority to license or register firms, conduct exams, and take enforcement actions for violations of state laws or regulatory requirements.

---

## **Fintech Activities Can Provide Benefits and Pose Risks to Consumers and the Broader Financial System**

Fintech products in payments; lending; wealth management; and distributed ledger technology can provide consumers and the broader financial system with various benefits but may also pose risks similar to those of traditional products. While existing laws apply to fintech products and services in most cases, some products pose additional risks that may not be sufficiently covered by existing laws.<sup>15</sup>

---

<sup>15</sup> In addition, as discussed in the next section, the extent to which federal regulators oversee fintech firms' compliance with applicable laws can vary.

---

## Fintech Products Can Provide Various Consumer Benefits

According to our prior work, literature we reviewed, and stakeholders we interviewed, consumer benefits of fintech products include greater convenience; lower cost; increased financial inclusion; faster services; and improved security.<sup>16</sup>

- **Greater convenience:** Consumers can use fintech products and services on their mobile device to make payments; transfer money; easily obtain payment for shared expenses; obtain loans; or to receive investment advice without the time and expense of visiting a financial service provider's physical location. They can also access these services outside of standard business hours. In addition, the ability to see information from all of their financial accounts together in a single dashboard provided by an account aggregator is more convenient than reviewing information from each account on separate statements.
- **Lower cost:** Innovations in payments, including the use of DLT, could reduce the cost of payments for consumers. For example, one fintech firm uses DLT to reduce the operational and liquidity costs traditionally incurred with some international payments.<sup>17</sup> Some fintech providers do not charge fees for payments, so consumers save by avoiding paying for checks or incurring automated teller machine fees. In addition, because fintech providers often do not have overhead costs associated with physical locations and use automation instead of relying on large staffs to provide services, they may be able to pass these cost savings on to consumers. For example, according to a Treasury report, automated loan processing, underwriting, and servicing may allow fintech lenders to offer lower rates or fees on their loans because they have to hire fewer loan officers.<sup>18</sup> Similarly, automation in robo-advising could allow consumers to obtain investment advice at a lower cost than if they obtained services from a firm that relied more heavily upon human advisers.

---

<sup>16</sup> GAO, *Financial Technology: Information on Subsectors and Regulatory Oversight*, [GAO-17-361](#) (Washington, D.C.: Apr. 19, 2017).

<sup>17</sup> This firm estimates its DLT product reduces bank operational costs by 30 percent to 33 percent. In addition it allows banks to avoid liquidity costs associated with pre-funding payments denominated in foreign currencies, which the firm notes are driven by implicit costs of compliance, correspondent banking, and opportunity cost.

<sup>18</sup> Department of the Treasury, *Opportunities and Challenges in Online Marketplace Lending* (Washington, D.C.: May 2016).

- 
- **Increased financial inclusion:** Using alternative data may allow fintech lenders to offer loans to consumers whose traditional credit history may have been insufficient for banks to extend them credit.<sup>19</sup> CFPB officials stated that using alternative data—including bill payment history as a proxy for debt repayment—could expand responsible access to credit, particularly to some consumers who are among the estimated 45 million people who lack traditional credit scores.<sup>20</sup> Similarly, a study by FDIC staff noted that fintech accounts may also enable consumers whose traditional accounts are closed due to lack of profitability for the provider or other reasons to continue to have access to financial services.<sup>21</sup> Also, robo-advising services can make investment advice more accessible to consumers who cannot meet account minimums at traditional advisers by offering lower account minimums.
  - **Faster services:** Automation may reduce transaction times for services like loan approval or investment advice. Stored payment data in fintech providers' mobile wallets may reduce transaction time for online purchases because consumers do not need to reenter billing information. Further, such data may reduce transaction time for in-store purchases because transactions using contactless payments are faster than transactions using card readers and cash. Peer-to-peer payments made via mobile wallets may transfer money faster than checks. Also, using DLT may greatly reduce settlement times for currency, derivatives, and securities transactions by improving processes or reducing the number of entities involved in a transaction. For example, one firm is using DLT to reduce settlement for securities from 2 days to the same day.
  - **Improved security:** While credit and debit transactions have traditionally transmitted sensitive information that can be hacked and used to make fraudulent transfers, fintech providers' mobile wallets generally replace this sensitive information with randomly generated numbers that mitigate the risk that transaction information can be

---

<sup>19</sup>Credit scores are typically calculated using information in consumers' credit reports, including bill payment history, unpaid debt, number and type of loans, debt collection, foreclosure, and bankruptcy. Alternative data that can also be used are drawn from sources such as bill payments for mobile phones and rent, and electronic transactions such as bank deposits and withdrawals or transfers.

<sup>20</sup>Consumer Financial Protection Bureau, *Data Point: Credit Invisibles* (Washington, D.C.: May 2015).

<sup>21</sup>Federal Deposit Insurance Corporation, *Assessing the Economic Inclusion Potential of Mobile Financial Services* (Washington, D.C.: June 2014).

---

used fraudulently (tokenization), according to the Federal Reserve's Mobile Payments Industry Workgroup. Similarly, while lost or stolen credit and debit cards can be used to make fraudulent payments, a lost or stolen mobile device can have security features that protect a mobile wallet from unauthorized use. For example, according to FTC, mobile device features such as device passwords, fingerprint readers, and face recognition software can help protect consumer accounts from unauthorized access. Additionally, FCC notes in a consumer guide that consumers' ability to disable their mobile devices remotely can help prevent fraudulent use of a consumer's fintech provider accounts if their mobile devices have been lost or stolen.<sup>22</sup> Further, mobile device Global Positioning System (GPS) data can help identify suspicious activity in consumer accounts or to ensure that a mobile phone being used at a particular merchant is actually at that location, according to the Federal Reserve's Mobile Payments Industry Workgroup and others.

---

## Fintech Products Generally Pose Consumer Risks Similar to Those of Traditional Products

The literature we reviewed and stakeholders we interviewed also identified potential risks fintech products pose to consumers, including fraud, discrimination, and unsuitable advice. In general, these risks are similar to those posed by traditional financial products. While laws that apply to traditional products also apply to fintech products in most cases, some fintech products pose additional risks that may not be sufficiently addressed by existing laws. While the legal framework for consumer protection applies to many of the risks associated with fintech products, the extent to which consumers benefit from these protections is a function of the existing regulatory framework and its coverage of fintech activity. We discuss the regulatory framework for fintech products in greater detail later in this report.

## Fintech Payments

Consumers face the risk of unauthorized transactions regardless of whether they use a traditional or fintech firm to make payments. CFPB officials we interviewed told us that some fintech products, such as mobile wallets, increase the number of firms involved in a transaction, which may increase the risk of unauthorized transactions. However, when consumers fund their mobile wallets by linking to traditional funding sources—debit or credit cards or bank accounts—consumer protection laws such as the Electronic Fund Transfer Act and the Truth in Lending

---

<sup>22</sup>Federal Communications Commission, *Consumer Guide: Mobile Wallet Services Protection* (Washington, D.C.: October 2016).

---

Act generally apply. These acts and their implementing regulations provide that consumers can dispute charges to these accounts and liability for losses may be limited to \$0 if disputes are made within specified time frames.<sup>23</sup>

Consumer protection laws, such as the Electronic Fund Transfer Act, which apply to traditional funding sources, do not yet cover payments funded by mobile wallet balances or mobile carrier billing. To address this gap in protections for mobile wallet funds, CFPB issued a final rule on prepaid accounts that will extend protections for error resolution and liability for unauthorized transfers to prepaid account and mobile wallet balances. This rule had previously been scheduled to become effective in April 2018, but in January 2018, CFPB delayed the effective date of the rule to April 1, 2019.<sup>24</sup> However, fintech firms we interviewed told us that even when certain consumer protections are not required by statute or regulation, they voluntarily provide similar protections and disclose these protections in their terms of service.

---

<sup>23</sup>For example, under the Electronic Fund Transfer Act, consumer liability is limited to \$50 for unauthorized transactions involving lost or stolen access devices, provided the loss or theft is reported within two business days after learning of the loss or theft of the access device. See 12 C.F.R. § 1005.6(b). If the consumer fails to notify the financial institution within two business days after learning of the loss or theft of the access device, the consumer's liability is generally capped at \$500 (though there are certain circumstances in which liability for unauthorized transfers may be unlimited). For other types of unauthorized or erroneous transactions, consumer liability may be limited to \$0. See, e.g., 12 C.F.R. pt. 1005, supp. I.

<sup>24</sup>See Rules Concerning Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth In Lending Act (Regulation Z), 83 Fed. Reg. 6364 (Feb. 13, 2018). CFPB's prepaid accounts rule will extend Regulation E and Regulation Z coverage to prepaid accounts. The rule's definition of prepaid accounts specifically includes accounts that are issued on a prepaid basis or capable of being loaded with funds, whose primary function is to conduct transactions with multiple, unaffiliated merchants for goods or services, or at automatic teller machines, or to conduct person-to-person transfers, and that are not checking accounts, share draft accounts, or negotiable order of withdrawal accounts. See Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth In Lending Act (Regulation Z), 81 Fed. Reg. 83934 (Nov. 22, 2016). This imposes a comprehensive regulatory regime for mobile wallets that are capable of storing funds and other prepaid accounts to ensure that consumers who use them receive consistent protections. 81 Fed. Reg. at 83936. In January 2018, CFPB announced that the rule's effective date, which had been scheduled for April 2018, was being extended to April 2019. See 83 Fed. Reg. at 6364.

---

Agencies have also issued tips for consumers to safeguard their mobile devices and identify fraudulent payments.<sup>25</sup> Similarly, wireless carriers have taken steps to mitigate fraudulent billing in response to enforcement actions, including offering services that prevent third parties from adding charges to consumer bills without consumers' knowledge or permission—a practice known as “cramming.” However, FCC has found that fraudulent billing continues to be a problem.<sup>26</sup> FCC’s July 2017 proposed cramming rule seeks to codify the agency’s existing prohibition against fraudulent billing through language explicitly prohibiting wireless carriers from placing third-party charges on consumers’ bills without consumer verification.<sup>27</sup> In addition, FCC and FTC have issued tips for consumers and firms publicizing practices that help avoid cramming.<sup>28</sup>

Consumers also face the risk their funds could be lost due to the failure of their payment provider. Although consumers with funds in a bank account have protection from this risk through federal deposit insurance up to \$250,000, consumers with funds in a mobile wallet may not be similarly protected. To address this risk, some fintech firms deposit consumers’ mobile wallet balances into an FDIC-insured bank or savings association, resulting in the funds being insured by FDIC up to the applicable deposit insurance limit in the event of the failure of the bank or savings association.<sup>29</sup> Other fintech firms voluntarily disclose to consumers in their terms and conditions that any mobile wallet balances they hold are not

---

<sup>25</sup>Federal Trade Commission, *Payments you didn’t authorize could be a scam* (Washington, D.C.: August 2017); and *An identity thief stole my phone!* (Washington, D.C.: June 2017). Federal Communications Commission, *Consumer Guide: Mobile Wallet Services Protection*.

<sup>26</sup>For example, in the 2-year period from the beginning of 2015 through the end of 2016, FCC received almost 8,000 slamming and cramming complaints, which according to FCC may understate the problem. For more information, see FCC 17-91 Notice of Proposed Rulemaking (Washington, D.C.: July 2017).

<sup>27</sup>Protecting Consumers From Unauthorized Carrier Charges and Related Unauthorized Charges, 82 Fed. Reg. 37830 (Aug. 14, 2017).

<sup>28</sup>Federal Communications Commission, *Consumer Guide: Cramming – Unauthorized Charges on Your Phone Bill* (Washington, D.C.: June 2016). Federal Trade Commission, *How to Say Scram to Crammed Charges on Your Mobile Bill* (Washington, D.C.: July 2014); and *Blog: Consider the cramifications* (Washington, D.C.: July 2012).

<sup>29</sup>In addition, where a fintech firm uses a pooled account to hold consumers’ funds, it must satisfy certain requirements set forth in FDIC’s regulations to ensure that each consumer obtains the full amount of deposit insurance coverage. For more information, see FDIC General Counsel’s Opinion No. 8, *Insurability of Funds Underlying Stored Value Cards and Other Nontraditional Access Mechanisms*, 73 Fed. Reg. 67155 (Nov. 13, 2008).



---

FDIC insured. However, according to the Conference of State Bank Supervisors (CSBS), 49 states have laws that require fintech firms engaged in money transmission or stored value to self-insure through bonding,<sup>30</sup> holding investments against funds held or transmitted,<sup>31</sup> and meeting minimum net worth requirements.<sup>32</sup>

Further, consumers face the risk that their mobile wallet balances will not be accessible in a timely manner. Under the Expedited Funds Availability Act, banks are required to make customers' deposited funds available to them within prescribed time frames.<sup>33</sup> For example, banks are typically required to make funds a customer receives through an electronic transfer available by the next business day. However, as nonbanks, fintech firms are not subject to this act's requirements and therefore do not have to make mobile wallet balances available under the same time frames. For example, one fintech firm we interviewed told us that most transfers from mobile wallets to bank accounts make funds available by the next business day, but certain circumstances, such as suspicious account activity, may cause the firm to delay transfers a few days. Another fintech firm we interviewed told us that transfer amounts are limited based on anti-money laundering requirements. However, fintech

---

<sup>30</sup>CSBS reports that every state requires licensed money transmitters to hold a bond, with the exception of Montana. The most common bonding requirement is \$500,000, and the average maximum bonding amount is \$916,000. Montana is the only state without a law for licensing money services businesses (MSBs). While often worded differently, CSBS reported that the MSB laws have the same general requirements, though often with different number ranges to reflect differences in state markets and risk averseness.

<sup>31</sup>These investments are commonly referred to as "Permissible Investments." The Uniform Law Commission reviewed the purpose of these investments in their summary of the Uniform Money Services Act ("Licensees are required to maintain at all times investments with a market value greater than or equal to the aggregate amount of all outstanding payment instruments, stored value obligations, and transmitted money. The act specifies a list of permissible investments for this purpose, and provides that these investments are held in trust for the benefit of purchasers and holders, even if commingled, in the event of bankruptcy or receivership of the licensee."). See Uniform Law Commission, *Money Services Act*. Available at <http://www.uniformlaws.org/Act.aspx?title=Money%20Services%20Act>. While only 12 states and territories have adopted the Uniform Money Services Act in its entirety, CSBS representatives note that most states use definitions, concepts, and constructs in the uniform law to update their specific state law.

<sup>32</sup>CSBS reports that all states have net worth requirements, with the exception of Montana. The most common minimum net worth requirement is \$100,000.

<sup>33</sup>See 12 U.S.C. § 4002. These time frames are codified in Regulation CC and generally depend on how the funds are deposited and the source and amount of funds deposited, among other things. See 12 C.F.R. pt. 229, subpt. B.

---

firms we spoke with voluntarily disclose the availability of funds and any limits on access in the terms and conditions provided to customers when they create their accounts. However, FTC recently settled with a fintech payment provider for delays in fund accessibility experienced by its users.<sup>34</sup> In its complaint, FTC charged that the firm had failed to disclose that these funds could be frozen or removed based on the results of the firm's review of the underlying transaction. As a result, consumers complained that at times, the firm delayed the withdrawal of funds or reversed the underlying transactions after initially notifying them that the funds were available.

## Fintech Lending

Consumers face risks associated with unclear terms and conditions regardless of whether they borrow from a traditional or fintech lender. For example, consumers could have difficulty understanding their repayment obligations or how those terms compare to terms offered by other lenders. However, the Truth in Lending Act requires lenders to provide consumers with standardized, easy-to-understand information about the terms of the loan and enables consumers to make claims against lenders for violating Truth in Lending Act requirements.<sup>35</sup>

Consumers also face risk of discrimination and unfair credit practices regardless of whether they borrow from a traditional or fintech lender. However, these risks may not be fully understood with fintech lenders that use alternative underwriting standards and consumer data—such as information on rent payments and college attended. For example, fintech firms assessing applicants' creditworthiness with criteria highly correlated with a protected class—such as race or marital status—may lead to a

---

<sup>34</sup>See *In the Matter of PayPal, Inc.*, File No. 162-3102 (March 5, 2018); see also PayPal, Inc.; Analysis To Aid Public Comment, 83 Fed. Reg. 9316 (March 5, 2018). The complaint also alleges weaknesses in the company's disclosures regarding privacy practices and its characterizations of its information security practices.

<sup>35</sup>The Truth in Lending Act and its implementing regulation, Regulation Z, require clear and conspicuous disclosures about credit terms and cost, generally in writing and in specific formats. See 12 C.F.R. § 1026.5(a). Consumers can make claims regarding Truth in Lending Act violations against a lender as well as any assignees of a loan, such as a licensed operator or an investor in the case of marketplace lending. See 15 U.S.C. § 1640.

---

disproportionate negative effect.<sup>36</sup> As with traditional lenders, federal fair lending laws, such as the Equal Credit Opportunity Act, apply to fintech lenders.<sup>37</sup> In addition, some fintech lenders have taken steps that aim to address this risk. For example, one fintech lender said it monitors the effect any changes to their underwriting models may have on fair lending risk.

Consumers face risk of harm due to inaccurate credit assessments, but these risks are also less understood with fintech lenders that use alternative data to underwrite loans. For example, inaccurate data or models used by a fintech lender could classify borrowers as higher credit risks than they actually are. This could result in those borrowers paying unnecessarily high interest rates and increasing their risk of default or could result in creditworthy borrowers being denied credit. Whereas the Fair Credit Reporting Act requires that borrowers have an opportunity to check and correct inaccuracies in credit reports, borrowers could face more challenges in checking and correcting alternative data that some fintech lenders use to make underwriting decisions because alternative data are not typically reflected in credit reports.<sup>38</sup> However, the Equal Credit Opportunity Act requires lenders, including fintech lenders, that deny credit to applicants to disclose the specific reasons for denial.<sup>39</sup> Alternatively, if the fintech lender's underwriting is too lax, loans could be made to borrowers who lack the ability to repay them.<sup>40</sup> Borrowers who default under these circumstances then face limited access to and higher prices for credit in the future.

---

<sup>36</sup>The Equal Credit Opportunity Act, which prohibits discrimination by race, gender, and certain other borrower characteristics (see 15 U.S.C. § 1691), has two principal theories of liability: disparate treatment and disparate impact. Disparate treatment occurs when a creditor treats an applicant differently based on a prohibited basis such as race or national origin. See 12 C.F.R. pt. 1002, supp. I, § 1002.4. Disparate impact occurs when a creditor employs facially neutral policies or practices that have an adverse effect or impact on a member of a protected class unless they meet a legitimate business need that cannot reasonably be achieved by means that are less disparate in their impact. See 12 C.F.R. pt. 1002, supp. I, § 1002.6.

<sup>37</sup>See 15 U.S.C. § 1691c.

<sup>38</sup>For example, according to Federal Reserve staff, when payment of rent or utility bills is factored into a model, consumers do not have a ready ability to review or correct inaccurate information.

<sup>39</sup>See 15 U.S.C. § 1691(d)(3).

<sup>40</sup>Faulty or overly lax credit administration practices may arise from the data, criteria, or model used in underwriting.

---

## Fintech Wealth Management

Consumers face risks of receiving unsuitable investment advice regardless of whether they obtain advice from a traditional or robo-adviser.<sup>41</sup> While a human adviser may be able to mitigate this risk by probing consumers for more information to assess needs, risk tolerance, or other important factors, a robo-adviser's ability to mitigate this risk may be based on a discrete set of questions to develop a customer profile.<sup>42</sup> In addition, advisers could make inaccurate or inappropriate economic assumptions, perhaps due to a failure to factor in changing economic conditions, which could result in flawed investment recommendations.<sup>43</sup> While human advisers may be able to mitigate this risk to some degree based on their ability to adjust to economic conditions, a robo-adviser's ability to mitigate this risk is based on whether its algorithm has been updated to reflect the most recent economic conditions. Because, as we discuss below, robo-advisers generally are required to comply with the same requirements as traditional investment advisers, customers of robo-advisers and traditional advisers receive the same protection from these risks.<sup>44</sup>

Consumers who use fintech services that provide an aggregated view of their accounts at other financial institutions could potentially be more exposed to losses due to fraud. If a consumer authorizes an account aggregator to access their financial accounts and grants the aggregator

---

<sup>41</sup>Robo-advisers can be investment advisers or broker dealers. FINRA rules govern broker dealers and SEC rules govern investment advisers.

<sup>42</sup>According to FINRA, consumer-specific suitability of robo-adviser tools depend on factors including whether a tool is designed to (1) collect and sufficiently analyze all of the required information about customers to make a suitability determination, (2) resolve conflicting responses to customer profile questionnaires, and (3) match customers' investment profiles to suitable securities or investment strategies. For more information, see Financial Industry Regulatory Authority, *Report on Digital Investment Advice* (Washington, D.C.: March 2016).

<sup>43</sup>For more information, see [GAO-17-361](#).

<sup>44</sup>For example, an investment adviser is a fiduciary whose duty is to serve the best interests of its clients and to provide only suitable investment advice; see also *Securities and Exchange Commission, IM Guidance Update: Robo-Advisers*, Issue No. 2017-02 (Washington, D.C.: February 2017). SEC has issued guidance recommending that robo-advisers disclose the risks associated with their reliance on customer input and underlying assumptions that their investment algorithms use. Securities and Exchange Commission, *IM Guidance Update: Robo-Advisers*, Issue No. 2017-02 (Washington, D.C.: February 2017). FINRA has also issued a report on robo-advisers to remind broker-dealers of their obligations under FINRA rules as well as to share effective practices among financial services firms related to digital wealth management. Financial Industry Regulatory Authority, *Report on Digital Investment Advice* (Washington, D.C.: March 2016).

---

authority to make transfers, the consumer may be liable for fraudulent transfers made. CFPB is studying risks associated with entities that rely on access to consumer financial accounts and account-related information, and has issued a related request for information (we address this issue later in this report).<sup>45</sup>

## Distributed Ledger Technology

DLT can be used to issue and distribute digital assets known as tokens to consumers and investors. Virtual currencies—tokens that are digital representations of value that are not government-issued legal tender—could pose some unique risks to consumers.<sup>46</sup> For example, the ability of virtual currency users to recover funds lost due to fraud or errors may be more limited than that of customers using traditional products like payment cards or bank transfers to make payments.<sup>47</sup> Whereas traditional transactions can be reversed to correct fraud or errors, many virtual currency transactions are designed to be irreversible.<sup>48</sup> Also, unlike storing dollars in a bank account, if a consumer stores their virtual currency in a mobile wallet, their wallet provider may disclaim responsibility for replacing virtual currency that is stolen. Further, CFPB's prepaid accounts rule, which will extend consumer protections to prepaid cards and mobile wallets with stored value, explicitly does not extend consumer protections to virtual currencies.<sup>49</sup> However, firms that transmit,

---

<sup>45</sup>Request for Information Regarding Consumer Access to Financial Records, 81 Fed. Reg. 83806. (Washington, D.C.: Nov. 22, 2016).

<sup>46</sup>Commodity Futures Trading Commission LabCFTC, *A CFTC Primer on Virtual Currencies* (Washington, D.C.: October 2017). See [GAO-14-496](#) for more information on risks related to DLT.

<sup>47</sup>CFPB, CFTC, and FTC have reported that virtual currencies may pose consumer risks including theft, error, volatility due to speculation, and limited fraud or error protections. See Commodity Futures Trading Commission, LabCFTC, *A CFTC Primer on Virtual Currencies*; Federal Trade Commission, *Staying current: Bitcoin and other cryptocurrencies* (Washington, D.C.: September 2014); and Consumer Financial Protection Bureau, *Consumer Advisory: Risks to Consumers Posed by Virtual Currencies* (Washington, D.C.: August 2014).

<sup>48</sup>While transactions on many public DLT networks are designed to be irreversible, in some cases it is possible for transactions to be reversed through consensus of network participants. For example, on July 20, 2016, Ethereum transactions were reversed by consensus to return funds stolen in a hack.

<sup>49</sup>See Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth In Lending Act (Regulation Z), 81 Fed. Reg. 83934, 83978 (Nov. 22, 2016). CFPB notes that as part of its broader administration and enforcement of the enumerated consumer financial protection statutes and title X of the Dodd-Frank Act, CFPB continues to analyze the nature of products or services tied to virtual currencies. See *id.*

---

exchange, hold, or otherwise control virtual currency may be subject to state consumer protection law.<sup>50</sup>

In addition to fraud and errors, consumers who use virtual currencies may face other risks of loss. Federal deposit insurance does not apply to virtual currency balances. As a result, according to FDIC staff, consumers could face losses if they store their virtual currencies with a mobile wallet firm that goes out of business unless the firm offers private insurance.<sup>51</sup> Further, if consumers store their virtual currency on their own and misplace or forget their account access information, they may lose access to their funds. Unlike bank accounts for which users can reset passwords or usernames, some wallets do not offer a way to reset such information. To help consumers address these risks, federal agencies and state regulators have issued documents publicizing practices that may help consumers use virtual currency more safely.<sup>52</sup>

Tokens—which may also function similarly to a security—could pose some unique risks to investors, and some investor protections may not be available. Token sales, sometimes known as initial coin offerings or ICOs, are being used by firms to raise capital from investors and may pose investor risks, including fraud and theft.<sup>53</sup> For example, one firm allegedly promised investors it would invest its token sale earnings in real estate, but instead allegedly defrauded investors of their investments.<sup>54</sup> Fraud and theft are risks of other securities offerings, and investors receive

---

<sup>50</sup>According to CSBS, depending on the services offered, certain virtual currency business models are also subject to state MSB laws. For more information, see Conference of State Bank Supervisors, *Model Regulatory Framework for Virtual Currencies* (Sept. 15, 2015). Available at <https://www.csbs.org/model-regulatory-framework-virtual-currencies>.

<sup>51</sup>Some virtual currency wallets offer private insurance for virtual currency held online. <https://support.coinbase.com/customer/portal/articles/1662379-how-is-coinbase-insured->

<sup>52</sup>Federal Trade Commission, *Staying current: Bitcoin and other cryptocurrencies*. Consumer Financial Protection Bureau, *Consumer Advisory: Risks to Consumers Posed by Virtual Currencies*. Congress of State Bank Supervisors and North American Securities Administrators Association, *Model State Consumer and Investor Guidance on Virtual Currency* (Apr. 13, 2014).

<sup>53</sup>Token sale investors generally provide funds to the token sale sponsor and in return receive virtual tokens that may represent ownership, royalties, or other rights. For more information, see SEC, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (Washington, D.C.: July 2017).

<sup>54</sup>Securities and Exchange Commission, *SEC Exposes Two Initial Coin Offerings Purportedly Backed by Real Estate and Diamonds* (Washington, D.C.: September 2017).

---

protections from these risks under the Securities Act of 1933 and the Securities Exchange Act of 1934 for token sales that meet SEC’s definition of a security.<sup>55</sup> However, these protections do not apply to investors who participate in token sales that do not meet the definition of a security. In December 2017, SEC issued a cease-and-desist order to one firm for failure to register their token sale with SEC.<sup>56</sup> In addition, SEC has reported that an investor’s ability to recover funds may be limited if key parties to token sales are located overseas or operating unlawfully.<sup>57</sup> To help investors address these risks, SEC and FINRA have issued documents publicizing risks of token sale investment.<sup>58</sup>

Tokens traded on a platform may also be considered commodities and may pose investor risks including fraud and theft. Platforms that facilitate leveraged, margined, or financed trading of tokens may be subject to a requirement to register with the CFTC. To help investors understand tokens, CFTC has issued a report publicizing potential risks of virtual currencies and clarifying cases in which investors may be at risk because CFTC does not have oversight authority. For example, virtual currency and token exchanges that conduct certain spot or cash market transactions but do not use leverage, margin, or financing are not

---

<sup>55</sup>Securities and Exchange Commission, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, Exchange Act Release No. 81207 (July 25, 2017).

<sup>56</sup>Securities and Exchange Commission, *Company Halts ICO after SEC Raises Registration Concerns* (Washington, D.C.: December 2017).

<sup>57</sup>Securities and Exchange Commission, Office of Investor Education and Advocacy, *Investor Bulletin: Initial Coin Offerings* (Washington, D.C.: July 2017).

<sup>58</sup>Securities and Exchange Commission, Office of Investor Education and Advocacy, *Investor Bulletin: Initial Coin Offerings*; and *Investor Alert: Ponzi Schemes Using Virtual Currencies* (Washington, D.C.: July 2013). Financial Industry Regulatory Authority, *Investor Alerts: Initial Coin Offerings: Know Before You Invest* (Washington, D.C.: August 2017), *Bitcoin: More than a Bit Risky* (Washington, D.C.: May 2014), and *Don’t Fall for Cryptocurrency-Related Stock Scams* (Washington, D.C.: December 2017).

---

required to follow all of the rules that regulated exchanges are required to follow.<sup>59</sup>

DLT applications may pose other unknown risks compared to the technologies and processes they replace, given that the technology is in the early stages of development. For example, CFTC and the Federal Reserve have identified cybersecurity and operational risks as potential risks of DLT. FDIC officials said that finality of a transaction under a DLT settlement may potentially raise legal challenges. Also, applications of DLT that depend on consensus for validating transactions are vulnerable to a “51 percent attack,” which could defraud consumers by revising their transactions or sending fraudulent payments.<sup>60</sup> However, according to market observers, such an attack is unlikely and has not been carried out.

---

### Fintech Products Can Pose Other Risks to Consumers; Risks to the Broader Financial System Are Unclear

Consumers face the risk of financial loss due to data breaches regardless of whether they use a traditional or fintech firm, and these breaches could undermine the financial system by eroding consumer trust in financial institutions. Similar to traditional products and services that collect sensitive consumer information and are connected to the Internet, fintech products and services may be vulnerable to cyberattack and can pose data security risks. In addition, one market observer we interviewed told us that hackers may target these new fintech firms before their security systems are mature.

---

<sup>59</sup>See Commodity Futures Trading Commission, LabCFTC, *A CFTC Primer on Virtual Currencies*. CFTC has also taken an enforcement action against one firm that promised investors it would place their investments in a bitcoin commodity fund but instead allegedly defrauded investors of their investments. See *Commodity Futures Trading Commission v. Gelman Blueprint, Inc. and Nicholas Gelfman*, Case No. 1:17-cv-07181 (S.D.N.Y. Sept. 21, 2017) (complaint); CFTC, *CFTC Charges Nicholas Gelfman and Gelfman Blueprint, Inc. with Fraudulent Solicitation, Misappropriation, and Issuing False Account Statements in Bitcoin Ponzi Scheme* (Washington, D.C.: September 2017). In June 2016, CFTC brought an enforcement action against a Hong Kong-based bitcoin exchange for offering illegal commodity transactions in bitcoin and other virtual currencies, and for failing to register as a Futures Commission Merchant. See *In the matter of BFXNA Inc. d/b/a Bitfinex*, CFTC Docket No. 16-19 (June 2, 2016); CFTC, *CFTC Orders Bitcoin Exchange Bitfinex to Pay \$75,000 for Offering Illegal Off-Exchange Financed Retail Commodity Transactions and Failing to Register as a Futures Commission Merchant* (Washington, D.C.: June 2016).

<sup>60</sup>A 51 percent attack is when a party or parties who control the majority of the resources contributed to the consensus mechanism of a distributed ledger fraudulently revise recently settled transactions on the ledger, prevent current and future transactions from being completed, or double-spend tokens.



---

However, according to literature we reviewed and fintech firms and market observers we interviewed, some fintech firms have adopted technologies or practices designed to mitigate security risks. For example, new fintech firms can use the latest information technology systems to secure their products instead of having to update older systems. Additionally, as discussed above, some fintech firms use new techniques and leverage mobile device features to enhance data security, and one fintech firm said that it also uses technology that contacts clients if a data breach issue arises.<sup>61</sup> Like traditional financial institutions, rules and guidelines implementing the Gramm-Leach-Bliley Act (GLBA) generally require fintech firms to secure customer information.<sup>62</sup> In addition, some regulators have issued guidance to consumers publicizing practices that help avoid security problems when using fintech products.<sup>63</sup> Regulators have also issued guidance to businesses including fintech firms that recommends that they adopt policies and procedures that address the prevention and detection of, and response to, cybersecurity threats.<sup>64</sup> For example, the New York State Department of Financial

---

<sup>61</sup>For example, firms may use data encryption, secure elements of mobile hardware, and tokenization to help protect the transmission of consumer data.

<sup>62</sup>GLBA requires FTC and certain other federal agencies to establish standards for financial institutions relating to administrative, technical, and physical information safeguards. See 15 U.S.C. § 6801. GLBA defines financial institution as any institution the business of which is engaging in financial activities as described in the Bank Holding Company Act of 1956, including lending, transferring funds, and providing financial services (see 12 U.S.C. 1843(k)), but does not include entities subject to CFTC jurisdiction under the Commodity Exchange Act. See 15 U.S.C. § 6809(3). As part of its implementation of GLBA, FTC issued the Safeguards Rule, which requires financial institutions under FTC jurisdiction to have measures in place to secure customer information and ensure that affiliates and service providers also safeguard this information. See 16 C.F.R. pt. 314. The rule applies to many companies of all sizes that are significantly engaged in financial products and services, including consumer reporting agencies.

<sup>63</sup>See for example, Federal Trade Commission, *An identity thief stole my phone! and Payments you didn't authorize could be a scam*. Federal Communications Commission, *Consumer Guide: Mobile Wallet Services Protection*. Consumer Financial Protection Bureau, *Watch accounts closely when account data is hacked and report suspicious charges* (Washington, D.C.: January 2014). Securities and Exchange Commission, Office of Investor Education and Advocacy, *Updated Investor Bulletin: Protecting Your Online Investment Accounts from Fraud* (Washington, D.C.: April 2017). Commodity Futures Trading Commission, LabCFTC, *A CFTC Primer on Virtual Currencies*.

<sup>64</sup>Federal Trade Commission, *Data Breach Response: A Guide for Business* (Washington, D.C.: September 2016); and *Start with Security: A Guide for Business* (Washington, D.C.: June 2015). Securities and Exchange Commission, *Cybersecurity Guidance, IM Guidance Update No. 2015-02* (Washington, D.C.: April 2015).

---

Services requires regulated entities to meet cybersecurity requirements outlined in regulation.<sup>65</sup>

Some fintech firms may also pose privacy concerns because they may collect more consumer data than traditional firms. For example, fintech lenders that use alternative data in underwriting may have sensitive information about consumers' educational background, mobile phone payments, or other data. One fintech firm we spoke with requires consumers to provide additional data, such as what a payment is for, in order to make peer-to-peer payments. Some data aggregators may hold consumer data without disclosing what rights consumers have to delete the data or prevent the data from being shared with other parties. A leak of these or other data held by fintech firms may expose characteristics that people view as sensitive. GLBA generally requires fintech firms and traditional financial institutions to safeguard nonpublic personal information about customers.<sup>66</sup> According to literature we reviewed and fintech firms and market observers we interviewed, as with data security, some fintech firms use new technologies or mobile device features to mitigate data privacy risks. In addition, some regulators have issued guidance to consumers publicizing practices that help maintain privacy when using online products and services, including those provided by fintech firms.<sup>67</sup> Regulators have also issued GLBA guidance to businesses including fintech firms recommending that they adopt policies and procedures to prevent, detect, and address privacy threats.<sup>68</sup>

---

<sup>65</sup>New York State Department of Financial Services, *Cybersecurity Requirements for Financial Services Companies*, 23 NYCRR 500 (March 2017).

<sup>66</sup>GLBA restricts, with some exceptions, the disclosure of nonpublic information by companies defined as "financial institutions." See 15 U.S.C. § 6801.

<sup>67</sup>Securities and Exchange Commission, *Online Brokerage Accounts: What You Can Do to Safeguard Your Money and Your Personal Information* (Washington, D.C.: February 2009). Federal Trade Commission, *Understanding Mobile Apps* (Washington, D.C.: February 2017); and *How to Keep Your Personal Information Secure* (Washington, D.C.: July 2012). Financial Industry Regulatory Authority, *Investor Alerts: "Phishing" and Other Online Identity Theft Scams: Don't Take the Bait* (Washington, D.C.: February 2012).

<sup>68</sup>Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Washington, D.C.: October 2016); and *How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act* (Washington, D.C.: July 2002). Consumer Financial Protection Bureau, *Privacy of Consumer Financial Information – Gramm-Leach-Bliley Act (GLBA) examination procedures* (Washington, D.C.: October 2016).

---

Similar to traditional products and services, fintech products may be used to facilitate illicit activities, including money laundering, terrorist financing, and evading sanctions program requirements. For example, in 2015, the Financial Action Task Force (FATF) reported that new payment methods pose an emerging terrorist finance vulnerability because users can access these methods from anywhere in the world and it is difficult for enforcement agencies to identify the beneficiary.<sup>69</sup> However, FATF found that the extent to which terrorist groups actually exploit these technologies is unclear and said that enforcement agencies should monitor these risks for developments.<sup>70</sup> Further, FATF has stated that fintech innovations provide an opportunity to bring anti-money laundering efforts into the 21st century by reducing dependency on cash and informal systems and making it easier for authorities to detect and follow illicit financial flows. Relevant laws that prohibit financial crimes apply to fintech products. For example, the Bank Secrecy Act (which established reporting, recordkeeping, and other anti-money laundering requirements) and economic sanctions programs (which create economic penalties in support of U.S. policy priorities) apply to all financial firms that transmit money regardless of whether they use traditional or fintech products.<sup>71</sup>

Finally, market observers have questioned whether fintech activities could create risks to overall financial stability, but many have said such risks are relatively minimal due to fintech firms' small market presence. While direct or indirect linkages between large financial institutions could lead financial problems at one firm to create similar problems for other firms that can undermine financial stability, studies by regulators in various countries and international organizations found that fintech firms have not generally reached a level of interconnectedness where their financial distress would threaten the stability of other financial system

---

<sup>69</sup>FATF is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

<sup>70</sup>Financial Action Task Force, *Emerging Terrorist Financing Risks* (Paris, France: October 2015).

<sup>71</sup>For more information on the Bank Secrecy Act and U.S. sanctions program requirements, including agency responsibilities, see GAO, *Financial Institutions: Fines, Penalties, and Forfeitures for Violations of Financial Crimes and Sanctions Requirements*, [GAO-16-297](#) (Washington, D.C.: Mar. 22, 2016).

---

participants.<sup>72</sup> For example, the Bank for International Settlements and the Financial Stability Board reported that in 2015 fintech accounted for 2 percent of new credit in the United States.<sup>73</sup> Additionally, after assessing virtual currencies, the European Central Bank concluded in a November 2017 report that virtual currencies were not a threat to financial stability due to their limited connection with the real economy, their low volume traded, and the lack of wide user acceptance.<sup>74</sup>

However, the Financial Stability Board and other market observers have noted that fintech firms could potentially affect financial stability in both positive and negative ways as the activities and firms evolve.<sup>75</sup> For example, fintech firms could help decentralize and diversify the financial services market, and they could diversify exposure to risk by increasing access to financial services for consumers and small businesses. On the other hand, providers could potentially also increase risks to financial stability. For example, robo-advisers could amplify swings in asset prices if their risk models rely on similar algorithms, making the portfolio allocation methods of robo-advisers more highly correlated than those of traditional advisers, although according to the Financial Stability Oversight Council, this risk could also arise if traditional advisers follow similar allocation strategies. Similarly, according to the Financial Stability Board, fintech lenders could potentially amplify swings in credit availability if the investors that fund many marketplace lending products are more willing to fund loans during market upturns or less willing to fund loans

---

<sup>72</sup>Financial Stability Board, *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention* (June 2017). National Economic Council, *A Framework for Fintech* (January 2017). European Central Bank, *Virtual Currency Schemes* (October 2012). Bank for International Settlements and Financial Stability Board, *FinTech Credit; Market structure, business models and financial stability implications* (May 2017). International Organization of Securities Commissions, *IOSCO Research Report on Financial Technologies (Fintech)* (February 2017). Congressional Research Service, *Marketplace Lending: Fintech in Consumer and Small-Business Lending* (Washington, D.C.: September 2016).

<sup>73</sup>Bank for International Settlements and Financial Stability Board, *FinTech Credit*.

<sup>74</sup>Virtual currencies could threaten financial stability in the future if their use grows. For more information, see Randal Quarles, *Thoughts on Prudent Innovation in the Payment System* (speech delivered at the 2017 Financial Stability and Fintech Conference, sponsored by the Federal Reserve Bank of Cleveland, the Office of Financial Research, and the University of Maryland's Robert H. Smith School of Business (Washington, D.C.: November 2017).

<sup>75</sup>Financial Stability Board, *Financial Stability Implications from FinTech*. Bank for International Settlements and Financial Stability Board, *FinTech Credit*.

---

during market downturns. To help balance these potential benefits and risks, the Financial Stability Board recommended that international bodies and national authorities continue to monitor the issues and consider the effects of fintech in their risk assessments and regulatory frameworks.

---

## Fintech Firms' Compliance with Applicable Laws Is Subject to Varied Federal Oversight

The extent to which fintech firms are subject to federal oversight of their compliance with applicable consumer or other laws varied. Fintech firms that offer investment advice typically register with and are subject to examinations by federal securities regulators. Some fintech firms providing payments or loans that have partnered with federally regulated banks or credit unions may receive indirect oversight from federal financial regulators as part of their efforts to ensure that their regulated entities are adequately managing the risks of these arrangements. Nonpartnered fintech firms would not typically be subject to routine examinations by a federal financial regulator but would instead be subject to state regulatory oversight and enforcement. While fintech firms and financial institutions are subject to different degrees of routine federal oversight, we found that indications of fintech firms causing widespread harm were limited as they were subject to fewer complaints than large financial institutions.

---

## Fintech Firms Providing Investment Advice Are Subject to the Same Oversight as Traditional Financial Institutions

Fintech robo-advisers offering wealth management advice would generally be subject to the same federal and state oversight as traditional investment advisers. Under the Investment Advisers Act of 1940 and state securities laws, any entity or individual that offers investment advice for compensation generally must register as an investment adviser—with SEC or states—and adhere to various reporting and conduct requirements.<sup>76</sup> When providing advice, investment advisers—traditional or fintech—are considered fiduciaries to their clients, which means they owe a duty of care and loyalty to their clients, and they must disclose all actual or potential conflicts of interest, and act in their clients' best interest. To review for compliance with this standard and other applicable

---

<sup>76</sup>See 15 U.S.C. §§ 80b-3 – 80b-3a. Generally, states regulate investment advisers that have less than \$100 million in assets under management, that operate in fewer than 15 states, or that do not qualify for registration with SEC. See 15 U.S.C. § 80b-3a(a). In addition, if digital wealth management advisers provide investment advice exclusively through interactive websites, subject to certain exceptions, then the advisers may choose to register with SEC. See SEC rule 203A-2 Exemption for Certain Investment Advisers Operating Through the Internet for exemptions related to robo-advisers. See SEC rule 203A-2.

---

requirements, staff from SEC and state securities regulators conduct examinations of registered investment advisers.<sup>77</sup> Specifically, state regulators are responsible for conducting examinations of investment advisers that operate in fewer than 15 states and hold client assets under management of less than \$100 million. However, according to staff from the North American Securities Administrators Association—a membership organization for state, provincial, and territorial securities administrators in the United States, Canada, and Mexico—no robo-adviser firms were solely regulated by the states as of October 2017.<sup>78</sup>

---

### Fintech Firms That Partner with Financial Institutions May Be Subject to Indirect Federal Financial Regulator Oversight

Some fintech firms may be subject to indirect federal oversight as part of relationships they have entered into with regulated financial institutions. If fintech firms partner with federally-regulated financial institutions, such as a bank or credit union, federal financial regulators may conduct examinations of the regulated financial institution that could include some review of the extent to which the fintech firm may affect the partner financial institution's adherence to relevant regulations through the services provided to the financial institution. Regulators conduct these examinations in order to assess the risk to the regulated institution because the failure of the fintech firm to follow such laws could expose the bank or credit union to financial or other risks.

As part of the indirect oversight of fintech firms, the financial institution would be expected by its regulators, under various third-party guidance issuances by these regulators, to ensure that any risks to the institution resulting from the relationship with the fintech firm are assessed and

---

<sup>77</sup>According to SEC's 2018 National Exam Program Priorities, it will continue to examine investment advisers—including robo-advisers—that offer investment advice through automated or digital platforms. Examinations will focus on registrants' compliance programs, including oversight of computer program algorithms that generate recommendations, marketing materials, investor data protection, and disclosure of conflicts of interest.

<sup>78</sup>While no robo-adviser firm fitting the definition in this report was identified, there are state-registered investment advisers that use fintech as part of their business models and may be considered to be a robo-adviser by the relevant state securities regulatory authority, according to North American Securities Administrators Association staff.

---

mitigated.<sup>79</sup> Among other things, banks and credit unions should conduct due diligence on potential third-party partners, including having a process within the institution for managing the risks posed to their institution by the third party. For example, OCC third-party guidance states that banks should adopt risk management processes that are commensurate with the level of risk and complexity of the third-party relationship.<sup>80</sup> These processes include establishing risk-mitigating controls, retaining appropriate documentation of the bank's efforts to obtain information on third parties, and ensuring that contracts meet the bank's compliance needs.

Although fintech firms partnering with federally regulated institutions would be expected to follow the practices in this guidance, the extent to which they would be overseen by a federal financial regulator was limited. For example, FDIC and OCC staff told us that they had examined a fintech firm that provides financial account aggregation services to regulated institutions. This review focused on the fintech firm's data security rather than its activities with consumers. FDIC staff also said they conducted exploratory discussions with some fintech lenders, but these firms were not part of their technology service provider examination program. However, as of November 2017, FDIC and OCC staff noted that they had not completed examinations of fintech firms within our scope. NCUA staff noted that NCUA does not have authority to examine services provided to credit unions by third-party service providers. In order to examine any services provided to credit unions, NCUA must rely on credit unions voluntarily providing information on the third-party service provider.<sup>81</sup> However, NCUA's staff noted some of their examiners had accompanied state regulators in an examination that involved a credit union's partnership with a fintech payments firm.

---

<sup>79</sup>Third-party relationships include activities that involve networking arrangements, merchant payment processing services, and services provided by affiliates and subsidiaries; joint ventures; and other business arrangements in which a bank has an ongoing third-party relationship or may have responsibility for the associated records. See, e.g., Office of the Comptroller of the Currency, *Third-Party Relationships: Risk Management Guidance*, OCC Bulletin 2013-29, Oct. 30, 2013.

<sup>80</sup>Office of the Comptroller of the Currency, *Third-Party Relationships: Risk Management Guidance*, OCC Bulletin 2013-29, Oct. 30, 2013.

<sup>81</sup>We have previously submitted a matter for consideration to Congress for it to consider granting NCUA this authority. See GAO, *Cybersecurity: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information*, [GAO-15-509](#) (Washington, D.C.: July 2, 2015). As of December 2017, Congress has not acted on this matter.

---

## Other Fintech Firms Are Not Routinely Overseen by Federal Financial Regulators, but Are Subject to State Oversight

Fintech firms not providing investment advice or partnered with federally-regulated financial institutions would be subject to routine oversight by a federal regulator only under certain circumstances. For example, CFPB could examine some fintech firms as a result of its examination authorities. Specifically, it has supervisory authority over certain nondepository institutions, including mortgage lenders and servicers, payday and student loan providers, and “larger participants” in consumer financial product and service markets, which could include fintech providers.<sup>82</sup> CFPB has conducted or plans to conduct examinations of fintech firms that meet the agency’s definition of “larger participants” in sectors for which they have designated such participants.<sup>83</sup> For example, according to CFPB staff, it has conducted a stand-alone examination of a fintech payments company that provides international remittances, and it has scheduled an examination of a fintech lender that provides student loans. As of October 2017, it had not defined other “larger participants” specifically for other markets in which fintech firms may be active, but it is considering a proposed rule to supervise larger participants in the personal loan markets, which might include larger fintech lenders.<sup>84</sup> CFPB may also conduct examinations of individual companies that it determines

---

<sup>82</sup>According to CFPB officials, CFPB has examination authority based on 6 mechanisms: 1) insured depository institutions and insured credit unions with more than \$10 billion in assets, as well as affiliates of the insured depository institutions and credit unions; 2) certain types of nonbanks as provided by statute (including mortgage lenders and servicers and payday lenders); 3) larger participants of markets for other consumer financial products or services as defined by CFPB rulemaking; 4) third-party service providers to any of nonbank entities subject to CFPB supervisory authority, to any of the banking institutions with more than \$10 billion in assets, or to a substantial number of banking institutions with assets of \$10 billion or less; 5) individual companies that CFPB determines pose risks to consumers, as identified in public orders; and 6) certain examination authorities with respect to banking institutions with assets of \$10 billion or less. See 12 U.S.C. §§ 5514-5516.

<sup>83</sup>See 12 U.S.C. § 5514(a). Dodd-Frank Act section 1024 requires CFPB to define, by rule, the “larger participants of a market for consumer financial products or services before it can supervise the larger participants’ activities. See Pub. L. No. 111-203, § 1024(a)(1)(B); 124 Stat. 1376, 1987 (2010) (codified at 12 U.S.C. § 5514(a)(1)(B)). For example, in December 2014, CFPB’s final rule on larger participants of the international money transfer market (i.e. international remittances) became effective. The rule defines larger participants in the international money transfer market as any nonbank covered person that “has at least one million aggregate annual international money transfers.” See 12 C.F.R. § 1090.107(b). As of November 2017, CFPB has issued final rules defining larger participants of the following markets: international money transfer, automobile financing, student loan servicing, consumer debt collection, and consumer reporting.

<sup>84</sup>Semiannual Regulatory Agenda, 82 Fed. Reg. 40386, 40387 (Aug. 24, 2017).



---

pose risks to consumers, as identified in public orders. Furthermore, CFPB's supervisory authority also extends to third-party service providers of nondepository institutions overseen by the agency.

Fintech firms may also be subject to examinations related to their compliance with anti-money laundering laws and related requirements. FinCEN, which is responsible for administering federal anti-money laundering laws, has authority to examine any fintech firms conducting money transmission, according to Treasury officials. These firms would be required to comply with the applicable anti-money laundering and counter-terrorist financing requirements, including registering with FinCEN, establishing anti-money laundering programs, and reporting suspicious activities to FinCEN. However, FinCEN delegates routine anti-money laundering examinations of federally-chartered or registered financial institutions to the federal financial institution regulators. In other cases, firms subject to anti-money laundering requirements, including fintech payments or lending firms, could be examined by state regulators and the Internal Revenue Service.

Fintech firms not subject to routine federal supervisory oversight would instead generally be subject to state oversight. As of October 2017, 49 states, as well as the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands, required entities that provide money transfer services—which may include some fintech payments firms—to obtain licenses to conduct such activities in their jurisdictions according to documents from state regulator associations and CSBS staff.<sup>85</sup> In addition, all states and the District of Columbia required lending licenses for consumer lenders operating in their states, according to CSBS staff.<sup>86</sup>

---

<sup>85</sup>FinCEN defines Money Service Businesses as any person doing business, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities: currency dealer or exchanger; check casher; issuer of traveler's checks, money orders or stored value; money transmitter; or U.S. Postal Service. For complete regulatory definition, see 31 CFR 1010.100(ff). Similarly, according to CSBS staff, 36 states define electronic money transmitting as accepting or instructing to be delivered currency, funds, or other value, such as stored value, that substitutes for currency to another location or person by electronic means, such as mobile-to-mobile payments. This definition also likely covers all mobile wallet providers, according to CSBS staff.

<sup>86</sup>All states and the four other jurisdictions required licenses for mortgage activities, but we did not include mortgage activities in the scope of this report. According to CSBS staff, all states and four other U.S. jurisdictions have consumer lending licenses. While some jurisdictions only license payday or small dollar lending, other jurisdictions license a broader class of consumer lending.

---

Furthermore, some states have created or provided guidance on licensing statutes in order to include virtual currencies.<sup>87</sup> For example, in 2015 New York finalized a new license for virtual currency businesses under New York's financial services law.<sup>88</sup>

State regulators in these jurisdictions conduct examinations of the firms that hold licenses to assess their compliance with safety and soundness and various other requirements.<sup>89</sup> In addition, CSBS staff stated that as of February 2018, approximately 37 states authorize state regulators to examine banks' third-party service providers—which could include fintech companies.

According to state regulators we interviewed in Illinois, New York, and California, their agencies use the same approach to regulate and examine fintech firms and traditional financial institutions providing similar services. Furthermore, according to state regulatory associations and some state regulatory agencies, fintech firms such as money transmitters undergo regular supervision through on-site examinations to monitor compliance with federal and state capital, liquidity, and consumer protection requirements.<sup>90</sup> For example, Money Transmitters Regulators

---

<sup>87</sup>State governments have taken different approaches to licensing requirements for digital currencies. According to Coin Center, as of October 2017, only New York has a formal virtual currency licensing scheme. Other states have broadened their money transmission licensing to include digital currencies through either legislation or guidance. Texas, Kansas, and Tennessee have narrowed money transmitter licensing guidance to include only virtual currency companies that also deal in traditional currencies, according to a Coin Center report.

<sup>88</sup>New York's BitLicense regulation requires any New York business that transmits or receives virtual currency to have a license. The regulation also has capital; liquidity; bank account and clear ownership requirements, according to New York State Department of Financial Services staff.

<sup>89</sup>Federal regulators—such as FinCEN, NCUA and FDIC—may participate in joint examinations with state regulators. For example, NCUA noted that it participates in joint examinations of state-chartered, federally-insured credit unions, and occasionally credit union service organizations, but cannot take enforcement actions due to its lack of vendor authority. Furthermore, CSBS staff noted that when states solely conduct examinations regulators can subject fintech companies—such as licensed money lenders—to full examination, instead of the limited examination authority outlined by the Bank Service Company Act.

<sup>90</sup>According to two surveys of money transmitter licensing in the United States and its territories, 49 states; the District of Columbia; Guam; Puerto Rico; and the U.S. Virgin Islands have money transmitter licenses. Montana is the only U.S. jurisdiction that does not have a money transmitter license.

---

Association staff said that state regulators examine MSBs at least every 3 years depending on risk assessment and previous examination record, and that state examinations cover federal and state laws, including data security and anti-money laundering requirements. Similarly, staff from one state regulator noted that they conduct consumer protection examinations of direct lenders and take enforcement action if they identify potential violations. CSBS staff noted that state requirements do not differ for fintech firms because the requirements and examinations are activity-based. For example, most states have anti-money laundering requirements within their money transmitter license laws.<sup>91</sup> Due to state anti-money laundering examination cycles, CSBS staff stated that MSBs licensed in 40 or more total states experience an examination at least once every 14 months.

---

## Fintech Firms Can Be Subject to Enforcement Actions by Federal and State Regulators

Outside of examinations, fintech firms that violate federal and state regulations can be subject to enforcement actions by federal and state agencies with such authorities. The OCC, Federal Reserve, and FDIC may have enforcement jurisdiction over fintech firms when the fintech firm is an “institution affiliated party” under the Federal Deposit Insurance Act or a service provider under the Bank Service Company Act.<sup>92</sup> In addition, CFPB can take enforcement action against institutions under its jurisdiction for noncompliance with federal consumer protection laws. For example, in 2016, CFPB used its unfair, deceptive, or abusive acts or practices authorities to investigate and issue a consent order against a fintech firm operating an online payment system, which CFPB determined had made deceptive data security claims to customers.<sup>93</sup> FTC can also take enforcement actions against fintech firms not registered or chartered as a bank for violations of any federal consumer laws FTC enforces, including the FTC Act’s prohibition against unfair or deceptive acts or practices.<sup>94</sup> For example, in 2015, FTC took action against the providers

---

<sup>91</sup>According to CSBS, Montana, New Jersey, and Wisconsin do not have licensing requirements related to anti-money laundering.

<sup>92</sup> See Federal Deposit Insurance Act section 3, 12 U.S.C. § 1813(u), and Bank Service Company Act, 12 U.S.C. § 1867(c)(1).

<sup>93</sup>See *In the Matter of Dwolla, Inc.*, File No. 2106-CFPB-0007 Mar. 2, 2016. For more information on CFPB’s 2016 consent order with Dwolla, see <https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/>. Dwolla has since changed its business model.

<sup>94</sup>See 15 U.S.C. § 45.

---

of a smartphone application, alleging that they deceived consumers and installed hidden malicious software code to generate virtual currencies for the providers without consumer permission.<sup>95</sup> It can also bring enforcement action against non-bank service providers that maintain or process customer information under its GLBA authority.<sup>96</sup>

Other federal entities can pursue enforcement action against fintech firms. The Department of the Treasury's Office of Foreign Assets Control can take action against fintech firms that violate U.S. sanctions regulations. In addition, FinCEN can also pursue enforcement measures against fintech firms that transmit funds—such as certain fintech payment and lending firms—due to its authority to enforce compliance with the Bank Secrecy Act's anti-money laundering and prevention of terrorist financing provisions.<sup>97</sup> For example, FinCEN took enforcement action in May 2015 against the fintech firm Ripple—a company that allows users to make peer-to-peer transfers in any currency using a DLT-enabled process—for violating anti-money laundering requirements through its sale of virtual currency.<sup>98</sup> In 2016, CFTC brought an enforcement action against a Hong Kong-based fintech firm for offering illegal off-exchange financed retail commodity transactions in bitcoin and other

---

<sup>95</sup>See *Federal Trade Commission v. Equiliv Investments*, Case No. 2:2015-cv-04379-KM (D.N.J. June 24, 2015). FTC pursued enforcement action against Equiliv Investments, whose “Prized” application contained malware that took control of the mobile device and used its computing resources to “mine” for virtual currencies. For FTC's press release of its enforcement action against Equiliv Investments, see <https://www.ftc.gov/news-events/press-releases/2015/06/app-developer-settles-ftc-new-jersey-charges-it-hijacked>. For more information on mining, including relevant FinCEN guidance, see [GAO-14-496](#).

<sup>96</sup>See 15 U.S.C. § 6805; see also 16 C.F.R. pt. 234.

<sup>97</sup>For example, in 2015, FinCEN assessed a \$700,000 civil money penalty against one fintech payment provider for operating as an MSB and selling virtual currency without registering with FinCEN and for failing to have an adequate anti-money laundering / counter-terrorist financing program in place. *In the matter of Ripple Labs Inc.*, Assessment of Civil Money Penalty, FinCEN No. 2015-05 (May 5, 2015). Similarly, in 2015, PayPal agreed to pay \$7.7 million to settle potential civil liability for apparent violations of multiple U.S. sanctions regulations in response to an investigation by Treasury's Office of Foreign Assets Control. See *In re PayPal, Inc.*, Settlement Agreement, MUL-762365 (Mar. 23, 2015).

<sup>98</sup>See *In the matter of Ripple Labs Inc.*, Assessment of Civil Money Penalty, FinCEN No. 2015-05 May 5, 2015. For more information on FinCEN's 2015 enforcement action against Ripple, see <https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual>. Ripple has since changed its business model and is no longer consumer-facing.

---

cryptocurrencies, and for failing to register as a futures commission merchant.<sup>99</sup>

Finally, state regulators can also take enforcement action against financial institutions and fintech firms that violate state data security or consumer protection laws. In addition, state attorneys general may bring actions against fintech companies through consumer protection and deceptive trade practice acts, according to the National Association of Attorneys General.<sup>100</sup>

---

### In Some Cases, Fintech Firms May Not Be Subject to Financial Regulator Oversight

Some fintech companies may not be subject to any federal or state financial oversight if they do not meet federal or state definitions of a money service or other regulated business. For example, some fintech payments firms—such as certain mobile wallet providers—might not be subject to state or federal money service business requirements because their role in the payment process does not specifically involve transmitting money, according to state and federal regulators. One mobile wallet provider claimed that it is not subject to federal financial regulatory oversight because it does not transfer funds or authorize transactions, but instead facilitates the transfer of customer data as part of the credit card or debit card networks; it also does not retain any of its consumers' personal data, including data on purchase content, location, or dollar amount.

---

<sup>99</sup>See *In the matter of BFXNA Inc. d/b/a BitFinex*, Order Instituting Proceedings Pursuant To Sections 6(c) And 6(d) of The Commodity Exchange Act, As Amended, Making Findings And Imposing Remedial Sanctions, CFTC Docket No. 16-19 (June 2, 2016). For more information on CFTC's enforcement actions, see CFTC Press Release No. 7380-16, CFTC Orders Bitcoin Exchange Bitfinex to Pay \$75,000 for Offering Off-exchange Financed Retail Commodity Transactions and Failing to Register as a Futures Commission Merchant (June 2, 2016) and CFTC Press Release No. 7614-17, CFTC Charges Nicholas Gelfman and Gelfman Blueprint, Inc. with Fraudulent Solicitation, Misappropriation, and Issuing False Account Statements in Bitcoin Ponzi Scheme (Sept. 21, 2017).

<sup>100</sup>Consumer protection offices in Connecticut, Hawaii, and Utah have a primary or joint enforcement role with their states' Attorneys General, according to the National Association of Attorneys General.

---

## Indications of Fintech Activities Creating Widespread Consumer Harm Appear Limited Compared to Traditional Providers

Available regulatory data show that the number of consumer complaints against fintech activities appears modest compared to traditional providers. For example, although our analysis of the CFPB's consumer complaint database has limitations in assessing risk, the number of published complaints submitted against several prominent fintech firms from April 2012 through September 2017 included in this database was generally low, when compared to select large financial institutions.<sup>101</sup> Our analysis showed that for 13 large firms offering fintech payments, lending, investment advice, financial account aggregation, or virtual currencies, only 5 of the firms had complaints in the CFPB database, with 4 having received fewer than 400 complaints.<sup>102</sup> The largest number of published complaints had been submitted against a large fintech payment provider with over 3,500 published complaints. Further, the number of published complaints submitted against the fintech payment provider was relatively small compared to the number of published complaints submitted against other, often larger financial institutions. For example, our analysis showed that 10 large financial institutions each received between approximately 14,300 and 67,300 total complaints April 2012 through September 2017.<sup>103</sup>

---

<sup>101</sup> Although complaints submitted against companies indicates that these companies may be harming consumers, CFPB does not verify that the complaints are true and a lack of complaints does not guarantee that a company is not harming consumers, because harm can happen without consumers reporting it. In addition to searching CFPB's consumer complaint database for published complaints submitted against a large fintech payment provider, we also searched for published complaints submitted against other prominent fintech firms from April 2012 through September 2017. We identified between approximately 100 to approximately 400 complaints against three fintech lending firms, as well as, a virtual currency exchange company—an average of 1 to 6 complaints per month. We also identified zero published complaints against other prominent fintech payments firms, fintech lenders, robo-advisers, and data aggregators. However, agencies noted that number of complaints might not correlate with the existence or non-existence of a consumer problem.

<sup>102</sup> We analyzed the CFPB database to identify publicly available complaints against the following large firms: Apple; Betterment; Coinbase; Facebook; Google; Lending Club; Mint; PayPal; Prosper; Ripple; SoFi; Wealthfront; and Yodlee.

<sup>103</sup> In March 2017, CFPB identified these 10 companies as the 10 companies for which they had received the most complaints from September through December 2016. CFPB, *Monthly Complaint Report*, vol. 21, March 2017. We used CFPB's consumer complaint database to analyze the number of complaints they received from April 2012 through September 2017. Financial institutions may offer products and services not offered by a single fintech firm. Therefore, some consumer complaints could be about issues outside of our scope. For example, 3 companies received complaints related to credit reporting activities.

---

In addition, various federal regulators, including CFPB and FTC, can address the risk of consumer harm by taking actions against fintech firms for deceptive or unfair acts or practices when warranted. For example, in 2016, FTC reached a settlement with a firm that sold machinery designed to create virtual currencies—a process known as mining—and allegedly had been deceiving its customers about the availability and profitability of the machinery. As noted earlier, FTC also settled with a fintech payment provider in February 2018 over complaints by thousands of consumers the company had received regarding confusion over its funds availability practices. Additionally, in 2016 CFPB assessed a \$100,000 civil penalty against a fintech payments firm for deceiving consumers about its data security practices and the safety of its online payment system.<sup>104</sup>

---

## The U.S. Regulatory Environment Poses Various Challenges to Fintech Firms

Fintech firms can find that the complexity of the U.S. financial regulatory system creates challenges in identifying the laws and regulations that apply to their activities, and that complying with state licensing and reporting requirements can be expensive and time-consuming for mobile payment providers and fintech lenders. Also, federal agencies could improve collaboration and clarify issues related to financial account aggregation by making sure that interagency efforts dedicated to fintech include all relevant participants and incorporate other leading practices. In addition, because banks are liable for risks posed by third parties, fintech firms may face delays in entering into partnerships with banks.

---

## Challenges with Complexity of Financial Regulatory Structure

The complex U.S. financial regulatory structure can complicate fintech firms' ability to identify the laws with which they must comply and clarify the regulatory status of their activities. As noted in our past reports, regulatory oversight is fragmented across multiple regulators at the federal level, and also involves regulatory bodies in the 50 states and

---

<sup>104</sup>See *Federal Trade Commission, v. BF Labs, Inc., d/b/a Butterfly Labs*, Case No. 4:14-cv-00815-BCW (W.D. Mo. Feb. 18, 2016), and *In the Matter of Dwolla, Inc.*, File No. 2106-CFPB-0007 (Mar. 2, 2016). For more information on these actions, see <https://www.ftc.gov/news-events/press-releases/2016/02/operators-bitcoin-mining-operation-butterfly-labs-agree-settle> and <https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/>. For more information on mining, including relevant FinCEN guidance, see [GAO-14-496](#).

---

other U.S. jurisdictions.<sup>105</sup> Fintech firms and other stakeholders we interviewed told us that it was difficult for fintech firms to navigate this structure. In particular, understanding the laws and regulations that may apply to fintech firms was not easy because existing regulations were sometimes developed before the type of product or service they are now offering existed. In addition, the cost of researching applicable laws and regulations can be particularly significant for fintech firms that begin as technology start-ups with small staffs and limited venture capital funding. Fintech payments and DLT firms and other market participants told us that navigating this regulatory complexity can result in some firms delaying the launch of innovative products and services—or not launching them in the United States—because the fintech firms are worried about regulatory interpretation. For example, staff from one U.S. firm that developed a DLT payments technology told us that they and their peers only work with foreign customers due to the fragmented U.S. financial regulatory structure and lack of unified positions across agencies on related topics.

However, several U.S. regulators have issued rules and guidance to help fintech firms understand where their products and services may fit within the complex financial regulatory structure, as shown in the following examples.

- In December 2017, the Federal Reserve’s *Consumer Compliance Outlook* newsletter included an article that offered financial institutions and fintech firms general guideposts for evaluating unfair and deceptive practices and fair lending risk related to fintech, with a focus on alternative data.<sup>106</sup> Also, in 2016, a special edition of *Consumer Compliance Outlook* focused on fintech, including summarizing relevant federal laws, regulations, and guidance that may apply to mobile payments, fintech lending, and digital wealth management.<sup>107</sup> For example, the newsletter listed laws and regulations related to

---

<sup>105</sup>See GAO, *Financial Regulation: Complex and Fragmented Structure Could Be Streamlined to Improve Effectiveness*, [GAO-16-175](#) (Washington, D.C.: Feb 25, 2016), *Financial Regulation: Industry Trends Continue to Challenge the Federal Regulatory Structure*, [GAO-08-32](#) (Washington, D.C.: Oct. 12, 2007), and *Financial Regulation: Industry Changes Prompt Need to Reconsider U.S. Regulatory Structure*, [GAO-05-61](#) (Washington, D.C.: Oct. 6, 2004).

<sup>106</sup>Federal Reserve System, *Consumer Compliance Outlook*, 2nd ed. (Philadelphia, Pa.: December 2017).

<sup>107</sup>Federal Reserve System, *Consumer Compliance Outlook, Fintech Special Edition*, 3rd ed. (Philadelphia, Pa.: 2016).



---

credit, privacy, and data security; anti-money laundering requirements; and consumer and investor protection.

- In 2016, CFPB issued a final rule that will extend wide-ranging protections to consumers holding prepaid accounts, including peer-to-peer payments and mobile wallets that can store funds.<sup>108</sup> Also, in 2015, CFPB issued a set of nonbinding consumer protection principles for new faster payment systems, which outline CFPB expectations for payment services providers.<sup>109</sup>
- In February 2017, SEC issued updated guidance on robo-advisers that addresses the substance and presentation of disclosures provided to clients on the robo-adviser and the investment advisory services it offers, the obligation to obtain information from clients to ensure that recommended investments are suitable, and the need to implement effective compliance programs reasonably designed to address the unique nature of providing automated advice.<sup>110</sup> Similarly, in March 2016, FINRA issued a report on effective practices related to digital investment advice and reminded FINRA-registered broker-dealers of their obligations under FINRA rules.<sup>111</sup>
- In 2013, FinCEN issued guidance that clarified the applicability of anti-money laundering and related regulations to participants in certain virtual currency systems, and in 2014 FinCEN issued administrative

---

<sup>108</sup>See Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth In Lending Act (Regulation Z), 81 Fed. Reg. 83934 (Nov. 22, 2016). In January 2018, CFPB delayed the effective date of the rule from April 2018 to April 1, 2019, among other things. See Rules Concerning Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z), 83 Fed. Reg. 6364 (Feb. 13, 2018).

<sup>109</sup>Consumer Financial Protection Bureau, *Consumer Financial Protection Principles: CFPB's Vision of Consumer Protection in New Fast Payment Systems* (Washington, D.C.: July 2015).

<sup>110</sup>Securities and Exchange Commission, *IM Guidance Update: Robo-Advisers*, Issue No. 2017-02 (Washington, D.C.: February 2017).

<sup>111</sup>Financial Industry Regulatory Authority, *Report on Digital Investment Advice* (Washington, D.C.: March 2016).

---

rulings that further clarified the types of market participants to which the 2013 guidance applies.<sup>112</sup>

- In October 2017, CFTC issued a report on virtual currencies that explains that it considers virtual currencies to be commodities, outlines related examples of permissible and prohibited activities, and cautions investors and users on the potential risks of virtual currencies.<sup>113</sup>
- In July 2017, SEC issued a report on DLT token sales, which cautions market participants that sales with certain characteristics may be subject to the requirements of federal securities laws.<sup>114</sup> In general, the report uses one company's token sale as an example to illustrate how SEC could consider a token sale to be a securities offering, and why companies offering such products would have to register the offering with SEC or qualify for an exemption. In August 2017, FINRA also issued an investor alert on DLT token sales, which includes questions for investors to ask before participating in such sales.<sup>115</sup>
- In January 2017, FINRA issued a report on DLT uses more broadly, which outlines key regulatory considerations for firms that want to use DLT in equity, debt, and derivatives markets.<sup>116</sup> For example, the

---

<sup>112</sup>See Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001, March 18, 2013; *Application of FinCEN's Regulations to Virtual Currency Mining Operations*, FIN-2014-R001, January 30, 2014; *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FIN-2014-R002, January 30, 2014; and *Application of Money Services Business Regulations to the Rental of Computer Systems for Mining Virtual Currencies*, FIN-2014-R007, April 29, 2014; FinCEN, *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System*, FIN-2014-R011, October 27, 2014; and FinCEN, *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform*, FIN-2014-R012, October 27, 2014. For further information on this guidance, see [GAO-14-496](#).

<sup>113</sup>Commodity Futures Trading Commission, LabCFTC, *A CFTC Primer on Virtual Currencies* (Washington, D.C.: October 2017).

<sup>114</sup>See Securities and Exchange Commission, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, Release No. 81207 (Washington, D.C.: July 2017). A security includes an "investment contract" (see 15 U.S.C. §§ 77b-77c), which is an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others. See *SEC v. Edwards*, 540 U.S. 389, 393 (2004); *SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946).

<sup>115</sup>Financial Industry Regulatory Authority, *Initial Coin Offerings: Know Before You Invest* (Washington, D.C.: August 2017).

<sup>116</sup>Financial Industry Regulatory Authority, *Distributed Ledger Technology: Implications of Blockchain for the Securities Industry* (Washington, D.C.: January 2017).

---

report outlines securities-related regulatory considerations for DLT applications that could alter securities clearing arrangements, be used for recordkeeping by broker-dealers, or change the equity or debt trading process, among other things.

---

## Challenges Complying with Numerous State Regulatory Requirements

As mentioned previously, although federal oversight applies to some fintech firms, fintech payments and lending firms not subject to routine federal oversight must typically obtain state licenses based on their activities. Banks can choose to be chartered at the state level or as a national bank, which generally exempts them from state licensing requirements and examination. In contrast, fintech payment providers operating as MSBs—including those using DLT—and fintech firms offering consumer loans must typically hold licenses in each state in which they operate. Similarly, as mentioned above, small robo-advisers would generally have to be licensed in states in which they wish to operate.

State regulators and other market observers we interviewed told us that they believe state regulation of fintech firms provides benefits. Several market participants and observers said that states understand the needs of their local economies, consumers, and market participants and can use their authorities to craft tailored policy and regulation. For example, New York regulators created a special license for virtual currency firms. New York regulators told us that they did so because of New York's status as a financial and innovation hub, as well as activities and concerns of virtual currency firms operating within their jurisdiction.<sup>117</sup> In addition, state regulators may complement the federal oversight structure by dedicating additional resources to helping educate fintech firms on regulatory requirements and making sure that firms follow these requirements. For example, two state regulators told us that they work closely with many fintech start-ups to help educate them on regulatory requirements before they apply for licenses or begin operations, and a state regulatory association told us that fintech firms and state regulators often meet to discuss regulatory concerns. Representatives of a state regulatory association told us that federal agencies also rely increasingly on state examinations to ensure compliance with anti-money laundering requirements.

---

<sup>117</sup>As of March 2017, the New York State Department of Financial Services had granted five licenses and charters and issued letters ordering firms to cease operations.

---

Similarly, an industry association and state regulators told us that they believe states are very responsive to consumer complaints. For example, one state regulator told us that they investigate hundreds of consumer complaints per month and believed they often resolved consumer complaints more quickly than their federal consumer protection counterparts, although CFPB staff told us that CFPB handles thousands of complaints per month.<sup>118</sup> California regulators also told us they have initiated their own investigations into the extent to which fintech lenders comply with state lending and securities laws, and risks that fintech lenders may pose to consumers and to markets.

However, complying with fragmented state licensing and reporting requirements can be expensive and time-consuming for mobile payment providers and fintech lenders. For example, stakeholders we interviewed said that obtaining all state licenses generally costs fintech payments firms and lenders \$1 million to \$30 million, including legal fees, state bonds, and direct regulatory costs. Also, market participants and observers told us that fintech firms may spend a lot of time on state examinations because state exam requirements vary and numerous states may examine a fintech firm in 1 year. For example, staff from a state regulatory association said that states may examine fintech firms subject to coordinated multistate exams 2 or 3 times per year, and as many as 30 different state regulators per year may examine firms that are subject to state-by-state exams.

Although these challenges are not unique to fintech firms, they may be more significant for fintech firms than for other MSBs and lenders. For example, some MSBs and lenders operate in a limited geographic area that can require them to be licensed by one state only. Other firms operate in multiple states or nationwide, but may have started with a license in one state and then obtained additional licenses and spread these compliance costs as they grew over time. In contrast, fintech firms are generally online-only businesses that likely seek to operate nationwide from their inception, which immediately requires licenses in all states and generates higher up-front compliance costs that may strain limited venture capital funding. For example, one firm we interviewed that funds fintech start-ups told us that one of their fintech firms spent half of the venture capital funds it had raised obtaining state licenses. As a

---

<sup>118</sup>CFPB staff told us that, in 2017, CFPB handled more than 26,000 complaints per month by sending complaints to companies for resolution or to other regulators.

---

result, some firms may choose not to operate in the United States. For example, one DLT provider we interviewed told us that although they are based in the United States, they operate abroad exclusively because state licensing costs are prohibitively expensive.

Bank partnerships and specialized operating charters offered by federal and state banking regulators may help fintech firms more easily operate nationwide by generally preempting state licensing requirements. For example, some fintech payments firms and fintech lenders have chosen to partner with nationally chartered and state-chartered banks, which allows them to operate nationwide without having to obtain individual state licenses. Also, two fintech lenders have applied for an Industrial Loan Corporation (ILC) charter, an FDIC-supervised state banking charter, which commercial firms other than regulated financial institutions can obtain in certain states to operate nationally.<sup>119</sup> Such ILCs would also be overseen by FDIC if they obtain FDIC deposit insurance.

In addition, in December 2016, OCC announced its intent to consider applications for special-purpose national bank charters from fintech firms such as lenders, which would allow such firms to operate nationally under a single national bank charter if finalized.<sup>120</sup> However, OCC officials we interviewed told us that this special-purpose national bank charter is on hold because they are still reviewing whether to go forward with the

---

<sup>119</sup> ILCs are limited-service financial institutions that make loans and may raise funds by selling certificates called “investment shares” and by accepting deposits. ILCs differ from finance companies because ILCs accept deposits in addition to making consumer loans, while ILCs differ from commercial banks because most ILCs do not offer demand deposit (checking) accounts. FDIC staff told us that as of October 2017, there were 24 ILCs in the United States. Although two fintech lenders have applied for an ILC charter, one of the two fintech lenders withdrew its application. See GAO, *Bank Holding Company Act: Characteristics and Regulation of Exempt Institutions and the Implications of Removing the Exemptions*, [GAO-12-160](#) (Washington, D.C.: Jan. 19, 2012) for more information on ILCs.

<sup>120</sup> Office of the Comptroller of the Currency, *Exploring Special Purpose National Bank Charters for Fintech Companies* (Washington, D.C.: December 2016). In March 2017, OCC published a draft supplement to its existing licensing manual that outlined the way it would apply existing licensing standards and requirements in its policies to fintech companies that apply for special-purpose national bank charters. OCC solicited public comments on the December 2016 paper and March 2017 draft. For more information, see Office of the Comptroller of the Currency, *OCC Summary of Comments and Explanatory Statement: Special Purpose National Bank Charters for Financial Technology Companies* (Washington, D.C.: March 2017); and Office of the Comptroller of the Currency, *Comptroller’s Licensing Manual Draft Supplement, Evaluating Charter Applications from Financial Technology Companies* (Washington, D.C.: March 2017).

---

proposal, and CSBS has filed a lawsuit against OCC challenging the fintech charter.<sup>121</sup> Some fintech lending firms and an industry association representing payments firms have expressed interest in applying for this special charter, but other stakeholders we interviewed told us that the proposed fintech charter may not be a good option for small fintech firms if the capital requirements are the same as those for banks.

In addition, state regulators are taking steps to make it easier for fintech firms seeking to operate across multiple states. For example, CSBS staff we interviewed told us that states leverage the Nationwide Multistate Licensing System—which enables firms to submit one application with information that fulfills most of the licensing requirements of each state that participates in this system.<sup>122</sup> Staff from CSBS, some fintech firms, and an industry observer we interviewed said that although the multistate licensing system has reduced administrative requirements somewhat, firms still have to make additional filings to address certain requirements unique to some states. In February 2018, seven state regulators also agreed to standardize key elements of the MSB licensing process and mutually accept licensing findings.<sup>123</sup> Additionally, in 2013, state regulators established the Multi-State MSB Examination Taskforce, which coordinates and facilitates multistate supervision of MSBs.<sup>124</sup> CSBS staff told us that multistate exams have made the state MSB exam process more efficient for state regulators and MSBs.

---

<sup>121</sup> See *Conference of State Bank Supervisors v. Office of the Comptroller of the Currency*, Case No. 1:17-cv-00763-JEB (D.D.C. Apr. 26, 2017). A similar lawsuit brought by the New York State Department of Financial Services against OCC was dismissed in December 2017 when the court ruled that plaintiff had not suffered an injury and therefore lacked standing and that plaintiff's claims were not ripe. See *Vullo v. Office of the Comptroller of the Currency*, Case No. 1:17-cv-03574-NPB (S.D.N.Y. Dec. 12, 2017) (memorandum and order granting defendant's motion to dismiss).

<sup>122</sup> The Nationwide Multistate Licensing System was originally developed as a voluntary system for state licensing and is the system of record for nondepository financial services, licensing, or registration in participating state agencies. Mortgage licensing is included in the Nationwide Multistate Licensing System under the Secure and Fair Enforcement for Mortgage Licensing Act of 2008, Pub. L. No. 110-289, Div. A, tit. V, 122 Stat. 2654, 2810.

<sup>123</sup> The seven states include Georgia, Illinois, Kansas, Massachusetts, Tennessee, Texas and Washington.

<sup>124</sup> CSBS staff said that in 2017, the taskforce coordinated 64 examinations of multistate MSBs where teams of examiners from different states conducted coordinated supervision.

---

In May 2017, the CSBS also announced they would be expanding efforts to modernize state regulation of fintech firms.<sup>125</sup> For example, under this initiative, officials we interviewed told us they

- plan to redesign their multistate licensing system to provide a more streamlined licensing process for new applicants and shift state resources to higher-risk cases by 2018;
- plan to harmonize multistate supervision by establishing model approaches to key aspects of nonbank supervision, making examinations more uniform, identifying and reporting violations at the national level, and creating a common technology platform for examinations by 2019; and
- have formed a fintech industry advisory panel—with sub-groups on payments, lending, and banking—to identify licensing and regulatory challenges.<sup>126</sup>

---

## Challenges with Interagency Collaboration

Although a few fintech market participants and observers we interviewed told us that they thought regulatory collaboration on fintech was sufficient, the majority of market participants and observers we interviewed who commented on interagency collaboration said that it could generally be improved. Some also cited additional areas in which better interagency collaboration could facilitate innovation:

- **Use of alternative data and modeling in fintech lending.** Fintech lenders may face challenges because agencies with authorities related to consumer protection and fair lending have not issued guidance on the use of alternative data and modeling. For example, one fintech lender we interviewed told us that they discussed using alternative data to assess creditworthiness with FDIC and FTC, but they do not understand what each agency might consider to be an unfair, deceptive, or abusive practice because the agencies have not coordinated positions. Staff we interviewed from two consulting firms that advise on fintech told us that lack of clarity or coordination on fair lending and use of alternative data and modeling creates uncertainty for fintech lenders. This has led some fintech lenders to forgo use of alternative data for underwriting purposes since they do not know if it

---

<sup>125</sup>Conference of State Bank Supervisors, *CSBS Announces Vision 2020 for Fintech and Non-Bank Regulation* (Washington, D.C.: May 2017).

<sup>126</sup>For more information on efforts related to the Nationwide Multistate Licensing System, see <https://new.nmls.org/>, <https://new.nmls.org/ses>, and <https://fintech.csbs.org/>.

---

will produce outcomes that violate fair lending laws and regulations. However, FDIC staff told us that FDIC applies the same standards as FTC in determining whether an act or practice is unfair or deceptive and that existing guidance on fair lending applies broadly to traditional and nontraditional modeling techniques and data sources.<sup>127</sup>

- **OCC special-purpose national bank charter.** A few market participants and observers we interviewed told us that fintech payment providers and lenders may face challenges because OCC has not sufficiently coordinated with the Federal Reserve and FDIC on OCC's special-purpose national bank charter. Despite OCC discussion with the Federal Reserve, the charter proposal does not specify whether recipients could access the Federal Reserve payments system. Federal Reserve officials have said that the Federal Reserve will likely not take any policy positions or make any legal interpretations about the proposed charter until OCC finalizes the charter's terms and a firm applies for a charter. Officials have said that this is their position because the potential policy and legal interpretation issues that could arise related to membership and access to Federal Reserve services will require a case-by-case, fact-specific inquiry unique to any firm that moves forward with an application. One fintech lender we interviewed told us that obtaining consistent and complete information from OCC and the Federal Reserve on the specific rights this charter would grant a fintech lender had been challenging, and that this lack of consistency and clarity could discourage fintech firms from applying for the charter. However, OCC staff we interviewed told us that the charter is not yet final and that they facilitate communication between fintech firms that are interested in the special charter and the Federal Reserve. Also, OCC staff said that they briefed FDIC staff on the special charter, but will coordinate further if appropriate.<sup>128</sup>
- **Differing regulatory interpretation of consumer protection requirements.** As discussed above, fintech firms may be subject to

---

<sup>127</sup>For example, FDIC staff cited the 2009 Interagency Fair Lending Procedures and the 1994 Interagency Policy Statement on Discrimination in Lending as existing guidance on fair lending that applies broadly to traditional and nontraditional modeling techniques and data sources.

<sup>128</sup>OCC's draft licensing manual supplement clarifies that the special charter is specifically for uninsured entities. OCC staff said that FDIC would therefore likely not have a role. See Office of the Comptroller of the Currency, *Comptroller's Licensing Manual Draft Supplement: Evaluating Charter Applications from Financial Technology Companies* (Washington, D.C.: March 2017).



---

CFPB oversight and limited federal financial regulatory oversight if they also partner with financial institutions. In addition, FTC and CFPB can also take enforcement actions against fintech firms not registered or chartered as a bank for violations of any federal consumer protection laws they enforce. Fintech firms we spoke with said that this can cause challenges because firms are concerned that regulators may have different interpretations of what conduct might merit consumer protection enforcement actions, and a research and consulting firm we interviewed that works with fintech start-ups told us that this is one of the industry's biggest challenges. Similarly, the potential for differing regulatory interpretation may limit the effectiveness of agency efforts to innovate. For example, fintech firms can apply for a CFPB No Action Letter, which is intended to reduce regulatory uncertainty for financial products or services that promise substantial consumer benefit but face uncertainty regarding consumer protection requirements. However, some entities we spoke with said that few firms have applied, in part because a letter provided by CFPB may not preclude prudential regulators or FTC from taking enforcement actions in cases where they have jurisdiction.<sup>129</sup>

Although stakeholders indicated that agencies could improve interagency collaboration on other fintech issues, federal agencies said that they already collaborate through a variety of informal and formal channels at the domestic and international levels. Domestically, in addition to informal discussions and participation in fintech events hosted by other agencies, some agencies have coordinated examinations of third-party service providers and enforcement actions. For example, in 2014 and 2015, CFPB, FCC, FTC, and state regulators coordinated on enforcement actions related to unauthorized mobile carrier billing charges. Also, U.S. agencies have had informal discussions regarding fintech with their foreign counterparts. For example, Treasury staff have discussed regulations designed to counter money laundering and terrorist financing

---

<sup>129</sup>According to CFPB's No Action Letter policy, a No Action Letter is not issued by or on behalf of any other government agency or any other person, and is not intended to be honored or deferred to in any way by any court or any other government agency or person. Consumer Financial Protection Bureau, Policy on No-Action Letters; Information Collection, 81 Fed. Reg. 8686, 8695 (Feb. 22, 2016). As of October 2017, CFPB had issued one No Action Letter to Upstart Network, Inc., a company that uses alternative data in making credit and pricing decisions. As a condition of the No Action Letter, Upstart will regularly report lending and compliance information to CFPB to mitigate risk to consumers and aid the Bureau's understanding of how alternative data affects lending decision-making. For more information, see <https://www.consumerfinance.gov/about-us/newsroom/cfpb-announces-first-no-action-letter-upstart-network/>.

---

with officials from countries such as France and the United Kingdom. In addition, federal agencies have begun to collaborate on fintech regulatory issues through formal interagency working groups that are primarily concerned with other financial regulatory issues. For example, at the domestic level, U.S. prudential regulators have discussed issues related to potential risks of fintech lending and DLT through the Financial Stability Oversight Council. At the international level, the Federal Reserve represents the United States at the Bank for International Settlements, which has published papers on fintech topics including payments, fintech lending, and DLT. For more information on these efforts and others, see appendix II.

Further, federal agencies said that they have recently organized the following interagency collaborative groups dedicated to fintech, as detailed in appendix II:

- In March 2017, the Federal Reserve convened the Interagency Fintech Discussion Forum, an informal group which meets approximately every 4 to 6 weeks and aims to facilitate information sharing among consumer compliance staff from the federal banking regulators on fintech consumer protection issues and supervisory outcomes. Discussion topics have included account aggregation, alternative data and modeling techniques, and third-party oversight.
- In 2016, Treasury created the Interagency Working Group on Marketplace Lending, which was active over the course of fiscal year 2016, meeting 3 times.<sup>130</sup> This group shared information among industry participants and public interest groups, and discussed issues from a Treasury report on benefits and risks associated with online marketplace lending.<sup>131</sup>
- In 2010, the Federal Reserve Banks of Atlanta and Boston created the Mobile Payments Industry Workgroup to facilitate discussions among industry stakeholders about how a successful mobile payments system could evolve in the United States. This group also functions as an interagency collaboration mechanism through biennial meetings between industry stakeholders and relevant regulators that

---

<sup>130</sup>Treasury staff we interviewed told us in October 2017 that they did not have plans to reconvene the group.

<sup>131</sup>Department of the Treasury, *Opportunities and Challenges in Online Marketplace Lending* (Washington, D.C.: May 2016).

---

update industry on regulatory concerns, identify potential regulatory gaps, and educate regulators on mobile payment technologies.

However, we found that these groups do not include all relevant participants. For example, NCUA was not included in the Interagency Fintech Discussion Forum or the Interagency Working Group on Marketplace Lending, and FCC has not participated in the biennial regulator meetings of the Mobile Payments Industry Workgroup since 2012. Federal Reserve staff said that they did not include NCUA in the Interagency Fintech Discussion Forum because NCUA is not a bank regulator. Treasury staff noted that staff who could explain why NCUA had not been invited to participate in the Interagency Working Group on Marketplace Lending were no longer with the agency. Similarly, FCC staff could not recall why they had not participated in recent biennial regulator meetings of the Mobile Payments Industry Workgroup.

However, NCUA has experiences and perspectives that would make it a relevant participant in the Interagency Fintech Discussion Forum, and NCUA officials said that they would participate in these interagency efforts if invited. NCUA would be a relevant participant because, although it does not oversee banks, it oversees credit unions that have entered into partnerships with fintech lenders and virtual currency exchanges, and could enter into partnerships with other fintech firms. Similar to fintech partnerships with banks, these partnerships could create risks related to safety and soundness and consumer protection. Further, NCUA's 2018–2022 draft strategic plan includes fintech as a key risk to the credit union system because fintech could provide a competitive challenge to credit unions or take advantage of differences in how credit unions and fintech firms are regulated, among other things.<sup>132</sup>

Likewise, as Federal Reserve staff have acknowledged, FCC could be a relevant participant in biennial regulators meetings of the Mobile Payments Industry Workgroup because FCC could share valuable insight on regulatory concerns related to mobile device security with other regulators and industry participants. Specifically, FCC has facilitated and encouraged industry efforts to improve security of mobile devices, on which consumers make fintech payments, and has conducted related consumer education efforts. FCC staff said they would consider participating in future biennial regulator meetings of the Mobile Payments

---

<sup>132</sup>National Credit Union Administration, *2018-2022 Draft Strategic Plan* (Washington, D.C.: October 2017).

---

Industry Workgroup if the topics discussed aligned with FCC's work on mobile device security.

Our past work has identified key practices relating to collaborative mechanisms among agencies that increase their effectiveness, such as including participants with the appropriate knowledge, skills, and abilities.<sup>133</sup> In addition, these key practices also state that an interagency group should continue to reach out to potential participants who may have a shared interest in order to ensure that opportunities for achieving outcomes are not missed.<sup>134</sup>

However, we found that interagency collaborative efforts dedicated to fintech issues were not fully leveraging relevant agency expertise. Lack of NCUA participation in the Interagency Fintech Discussion Forum may preclude NCUA and the other participating agencies from sharing information that could be useful in efforts to oversee the risks that fintech poses to their regulated institutions. Similarly, lack of FCC participation in the biennial regulators meetings of the Mobile Payments Industry Workgroup could preclude industry participants from receiving updates on FCC regulatory concerns related to mobile device security and could preclude FCC from learning about new risks that fintech payments products pose to mobile device security.

Furthermore, OCC and international bodies have identified fintech as an area where collaboration among agencies can be helpful. For example, OCC has stated that collaboration among supervisors can promote a common understanding and consistent application of laws, regulations, and guidance through steps such as establishing regular channels of communication.<sup>135</sup> At the international level, the Bank for International Settlements has recommended that bank supervisors in jurisdictions where responsibilities related to fintech are fragmented among a number of regulators with overlapping authorities should collaborate with other relevant agencies to develop standards and regulatory oversight for

---

<sup>133</sup>[GAO-12-1022](#).

<sup>134</sup>GAO, *Managing for Results: Implementation Approaches Used to Enhance Collaboration in Interagency Groups*, [GAO-14-220](#) (Washington, D.C.: Feb. 14, 2014).

<sup>135</sup>Office of the Comptroller of the Currency, *Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective* (Washington, D.C.: March 2016).

---

fintech, as appropriate.<sup>136</sup> Similarly, the Financial Stability Board has suggested that responsible agencies further open lines of communication to address cross-cutting fintech issues.<sup>137</sup>

---

### Industry Disagreements on Aggregation of Consumer Financial Account Information Create the Need for Stronger Collaboration

Among other consumer protection issues related to financial account aggregation, market participants do not agree about whether consumers using account aggregators will be reimbursed if they experience fraudulent losses in their financial accounts. While some account aggregators negotiate contracts with the financial institutions that hold the consumer accounts that are being aggregated, other account aggregators have no relationship with the financial institutions holding the consumer accounts that they access on behalf of those consumers. Officials from at least one large bank have made public statements that they may not reimburse losses from consumer accounts if the consumer provided his or her account credentials to an account aggregator and fraudulent activity subsequently occurs in the consumer's account. In contrast, some account aggregators and consumer protection groups have argued that consumer protection law establishes that banks retain the obligation to reimburse losses due to transactions not authorized by the consumers.

To date, CFPB and the Federal Reserve have taken varying public positions on this disagreement among market participants, and some regulators told us that they have held related discussions with market participants and observers. In October 2017, CFPB issued principles for consumer-authorized financial data sharing and aggregation that stated that consumers should have reasonable and practical means to dispute and resolve instances of unauthorized transactions.<sup>138</sup> However, CFPB's principles are not binding and federal financial regulators have not issued guidance or rules to clarify this issue. As previously mentioned, CFPB also issued a request for information studying these topics to various

---

<sup>136</sup>Bank for International Settlements, *Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors*, August 2017.

<sup>137</sup>Financial Stability Board, *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention*, June 2017.

<sup>138</sup>Consumer Financial Protection Bureau, "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation" (Washington, D.C.: October 2017).

---

industry members, observers, and consumers in November 2016.<sup>139</sup> A member of the Board of Governors of the Federal Reserve System has publicly stated that industry stakeholders will need to come to agreement on which party bears responsibility for unauthorized transactions.<sup>140</sup> Also, Federal Reserve staff told us that some financial institutions and account aggregators are negotiating contractual arrangements that could address this issue on a case-by-case basis. In addition, staff from FDIC, the Federal Reserve, and OCC said that they have discussed related issues with market participants and observers.

The financial regulators have recently begun to hold collaborative information sharing discussions on consumer compliance issues surrounding financial account aggregation, but this collaboration has not resulted in any coordinated public outcomes on the issues. In May 2017, the federal financial regulators—CFPB, the Federal Reserve, FDIC, NCUA, and OCC—and representatives of state financial regulators began to share information on account aggregation and related consumer compliance issues through the Federal Financial Institutions Examination Council (FFIEC) Task Force on Supervision and the FFIEC Task Force on Consumer Compliance. The regulators are collaborating through FFIEC because they acknowledge that account aggregation issues cross agency jurisdictions. According to participating agency officials, FFIEC discussions have covered responsibilities for consumer reimbursement due to fraudulent charges and access to consumer data, generated an internal paper on consumer compliance issues, and previewed CFPB’s principles for consumer-authorized financial data sharing and aggregation prior to publication. However, as of November 2017, these efforts have not generated public outcomes to guide market participants.

The federal financial regulators’ missions include ensuring that consumers are protected. CFPB’s primary mission is to protect consumers in the financial marketplace, including ensuring that markets

---

<sup>139</sup>Consumer Financial Protection Bureau, Request for Information Regarding Consumer Access to Financial Records, 81 Fed. Reg. 83806. (Nov. 22, 2016) and “Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation” (Washington, D.C.: October 2017).

<sup>140</sup>These remarks were made by the member of the Board of Governors of the Federal Reserve System in a personal capacity. Board of Governors of the Federal Reserve System, *Remarks by Lael Brainard, Member of the Board of Governors of the Federal Reserve*, “Where Do Consumers Fit in the Fintech Stack?” (Ann Arbor, Mich.; November 2017).

---

for consumer financial products and services operate transparently and efficiently to facilitate access and innovation. Similarly, according to their mission and vision statements, the banking and credit union regulators help protect consumer rights by supervising financial institutions to help ensure compliance with consumer protections.

However, some of the regulators told us that they have not taken more steps to resolve the disagreements surrounding financial account aggregation because they are concerned over acting too quickly. For example, Federal Reserve staff we interviewed told us that premature regulatory action could be detrimental to the negotiations between individual financial institutions and financial account aggregators. Similarly, OCC staff we interviewed told us that OCC staff does not recommend publishing guidance or rules while the account aggregation industry is evolving because regulation should not constantly change. Nonetheless, the financial regulators could take additional steps to address these issues without prematurely issuing rules or regulations. Further, the FFIEC IT Examination Handbook on e-Banking's appendix on aggregation services, which the financial regulators use in their examinations of banks, indicates that the financial regulators have been aware since at least 2003 that regulatory requirements related to consumer protection responsibilities of financial account aggregators are not clear.<sup>141</sup>

Incorporating leading practices on collaboration could strengthen the efforts that regulators are making to address financial account aggregation issues. As discussed previously, our prior work has developed interagency collaboration principles that make efforts among agencies more likely to be effective.<sup>142</sup> These principles find that collaborative efforts should define the short-term and long-term outcomes that the collaboration is seeking to achieve and clarify the roles and responsibilities of the participating agencies, among other things. Although banking regulators and CFPB have discussed issues related to account aggregation within FFIEC, these discussions have not yet

---

<sup>141</sup>Federal Financial Institutions Examination Council, *Information Technology Examination Handbook, E-Banking Booklet Appendix D: Aggregation Services* (Washington, D.C.: August 2003).

<sup>142</sup>GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, [GAO-12-1022](#) (Washington, D.C.: Sept. 27, 2012), and *Managing for Results: Implementation Approaches Used to Enhance Collaboration in Interagency Groups*, [GAO-14-220](#) (Washington, D.C.: Feb. 14, 2014).

---

defined outcomes or produced any public outcomes to help guide fintech firms and traditional financial institutions which could help lead to market-based solutions, or defined agency roles and responsibilities. In addition, market participants, CSBS staff, and a member of the Board of Governors of the Federal Reserve System have said that additional collaboration on financial account aggregation issues—including reimbursement for unauthorized transactions—would be beneficial.<sup>143</sup> Similarly, in its 2017 annual report, the Financial Stability Oversight Council encouraged financial regulators to monitor how fintech products affect consumers and regulated entities and to coordinate regulatory approaches, as appropriate.<sup>144</sup>

Acting collaboratively to help address consumer compliance issues related to financial account aggregation could help financial regulators better meet their consumer protection missions. Improved collaboration could help regulators and market participants resolve disagreements over account aggregation and related consumer compliance issues more quickly and in a manner that balances the competing interests involved. Taking steps now, while the discussion on financial account aggregation is in its relatively early stages, could help federal regulators better address these needs over the long term. Until regulators coordinate and assist the industry in clarifying and balancing the valid interests on both sides, consumers could have to choose between facing potential losses or not using what they may find to be an otherwise valuable financial service, and fintech firms providing useful services to consumers will face barriers to providing their offerings more broadly.

---

## Challenges Involving Fintech Partnerships with Banks

Partnerships between fintech firms and financial institutions are increasingly common because such partnerships offer benefits to both parties involved. According to literature we reviewed and market participants and observers we interviewed, the benefits to banks can include the ability to meet consumer demand by providing their customers with access to innovative products that provide good user experiences

---

<sup>143</sup>Board of Governors of the Federal Reserve System, *Remarks by Lael Brainard, Member of the Board of Governors of the Federal Reserve, "Where Do Consumers Fit in the Fintech Stack?"* (Ann Arbor, Mich.; Nov. 2017), and *Remarks by Lael Brainard, Member of the Board of Governors of the Federal Reserve, "Where Do Banks Fit in the Fintech Stack?"*, April 2017.

<sup>144</sup>Financial Stability Oversight Council, *2017 Annual Report* (Washington, D.C.: Dec. 14, 2017).



---

without having to dedicate extensive internal time or resources. Market observers and Federal Reserve staff we interviewed told us that this benefit may be particularly important for small banks and credit unions, which have fewer staff and fewer financial resources for research and development. Similarly, the benefits to fintech firms can include access to banking services and networks, customer acquisition, and assistance with regulatory compliance. Some fintech firms enter contractual agreements to partner with banks through white-labeling, a type of partnership where the bank markets the fintech firm's product as its own when soliciting customers. Other fintech firms enter contractual partnerships with banks as stand-alone third-party relationships. For example, some fintech lenders make loans to customers and partner with a bank that originates or purchases loans sourced through the fintech lender.

However, because banks are liable for risks posed by third parties as discussed above, fintech firms may face delays in entering into partnerships with banks. Financial regulators have issued guidance on risk management for financial institutions' relationships with third parties.<sup>145</sup> Among other things, this guidance explains that financial institutions are expected to conduct proper due diligence in selecting partners and to monitor the activities conducted by third parties for compliance with relevant laws, rules, and regulations, considering areas such as consumer protection, anti-money laundering/counter-terrorist financing, and security and privacy requirements. Banks, fintech firms, and market observers we interviewed told us that banks may interpret this guidance conservatively. Large banks may also spend significant time conducting due diligence on the practices and controls in place at the fintech firms seeking to partner with them in order to prevent unnecessary

---

<sup>145</sup>Regulators have noted that risk posed by third parties to banks and the overall payment system require caution in guidance and outlined risk management requirements in related guidance, sometimes focused on fintech. Federal Financial Institutions Examination Council, *Information Technology Examination Handbook, Retail Payment Systems, Appendix E: Mobile Financial Services* (Washington, D.C.: April 2016) and *Information Technology Examination Handbook, Appendix D: E-Banking* (Washington, D.C.: August 2003); Federal Deposit Insurance Corporation, *Guidance For Managing Third-Party Risk*, FIL-44-2008 (Washington, D.C.: June 2008); Office of the Comptroller of the Currency, *Risk Management Guidance*, OCC Bulletin 2013-29 (Washington, D.C.: October 2013), as supplemented by *Frequently Asked Questions to Supplement OCC Bulletin 2013-29*, OCC Bulletin 2017-21 (Washington, D.C.: June 2017); and Consumer Financial Protection Bureau, *Compliance Bulletin and Policy Guidance; 2016-02, Service Providers* (Washington, D.C.: October 2016). For more information on FDIC's proposed third-party lender guidance, see Federal Deposit Insurance Corporation, *Examination Guidance for Third-Party Lending* (Washington, D.C.: July 2016).

---

compliance or operational risks, while a banking association told us that small banks with fewer resources to dedicate to due diligence may be unwilling to risk partnering with fintech firms. Banks, fintech firms, and market observers we interviewed told us that bank due diligence can also lead to lengthy delays in establishing partnerships, which can put fintech firms at risk of going out of business if they do not have sufficient funding and are not able to access new customers through a bank partner. For example, officials we interviewed from one bank told us that it takes about 18 months to launch a partnership with a fintech firm, and acknowledged that this is too slow to align with venture capital funding cycles that many fintech providers rely upon.

---

## Consideration of Regulatory Approaches Abroad Could Benefit Fintech Regulation and Innovation

Regulators abroad have addressed the emergence of financial innovation through various means, including establishing innovation offices; establishing mechanisms for allowing fintech firms to conduct trial operations; holding innovation competitions; providing funding for firms through business accelerators; and using various methods to coordinate with other regulators domestically and internationally. While certain U.S. regulators have adopted similar efforts, further adoption of these approaches by U.S. regulators could facilitate interactions between regulators and fintech firms and improve regulators' knowledge of fintech products. However, some initiatives may not be appropriate for the U.S. regulatory structure. For example, adopting certain initiatives could raise concerns about U.S. agencies picking winners, in which firms that participate in these programs may be better positioned to succeed than other firms. Further, particular initiatives may not align with agencies' legal authorities or missions.

---

---

## Regulators in the U.S. and Abroad Have Developed Approaches to Improve Interaction with Firms and Help Them Identify Applicable Regulatory Requirements

Citing the complexity of the U.S. financial regulatory system, fintech firms and industry observers noted having difficulty identifying which regulations they were subject to or which regulators would oversee their activities. Further, one fintech firm noted that when they were able to identify their regulators, they had difficulty finding a point of contact at the regulators. Officials from three regulators that we interviewed also noted that they had been contacted by fintech firms that were confused about their regulatory status and did not fall under the agency's regulatory authority, but were subject to oversight by other regulators.

Regulators in the U.S. and abroad have taken steps to better facilitate interactions with fintech firms, including by establishing innovation offices with dedicated staff to serve as a front door for start-up firms or innovators to find information on regulation and to contact the agency. These innovation offices generally maintain a webpage hosted on the agencies' websites, a dedicated e-mail address, or dedicated staff. Through these innovation offices, some agencies offer services including office hours during which regulatory staff are available to meet and provide informal guidance. For example, CFPB officials said that, as of August 2017, they had met with approximately 115 companies in four such events in New York and San Francisco, under the agency's Project Catalyst. Similarly, OCC officials noted that through their Office of Innovation, they have been able to answer regulatory questions for fintech firms and connect firms to relevant OCC offices. Since the launch of LabCFTC, CFTC's innovation office, in May 2017, CFTC officials have met with more than 100 entities through office hour sessions in New York, Chicago, and Washington, D.C.

In addition to office hours, several regulators have held fintech events through their innovation offices. For example, FTC has held three fintech forum events comprising panel discussions with industry experts, covering topics such as marketplace lending and distributed ledger technology. Several regulators have also issued publications on various fintech topics, which are posted to the dedicated webpages for those agencies with innovation offices.

Some regulators from other jurisdictions also facilitated regular interaction with firms through their innovation offices. For example, through its Innovation Hub, the United Kingdom's (UK) Financial Conduct Authority offers informal regulatory guidance to individual firms directly and through posted publications; operates its regulatory sandbox, described below; and engages with industry participants through various events. Similarly,

---

through a program called Looking Glass, the Monetary Authority of Singapore offers fintech firms training and consultation on regulation and provides a space for fintech firms to give product demonstrations to regulators and banks. Regulators and fintech firms we interviewed abroad said that these innovation offices have helped firms better understand their regulatory obligations and help regulators identify and address risks early. For example, representatives of a robo-adviser firm we interviewed in Hong Kong said that their interactions with the Hong Kong Securities and Futures Commission's innovation office—known as the Fintech Contact Point—made identifying and obtaining guidance from the appropriate regulatory officials easier, which helped the firm more efficiently develop a product compliant with applicable regulations.

Some fintech firms and industry observers stated that U.S. regulators' innovation offices have helped fintech firms by offering a point of contact for new entrants in the industry. Additionally, in a 2009 report, we created a framework that identified characteristics of an effective financial regulatory system.<sup>146</sup> One of the characteristics was that regulators should oversee new products as they come onto the market to take action as needed to protect consumers and investors, without unnecessarily hindering innovation. Figure 5 summarizes efforts that we reviewed by regulators in the U.S. and abroad to implement initiatives to improve interactions with fintech firms.

---

<sup>146</sup>GAO, *Financial Regulation: A Framework for Crafting and Assessing Proposals to Modernize the Outdated U.S. Financial Regulatory System*, [GAO-09-216](#) (Washington, D.C.: Jan. 8, 2009).

**Figure 5: Select Interaction-Building Initiatives among U.S. Federal and Other Jurisdictions' Regulators**

	U.S. Financial Regulatory Agencies									United Kingdom	Singapore	Hong Kong
	CFPB	CFTC	FDIC	Federal Reserve	FINRA	FTC	NCUA	OCC	SEC			
Innovation office	○	○	--	○ <sup>a</sup>	○	○	--	○	○	○	○	○
Dedicated webpage	○	○	--	○ <sup>a</sup>	○	○	--	○	○	○	○	○
Dedicated e-mail address	○	○	--	○ <sup>a</sup>	○	--	--	○	○	○	○	○
Dedicated phone number	--	○	--	--	--	--	--	○	--	○	--	--
Office hours	○	○	--	○ <sup>a</sup>	○	--	--	○	--	○	○	○
Fintech events	○	○	--	○	○	○	--	○	○	○	○	○
Issued publications	○	○	○	○	○	○	--	○	○	○	○	○

- No program  
 ○ Programs that are being developed  
 ● Established programs

Source: GAO analysis of agency and firm interviews and agency documents in the U.S. and abroad. | GAO-18-254

Notes: Fintech refers to traditional financial services provided by nontraditional technology-enabled providers.

Following are the acronym definitions for each of the U.S. regulators—CFPB is Consumer Financial Protection Bureau; CFTC is Commodity Futures Trading Commission; FDIC is Federal Deposit Insurance Corporation; Federal Reserve is Board of Governors of the Federal Reserve System; FINRA is Financial Industry Regulatory Authority; FTC is Federal Trade Commission; NCUA is National Credit Union Administration; OCC is Office of the Comptroller of the Currency; and SEC is Securities and Exchange Commission.

Following are the agencies for each foreign jurisdiction in the figure—United Kingdom agencies are the Bank of England, Financial Conduct Authority, and Her Majesty's Treasury; Singapore agencies are the Monetary Authority of Singapore and SG Innovate; and Hong Kong agencies are Cyberport, Hong Kong Monetary Authority, and Hong Kong Securities and Futures Commission.

<sup>a</sup>The Federal Reserve Bank of San Francisco maintains an innovation office, which coordinates with the Federal Reserve System at large, called Fintech Navigate.

However, FDIC and NCUA have not established innovation offices for various reasons. For example, FDIC staff said that, although the agency has not formally evaluated establishing an innovation office, they have met with fintech firms to discuss deposit insurance applications. Associated with the deposit application process, the agency has established central points of contact for all interested parties, not only fintech firms. NCUA said that its lack of legal authority over third-party service providers limited the usefulness of an innovation office, since fintech providers are often third-party service providers. However, by not dedicating specific staff, as occurs with the establishment of an innovation office, these regulators could be less able to interact with fintech firms in

---

their sectors and fintech firms that partner with their regulated entities. Other regulators who, similar to FDIC and NCUA, generally do not directly oversee third-party providers, though they may have such authority, have noted benefits from establishing innovation offices. For example, OCC, which has a similar mission to these two regulators, has formed such an office and OCC staff said that the agency has benefited by learning about industry trends involving fintech and by improving interactions with fintech firms and banks. Similarly, Federal Reserve officials we interviewed said that efforts through its innovation office have helped staff better understand fintech issues and have particularly helped its examiners better understand banks that partner with fintech companies. Consideration of establishing innovation offices, as many U.S. regulators have recently done, could help FDIC and NCUA better enable new firms to become familiar with regulatory requirements and could better facilitate interaction between the agencies and fintech service providers.

---

### Regulators Abroad Use Various Approaches to Learn about and Enable Development of New Fintech Products, and U.S. Regulators Could Consider Taking Similar Steps

Internationally, some regulators have taken various approaches that help educate their staff on emerging products and help innovators develop products in limited-risk environments (see fig. 6). Based on interviews with regulators and firms abroad and a literature review, initiatives that we studied include regulatory sandboxes, proofs-of-concepts, innovation competitions or awards, and agency-led accelerators. Regulatory sandboxes that we studied were agency-led programs that allow firms to test innovative products; services; business models; or delivery mechanisms in a live environment, subject to agreed-upon testing parameters. The proofs of concept that we reviewed were similar to sandboxes, but for these programs regulators issued a request for proposals to industry to develop a product that is conceptual; that is, an idea for a product that is not yet on the market. In the fintech competitions that we studied, regulators invited firms to develop solutions to problem statements drafted by agencies or financial institutions. Accelerators that we reviewed provided funding; access to regulators and mentors; connections to outside funding sources; potential clients; and working space to fintech firms and start-ups.

**Figure 6: Select Knowledge-Building Initiatives among U.S. Federal and Other Jurisdictions' Regulators**

	U.S. Financial Regulatory Agencies									United Kingdom	Singapore	Hong Kong
	CFPB	CFTC	FDIC	Federal Reserve	FINRA	FTC	NCUA	OCC	SEC			
Sandbox	--	--	--	--	--	--	--	--	--	○	○	○
Regulatory relief tool <sup>a</sup>	○	○	--	--	--	--	--	--	○	○	○	○
Pilot programs	○	--	--	--	--	--	--	○	--	--	--	--
Proofs of concepts	--	--	--	--	--	--	--	--	--	○	○	○
Innovation competitions	--	○	--	--	○	○	--	--	--	--	○	--
Accelerator	--	--	--	--	--	--	--	--	--	--	○	○

- No program  
 ○ Programs that are being developed  
 ● Established programs

Source: GAO analysis of agency and firm interviews and agency documents in the U.S. and abroad. | GAO-18-254

Notes: Following are the acronym definitions for each of the U.S. regulators—CFPB is Consumer Financial Protection Bureau; CFTC is Commodity Futures Trading Commission; FDIC is Federal Deposit Insurance Corporation; Federal Reserve is Board of Governors of the Federal Reserve System; FINRA is Financial Industry Regulatory Authority; FTC is Federal Trade Commission; NCUA is National Credit Union Administration; OCC is Office of the Comptroller of the Currency; and SEC is Securities and Exchange Commission.

Following are the agencies for each foreign jurisdiction in the figure—United Kingdom agencies are the Bank of England, Financial Conduct Authority, and Her Majesty's Treasury; Singapore agencies are the Monetary Authority of Singapore and SG Innovate; and Hong Kong agencies are Cyberport, Hong Kong Monetary Authority, and Hong Kong Securities and Futures Commission.

<sup>a</sup>Regulatory relief tools include no action letters (a letter stating that the staff of a regulator will not recommend enforcement action against a firm following specified practices), trial disclosure waivers, regulatory waivers, and regulatory modifications.

## Regulatory Sandboxes

One approach regulators abroad were using to learn about fintech activities was regulatory sandboxes. While a few U.S. regulators have undertaken efforts that are similar to regulatory sandboxes, most have not. Two regulators that we interviewed stated that tools already exist, such as the comment process, to fulfill the role of a sandbox by helping them better understand innovation and assist in the development of rules and guidance. However, other U.S. regulators said that creating regulatory sandboxes by using tools such as No Action Letters could benefit regulators and firms. Based on our analysis of selected jurisdictions' efforts, regulatory sandbox programs generally may include the following elements:

- firms apply to participate;

- 
- firms and regulators agree on the parameters of how products or services will be tested, such as the number of consumers or transactions included in the test, the required product disclosures, or the time frame of the test;
  - firms secure the appropriate licenses, if applicable; and
  - firms and regulators interact regularly.

In some cases, the sandbox may include limited regulatory relief. For example, UK regulators we interviewed noted that they can waive or modify a rule, issue a “no enforcement action” letter, or provide a restricted license for a firm participating in the sandbox. However, these tools are used on a case-by-case basis for the duration of the sandbox test, are not used for every participating firm, and would not limit any consumer protections. Further, UK regulators we interviewed said that while waiving or modifying rules is possible, they are only used on an exceptional basis. Similarly, Singapore regulators said that they can relax specific legal and regulatory requirements, such as capital requirements, on a case-by-case basis for firms while they are participating in the sandbox. Also, Hong Kong regulators allow firms to operate without full regulatory compliance for the limited product offerings within the sandbox. Similar to UK and Singapore regulators, Hong Kong regulators we interviewed said that they have put safeguards in place to protect consumers from and manage the risk of the regulatory relief. For a more detailed description of the Hong Kong, Singapore, and UK sandboxes, see appendix III.

Regulators and market participants we interviewed abroad said that these fintech sandboxes have helped regulators better understand products and more effectively determine appropriate regulatory approaches while limiting the risk that the failure of a fintech firm could pose to consumers. Some participating firms we interviewed told us they benefited by being able to test products with customers, make changes to their business model, and understand how their products would be regulated. Moreover, two participating firms and a regulator we interviewed said that firms are able to introduce their products to the market more quickly because they are able to test their products in the market while becoming compliant with laws and regulations. One fintech firm that participated in the UK sandbox pointed out that the UK regulators better understood their firm’s technology and business model because of interactions in the sandbox. For example, although the company and regulatory officials had previously disagreed on whether the firm’s product needed to be regulated, after gaining a better understanding of the company’s business



---

model through interactions in the sandbox, the regulatory officials agreed that the product did not require regulatory oversight. Similarly, Singapore regulators we interviewed noted that their sandbox provides them a hands-on approach to learning about new technologies and how the technologies align with regulatory requirements.

Some U.S. regulators have programs that share some characteristics with sandboxes. As shown in figure 6, CFPB, SEC, and CFTC have issued No Action Letters in which agency staff state that they do not intend to recommend certain regulatory action against the firms if they offer the products in the way described in a request letter to the regulator. The issuance of such letters could assist fintech firms in cases in which the applicability of existing regulations to their product is unclear. However, similar to sandboxes abroad, CFPB officials stated that No Action Letters do not provide safe harbor for companies taking actions that are clearly not allowed under U.S. consumer regulations. As of March 6, 2018, CFPB had issued one No Action Letter to Upstart Network, a company that uses alternative data to assess creditworthiness and underwrite loans.<sup>147</sup> As a condition of the No Action Letter, Upstart will regularly report lending and compliance information to CFPB to mitigate risk to consumers and inform CFPB about the impact of alternative data on lending decisions.

In addition, CFPB officials we interviewed said that they can use a similar tool known as trial disclosure waivers, which allow industry participants to seek CFPB approval to test an innovative disclosure or way of delivering a disclosure to consumers that includes a safe harbor provision during which the industry participant may be exempted from statutory or regulatory requirements.<sup>148</sup> As of March 6, 2018, CFPB had not issued any trial disclosure waivers.

Through its Project Catalyst, CFPB has also established a research pilot program where it collaborates with firms that are testing innovative products to understand consumer use and policy implications of innovative products. CFPB officials said that research pilots have similar elements to sandboxes, including participant application, agreement of testing parameters, and regular meetings between CFPB and the

---

<sup>147</sup>Consumer Financial Protection Bureau, *No-Action Letter to Upstart Network, Inc.* (Washington, D.C.: September 2017).

<sup>148</sup>CFPB has authority to offer trial disclosure waivers under section 1032(e) of the Dodd-Frank Act. See Pub. L. No. 111-203, § 1032(e); 124 Stat. 1376, 2007 (2010) (codified at 12 U.S.C. § 5532(e)).

---

participating firm. Four firms have concluded research pilots with CFPB and three other firms are currently participating in pilots. Similarly, OCC officials said that they are considering developing a pilot program, which will allow banks or fintech firms partnering with banks to test innovative products with the involvement and interaction of OCC staff. OCC officials said that they have not set a date for determining whether to go forward or implement the program.

## Proofs of Concept

Another approach regulators abroad were using to learn about fintech activities was establishing proofs of concept. The proofs of concept that we studied are similar to sandboxes in that the regulator has regular interaction with the company to better understand the product or technology, but the product is not introduced into the market during the proof of concept period. For example, the Bank of England, through its Accelerator program, uses proofs of concept to have firms develop technology that can help the agency improve its operations, according to agency officials. The Hong Kong Monetary Authority, which, among other things, regulates banks in its jurisdiction, uses proofs of concept to allow industry participants to develop products that are conceptual and not ready for market implementation. A firm we interviewed that participated in a proof of concept with Hong Kong Monetary Authority said that it offered the regulator the opportunity to gain a working understanding of the technology, while providing a test environment for the company to tailor the technology to adhere to regulatory requirements.

CFTC officials noted that they are exploring the ability to conduct proofs of concept through LabCFTC. CFTC officials noted that the agency would be well positioned to conduct proofs of concept because they already collect large amounts of market data that could potentially be leveraged for such projects. However, CFTC officials expressed concerns that receiving services as part of proofs of concept may violate gift or procurement laws.<sup>149</sup> The Federal Reserve Bank of Boston participates in a collaborative effort called Hyperledger, which serves a similar purpose as a proof of concept for the Federal Reserve Bank. Hyperledger is a collaborative effort involving public and private entities created to advance

---

<sup>149</sup>Federal agencies are required to award government contracts in accordance with numerous acquisition laws and regulations, and federal agencies are prohibited from accepting voluntary services for the United States, among other things, under the Antideficiency Act. See 31 U.S.C. § 1342. Federal employees are prohibited from accepting anything of value from a person seeking official action from, doing business with, or conducting activities regulated by the employing agency. See 5 U.S.C. § 7353(a); 5 C.F.R. pt. 2635, subpt. B.

---

the use of blockchain technologies across various sectors. As observers in the Hyperledger, Federal Reserve Bank staff have gained hands-on experience with blockchain technology by experimenting with uses of the technology. None of the other regulators with whom we spoke said that they planned to conduct proofs of concept.

#### Innovation Competitions or Awards

Another approach used by regulators abroad for learning about fintech activities was establishing fintech competitions or awards to encourage financial innovation. Winning firms receive recognition, contracts, or cash prizes. For example, the Monetary Authority of Singapore operated an international competition called Hackcelerator to crowdsource innovative solutions to problems that Singaporean financial institutions identified, including insurance, customer identification, and data analytics, according to officials. Singapore regulators have also established FinTech Awards, which provide ex-post recognition to FinTech solutions that have been implemented. CFTC officials said that they are seeking public input to establish prize competitions and intend to launch such competitions in 2018. FTC officials said that in 2017, the agency challenged participants to create a technical solution, or tools, that consumers could use to guard against security vulnerabilities in software found on the Internet of Things devices in their homes.<sup>150</sup> FINRA staff noted that the agency holds internal innovation competitions, called CREATEathons, in which FINRA staff compete to develop solutions to various problems identified internally by staff. While external parties do not participate in these competitions, teams can consult with firms. Some U.S. regulators pointed out that while some regulators abroad are mandated to promote competition, no such mandate exists among most U.S. financial regulators.<sup>151</sup>

#### Agency-led Incubator or Accelerator

Two governments we studied abroad were also learning about fintech by establishing incubators or accelerators to encourage the development of a country's fintech industry and talent pool. The accelerators provide funding, access to regulators and mentors, connections to outside funding

---

<sup>150</sup>The Internet of Things refers to the technologies and devices that sense information and communicate it to the Internet or other networks and, in some cases, act on that information. GAO, *Technology Assessment: Internet of Things: Status and implications of an Increasingly Connected World*, [GAO-17-75](#) (Washington, D.C.: May 15, 2017).

<sup>151</sup>Regulators in some other jurisdictions are mandated to encourage market competition. For example, according to the UK Financial Conduct Authority, the agency's objective is promoting effective competition in consumers' interests in regulated financial services. The agency also has a competition duty. Together, this mandate empowers the agency to identify and address competition problems and requires the agency to adopt a more procompetition approach to regulation, Financial Conduct Authority staff said.

---

sources, potential clients, and working space to fintech firms and start-ups. For example, officials we interviewed from SG Innovate, Singapore's government led accelerator, said that the agency helps Singaporean businesses expand overseas, bring companies to Singapore, and connect start-ups to regulators and funding, among other things. None of the U.S. regulators we interviewed said that they planned to establish such accelerator programs. Regulators from the U.S. and abroad pointed out that the U.S. fintech industry is more developed than those of other jurisdictions with many fintech firms, large talent pools, and significant amounts of private funding or privately run accelerators.

Regulators and market participants we interviewed abroad said that these knowledge-building initiatives have helped regulators learn about new products and business models and have allowed firms to test products. Although CFTC and SEC can issue No Action Letters, those agencies have not adopted other approaches similar to these knowledge-building initiatives described above. Further, FDIC, the Federal Reserve, and NCUA have not adopted any of these approaches. U.S. regulators said that these initiatives could raise concerns about favoring certain competitors over others and also noted that they may not have the authority to initiate these programs. However, despite similar potential constraints with regard to competition and authority limitations, CFPB and OCC have formally evaluated undertaking relevant knowledge-building initiatives, through conversations with regulators abroad, general research, and documentation of their efforts; and they have begun developing similar approaches, according to agency officials.

A characteristic of an effective financial regulatory system we identified in our 2009 framework was that a regulatory system should be flexible and forward looking, which would allow regulators to readily adapt to market innovations and changes. Consideration by U.S. regulators of adopting approaches taken by regulators abroad, where appropriate, could result in the implementation of initiatives that help improve their overall ability to oversee fintech and how it affects the entities they currently regulate. While constraints may limit the ability or willingness of regulators to fully adopt these practices, opportunities exist to assess ways to tailor them to the U.S. context.

## Regulators in the U.S. and Abroad Have Adopted Approaches to Facilitate Coordination on Financial Innovation

Regulatory coordination is less of an issue for regulators abroad because most jurisdictions have fewer financial regulators. For example, the UK has 3 agencies involved in financial regulation, Singapore has 1 financial regulator, and Hong Kong has 4 financial regulators, compared to the 10 federal agencies involved in the regulation of fintech in some capacity in the United States. However, regulators abroad have undertaken efforts to bolster coordination among domestic regulators—as applicable—as well as regulators abroad and industry representatives (see fig. 7). These collaborative efforts include advisory councils and steering committees dedicated to fintech issues; and fintech-specific cooperation agreements.

**Figure 7: Select Regulatory Coordination Initiatives among U.S. Federal and Other Jurisdictions’ Regulators**

	U.S. Financial Regulatory Agencies									United Kingdom	Singapore	Hong Kong
	CFPB	CFTC	FDIC	Federal Reserve	FINRA	FTC	NCUA	OCC	SEC			
Fintech advisory council	--	●	--	--	●	--	--	--	--	--	●	●
Fintech steering committee	--	--	●	--	●	--	--	●	--	--	●	●
Fintech-specific cooperation agreements	--	●	--	--	--	--	--	--	--	●	●	●
Fintech-related interagency collaborative group	●	--	●	●	--	●	●	●	●	--	--	--

- No program
- Programs that are being developed
- Established programs

Source: GAO analysis of agency and firm interviews and agency documents in the U.S. and abroad. | GAO-18-254

Notes: Fintech refers to traditional financial services provided by nontraditional technology-enabled providers.

Following are the acronym definitions for each of the U.S. regulators—CFPB is Consumer Financial Protection Bureau; CFTC is Commodity Futures Trading Commission; FDIC is Federal Deposit Insurance Corporation; Federal Reserve is Board of Governors of the Federal Reserve System; FINRA is Financial Industry Regulatory Authority; FTC is Federal Trade Commission; NCUA is National Credit Union Administration; OCC is Office of the Comptroller of the Currency; and SEC is Securities and Exchange Commission.

Following are the agencies for each foreign jurisdiction in the figure—United Kingdom agencies are the Bank of England, Financial Conduct Authority, and Her Majesty’s Treasury; Singapore agencies are the Monetary Authority of Singapore and SG Innovate; and Hong Kong agencies are Cyberport, Hong Kong Monetary Authority, and Hong Kong Securities and Futures Commission.

---

## Fintech Advisory Councils and Steering Committees

In the jurisdictions we examined, two agencies have established fintech advisory councils or steering committees of industry participants and government officials. Fintech advisory councils and steering committees may provide a valuable connection to industry, through which U.S. regulators could gain insight into industry developments. For example, the Hong Kong securities regulator has established an advisory council comprised of members with knowledge and experience of various parts of Hong Kong's fintech industry. Officials of this agency told us that the advisory council provides valuable market data, a forum that offers firms a preliminary check for interpretation of their rules and updates on emerging issues. Advisory council members said that the council gives this regulator a cross-functional perspective from industry experts and enables the agency to learn about emerging issues and related regulatory challenges early in their development.

Selected U.S. regulators have established formal advisory committees dedicated to fintech issues, as shown in figure 7.

- FINRA has established a Fintech Industry Committee through which FINRA member and nonmember firms are provided a platform for ongoing dialogue and analysis of fintech developments related to FINRA's purview. FINRA officials said that the agency has also established the FinTech Advisory Group, a forum to identify and prioritize FinTech topics and coordinate appropriate regulatory approaches with key stakeholders.
- CFTC staff noted that the agency restarted its Technology Advisory Committee in late 2017 to explore a range of fintech topics and augment the work of LabCFTC.
- FDIC officials noted that the agency has a Fintech Steering Committee, which aims to help FDIC understand fintech developments by identifying, discussing, and monitoring fintech trends through reports from the staff working groups that the steering committee has established. The Fintech Steering Committee had not made any formal recommendations as of March 13, 2018.

As previously mentioned, U.S. regulators we interviewed said that they have coordinated with other regulators and industry through various mechanisms, as the following examples illustrate. (For additional information on interagency collaborative efforts, see app. II).

- The Federal Reserve has coordinated with relevant industry participants and other regulators including CFPB, FDIC, FTC, NCUA,

---

OCC, Treasury, and CSBS through its Mobile Payments Industry Working Group and its Faster Payments Task Force.

- FTC solicits insight from industry participants, observers, and regulators through its fintech forums.
- Regulators have also coordinated with each other through domestic and international interagency financial regulatory bodies, as well as a recently organized interagency collaborative group dedicated to fintech, the prudential regulators' Interagency Fintech Discussion Forum.

## Cooperation Agreements

Some regulators abroad have cooperation agreements with other regulators abroad to share information and to help fintech firms begin operations in other jurisdictions. For example, Singapore regulatory staff told us that the regulator has 16 such agreements with entities from 15 regions that typically consist of (1) referrals to regulatory counterparts for firms attempting to operate in a new country, (2) guidance to firms on regulation in the firm's new country of operation, and (3) information exchange among regulators and between regulators and fintech firms. UK regulators said that these agreements outline how the agencies in each country pledge to assist each other's fintech firms seeking to operate in their country with business-to-business contacts, office space, and other assistance. For example, regulators can discuss trends related to their authorities and share information on fintech firms seeking to expand operations in the other country. A fintech firm we interviewed said that because much financial innovation is international in scope, sharing information across borders with cooperation agreements is important for regulators to understand the new technologies and to be responsive to risks. On February 19, 2018, CFTC and UK Financial Conduct Authority signed a cooperation agreement, which, according to CFTC officials, will focus on information sharing and facilitate referrals of fintech companies interested in entering the other regulator's market. None of the other U.S. regulators that we interviewed had fintech-specific cooperation agreements with regulators abroad. Most of them said that existing memoranda of understanding were sufficient to facilitate information sharing. One regulator we interviewed abroad noted that establishing fintech-specific cooperation agreements with U.S. regulators is difficult because no direct regulatory counterpart exists since the U.S. financial regulatory structure is significantly different from those of other jurisdictions.

---

## Conclusions

The emergence of various fintech products has produced benefits to consumers and others. Fintech products often pose risks to those of

---

traditional financial products, although in some cases fintech products pose additional risks. While existing consumer protection and other laws apply to some fintech products and services, in some cases fintech transactions may not be covered by such protections. The extent to which the activities of fintech providers are subject to routine federal oversight varies, but fintech firms not overseen by a federal body generally are subject to oversight by state regulators. While limited evidence of widespread problems has surfaced to date, as the prevalence of fintech products grows, risks posed by segments of the industry that regulators do not routinely examine could correspondingly grow. Therefore, efforts by regulators to monitor developments and risks posed by these firms and their financial innovations remains a sound approach.

With fintech products spanning across financial sectors and jurisdictions of the numerous U.S. regulatory bodies, many parties have called for improved regulatory coordination. While regulators have taken steps to collaborate, opportunities remain to improve collaboration in line with GAO's leading practices. For example, the Interagency Fintech Discussion Forum and the biennial meetings of the Federal Reserve Mobile Payments Industry Workgroup do not include NCUA and FCC, respectively, agencies that could add valuable perspectives. Without these agencies, these efforts are not fully leveraging relevant agency expertise, and NCUA and FCC may be precluded from learning about risks that are relevant to their authorities.

Among other consumer protection issues related to financial account aggregation, market participants do not agree about whether consumers using account aggregators will be reimbursed if they experience fraudulent losses in their financial accounts. Until regulators coordinate and assist the industry in clarifying and balancing the valid interests of consumers, financial account aggregators, and financial institutions, consumers could have to choose between facing potential losses or not using what they may find to be an otherwise valuable financial service. Although regulators have been reluctant to act too quickly in light of related industry efforts, they could increase collaboration to address key issues such as consumer reimbursement for unauthorized transactions. Aligning ongoing collaborative efforts with leading practices could help regulators and market participants resolve disagreements over financial account aggregation and related consumer compliance issues more quickly and in a manner that balances the competing interests involved.

With our past work finding that an effective financial regulatory system needs to be flexible and forward looking to allow regulators to more



---

readily adapt and oversee new products, U.S. regulators could potentially improve their oversight of innovative fintech activities by considering adoption of some of the efforts already being successfully used by regulators abroad. While constraints may limit the ability or willingness of regulators to fully adopt these practices, opportunities exist to assess ways to tailor them to the U.S. context. Some U.S. regulators have established innovation offices that can help fintech providers more easily obtain needed information from relevant regulators; however, FDIC and NCUA have not established such offices, which could help facilitate these regulators' interactions with fintech firms and with the entities they regulate. Also, initiatives such as regulatory sandboxes or proofs-of-concept that provide fintech firms the opportunity to operate and share information with appropriate regulators have helped regulators abroad educate their staff and thereby improve their oversight capacities. However, the Federal Reserve, CFTC, FDIC, NCUA, and SEC have not initiated such programs due to concerns about favoring certain competitors over others or that they may not have the authority to initiate these programs. While constraints may limit the ability or willingness of regulators to fully adopt these practices, additional consideration by these regulators of some of the approaches taken by regulators abroad could assist U.S. regulators in learning more about new financial technologies that could provide useful knowledge for their own regulatory activities.

---

## Recommendations for Executive Action

We are making a total of sixteen recommendations.

The Chair of the Board of Governors of the Federal Reserve System should invite NCUA to participate in the Interagency Fintech Discussion Forum. (Recommendation 1)

The Chairman of the Federal Communications Commission (FCC) should discuss with the Presidents of the Federal Reserve Banks of Atlanta and Boston whether the topics of the 2018-2019 biennial regulators meeting of the Federal Reserve's Mobile Payments Industry Working Group would make FCC participation beneficial to the FCC or the group, and take steps accordingly. (Recommendation 2)

The President of the Federal Reserve Bank of Atlanta should discuss with the Chairman of the FCC and the President of the Federal Reserve Banks of Boston whether the topics of the 2018-2019 biennial regulators meeting of the Federal Reserve's Mobile Payments Industry Working Group would make FCC participation beneficial to the FCC or the group, and take steps accordingly. (Recommendation 3)

---

The President of the Federal Reserve Bank of Boston should discuss with the Chairman of the FCC and the President of the Federal Reserve Banks of Atlanta whether the topics of the 2018-2019 biennial regulators meeting of the Federal Reserve's Mobile Payments Industry Working Group would make FCC participation beneficial to the FCC or the group, and take steps accordingly. (Recommendation 4)

The Director of the Consumer Financial Protection Bureau should engage in collaborative discussions with other relevant financial regulators in a group that includes all relevant stakeholders and has defined agency roles and outcomes to address issues related to consumers' use of account aggregation services. (Recommendation 5)

The Chair of the Board of Governors of the Federal Reserve System should engage in collaborative discussions with other relevant financial regulators in a group that includes all relevant stakeholders and has defined agency roles and outcomes to address issues related to consumers' use of account aggregation services. (Recommendation 6)

The Chairman of the Federal Deposit Insurance Corporation should engage in collaborative discussions with other relevant financial regulators in a group that includes all relevant stakeholders and has defined agency roles and outcomes to address issues related to consumers' use of account aggregation services. (Recommendation 7)

The Chairman of the National Credit Union Administration should engage in collaborative discussions with other relevant financial regulators in a group that includes all relevant stakeholders and has defined agency roles and outcomes to address issues related to consumers' use of account aggregation services. (Recommendation 8)

The Comptroller of the Currency should engage in collaborative discussions with other relevant financial regulators in a group that includes all relevant stakeholders and has defined agency roles and outcomes to address issues related to consumers' use of account aggregation services. (Recommendation 9)

The Chairman of the Federal Deposit Insurance Corporation should formally evaluate the feasibility and benefit of establishing an office of innovation or clear contact point, including at least a website with a dedicated email address. (Recommendation 10)

---

The Chairman of the National Credit Union Administration should formally evaluate the feasibility and benefit of establishing an office of innovation or clear contact point, including at least a website with a dedicated email address. (Recommendation 11)

The Chair of the Board of Governors of the Federal Reserve System should formally evaluate the feasibility and benefits to their regulatory capacities of adopting certain knowledge-building initiatives related to financial innovation. (Recommendation 12)

The Chairman of the Commodity Futures Trading Commission should formally evaluate the feasibility and benefits to their regulatory capacities of adopting certain knowledge-building initiatives related to financial innovation. (Recommendation 13)

The Chairman of the Federal Deposit Insurance Corporation should formally evaluate the feasibility and benefits to their regulatory capacities of adopting certain knowledge-building initiatives related to financial innovation. (Recommendation 14)

The Chairman of the National Credit Union Administration should formally evaluate the feasibility and benefits to their regulatory capacities of adopting certain knowledge-building initiatives related to financial innovation. (Recommendation 15)

The Chairman of the Securities and Exchange Commission should formally evaluate the feasibility and benefits to their regulatory capacities of adopting certain knowledge-building initiatives related to financial innovation. (Recommendation 16)

---

## Agency Comments and Our Response

We provided a draft of this report to CFPB; CFTC; FCC; FDIC; the Federal Reserve; FTC; NCUA; OCC; SEC; and Treasury, as well as CSBS and FINRA. We received written comments from all of these agencies except for Treasury and FINRA; the comments are reprinted in appendixes IV through XII, respectively. Agencies to which we directed recommendations agreed with our recommendations, as detailed below. All of these agencies except FCC and NCUA also provided technical comments, which we incorporated as appropriate.

In response to our recommendation that CFPB engage in collaborative discussions that incorporate leading practices with other financial regulators on financial account aggregation issues, CFPB stated in its

---

letter that it concurred. CFPB stated that it has taken steps to address related issues independently. CFPB also noted that it has participated in related ongoing collaborative discussions and that it would continue to do so.

CFTC concurred with our recommendation that it formally evaluate adopting knowledge-building initiatives related to financial innovation. CFTC also noted that it is either using or exploring the use of some of the knowledge-building initiatives identified in the report. However, the agency also raised concerns that, without targeted legislative changes, some of those initiatives may violate federal procurement laws and gift prohibitions.

In its letter, FCC agreed with our recommendation that it should discuss with the Presidents of the Federal Reserve Banks of Atlanta and Boston whether the topics of the 2018–2019 biennial regulator meeting of the Federal Reserve’s Mobile Payments Industry Working Group would make FCC participation beneficial to FCC or the group, and take steps accordingly. FCC noted that it will reach out to the Federal Reserve Banks of Atlanta and Boston to determine whether FCC participation would be beneficial.

Regarding our recommendation that FDIC engage in collaborative discussions that incorporate leading practices with other financial regulators on financial account aggregation issues, FDIC stated in its letter that it recognizes the benefits of engaging in collaborative discussions with other relevant regulators. It noted that it has been involved in ongoing collaborative discussions about such issues and that it would continue to do so, particularly regarding liability for unauthorized transactions and consumer reimbursement. Regarding our recommendation that FDIC formally evaluate the feasibility and benefit of establishing an Office of Innovation or clear contact point, FDIC stated that it would conduct such an evaluation, and acknowledged that it has a long history of engaging in open dialogue with any party interested in discussing matters related to FDIC’s mission and responsibilities. Regarding our recommendation that it formally evaluate adopting knowledge building initiatives related to financial innovation, FDIC stated that it recognizes the importance of knowledge building and has developed a framework and implemented initiatives to facilitate this. It also noted that it will continue ongoing efforts to build knowledge related to financial innovation and will consider other relevant knowledge building initiatives, as appropriate.

---

In response to our recommendations that the Federal Reserve include NCUA and FCC in relevant working groups, the Federal Reserve stated in its letter that its Board staff would seek NCUA's participation and that staff from the Reserve Banks in Atlanta and Boston would discuss FCC's participation in relevant working groups. Regarding our recommendation that the Federal Reserve engage in collaborative discussions that incorporate leading practices with other financial regulators regarding financial account aggregation issues, the Federal Reserve acknowledged the importance of working together to ensure that consumers were protected, and noted a variety of ways it already coordinates on such issues, and noted that it will continue to engage in such discussions to address the important issues surrounding reimbursement for consumers using these services. Regarding our recommendation that it formally evaluate adopting knowledge-building initiatives related to financial innovation, the Federal Reserve noted that it recognizes the importance of such efforts and has recently organized a team of experts to ensure that fintech-related information is shared across its organization.

NCUA stated in its letter that it concurred with our recommendations to engage in collaborative discussions that incorporate leading practices with other financial regulators on financial account aggregation issues, formally evaluate the feasibility and benefit of establishing an office of innovation or clear contact point, and formally evaluate the feasibility and benefits to their regulatory capacities of adopting certain knowledge-building initiatives related to financial innovation. NCUA noted that evaluations of fintech activities are challenging for NCUA because it does not have vendor authority like the other federal banking regulators. We have previously raised NCUA's lack of vendor authority as a matter for congressional consideration. NCUA stated it will continue to monitor risks posed by fintech firms to the credit union industry by working with the banking regulators.

Regarding our recommendation that OCC engage in collaborative discussions that incorporate leading practices with other financial regulators on financial account aggregation issues, OCC stated in its letter that it recognizes the importance of this recommendation. It noted that it has been involved in ongoing collaborative discussions about such issues and that it would continue to do so.

SEC stated in its letter that it concurred with our recommendation to formally evaluate the feasibility and benefits to their regulatory capacities of adopting certain knowledge-building initiatives related to financial

---

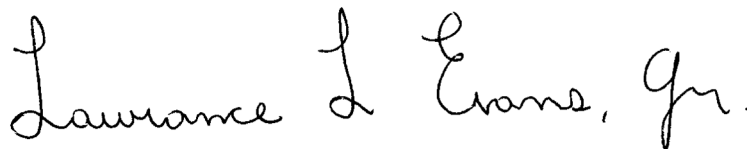
innovation. SEC also stated that it will coordinate with other agencies as appropriate during its assessment.

In its letter, CSBS drew connections between steps that state regulators have taken and those that we are recommending to federal agencies. CSBS also provided additional information regarding state licensing requirements, which we incorporated into our report. Additionally, CSBS expressed support for our recommendations on federal interagency collaboration and stated that it would support related efforts that respected the role of state regulators. In addition, CSBS said that these efforts could benefit from the participation of state regulators and that it would be willing to participate if invited. Similarly, CSBS expressed support for our recommendations that certain federal agencies formally evaluate the feasibility and benefit of establishing an office of innovation or clear contact point and formally evaluate the feasibility and benefit of adopting knowledge-building initiatives related to financial innovation. However, CSBS also cautioned that knowledge-building initiatives should not preempt state consumer protection and licensing laws for fintech payment providers or fintech lenders.

---

As agreed with your offices, we are sending this report to the appropriate members of Congress; CFPB; CFTC; FCC; FDIC; the Board of Governors of the Federal Reserve; FTC; NCUA; OCC; SEC; and Treasury, as well as CSBS and FINRA. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-8678 or [evansl@gao.gov](mailto:evansl@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.

A handwritten signature in black ink that reads "Lawrence L. Evans, Jr." The signature is written in a cursive, flowing style.

Lawrance L. Evans, Jr.  
Managing Director, Financial Markets and Community Investment

---

### *List of Requesters*

The Honorable Thomas R. Carper  
Ranking Member  
Permanent Subcommittee on Investigations  
Committee on Homeland Security and Governmental Affairs  
United States Senate

The Honorable Chris Coons  
United States Senate

The Honorable Gary C. Peters  
United States Senate

The Honorable Rick W. Allen  
House of Representatives

The Honorable Buddy Carter  
House of Representatives

The Honorable Randy Hultgren  
House of Representatives

The Honorable Michael McCaul  
House of Representatives

The Honorable Patrick McHenry  
House of Representatives

The Honorable Robert Pittenger  
House of Representatives

The Honorable Jared Polis  
House of Representatives

The Honorable Scott R. Tipton  
House of Representatives

The Honorable Ann Wagner  
House of Representatives

The Honorable Rob Woodall  
House of Representatives

---

# Appendix I: Objectives, Scope, and Methodology

---

This report examines (1) fintech benefits, risks, and extent of legal or regulatory protections for users; (2) efforts by U.S. regulators to oversee fintech activities; (3) challenges that the regulatory environment poses to fintech firms; and (4) the steps taken by domestic and other countries' regulators to encourage financial innovation within their countries.

While fintech does not have a standard definition, for the purposes of this report we focused on products and services leveraging technological advances offered by financial institutions; nonbank financial companies; and technology companies within the payment, lending, and wealth management sectors, as well as products or services operating under distributed ledger technology (DLT). Within these four identified sectors, we examined particular products and services. In the payments technologies sector we limited our scope to mobile wallets, peer-to-peer payments, and peer-to-business payments products and services. To identify these four sectors, we conducted background research and reviewed prior GAO reports on fintech, person-to-person lending, and virtual currencies. In the fintech lending sector, we focused on consumer lending—including credit card and home improvement loans—and small business lending services from direct and platform lending models; however, we did not include mortgage lending in our scope, due to the significant amount of regulation within the subsector. In the digital wealth management sector, we examined firms that exclusively offer advice using algorithms based on consumers' data and risk preferences to assist or provide investment recommendations and financial advice directly to consumers. We also examined issues relating to fintech account aggregation companies that consolidate and display data from consumers' accounts across financial institutions to help consumers more easily see their overall financial health. For DLT, we focused on providers that used DLT in payments and securities processing and token sales. We also included information on the use of DLT in virtual currencies, such as bitcoin and Ethereum. We also reviewed available data on transaction volumes for the payments, lending, and robo advising sectors.

To identify the benefits provided and risks posed to consumers by fintech services, we conducted a literature review of agency, industry participant, and industry observer documents that analyzed developments within fintech. Using ProQuest, Scopus, SSRN, and Nexis.com databases in the literature review, we identified over 500 relevant articles out of over 1,100 search results by using search terms associated with the four fintech subsectors mentioned above. Our search included articles from 2011 to October 2017. To determine the usefulness of the studies for inclusion, we conducted a review of search results involving multiple content



reviews by GAO analysts to determine which relevant articles could (1) provide credible sources of information to help address our researchable questions, or (2) help identify knowledgeable persons or groups to interview. We excluded documents based on the following criteria that eliminated articles that were (1) duplicated; (2) related to countries outside our review; (3) about virtual currencies; (4) categorized as “marginally relevant” by analysts based on the article’s title, publication date, and source; (5) less recent documents from each author or source; (6) from news outlets or nonauthoritative sources; or (7) deemed irrelevant or not useful.

To obtain the financial services and fintech stakeholder perspectives on fintech benefits and risk, we reviewed academic papers, reports, and studies by other organizations on fintech activities we identified through a literature search. We also conducted over 120 interviews with financial regulators; banks; fintech providers; consumer groups; trade associations; academics; think tanks; and consulting and law firms. We identified potential interviewees by conducting Internet research; reviewing literature search results; reviewing recommended interviewees from our initial interviews; and selecting interviewees based on their relevance to the scope of our review. We selected fintech firms and financial intuitions, industry observers, and federal agencies based on the product or service conducted by the firm, expertise of the industry observers, and oversight authority of the federal agencies. We identified fintech benefits and risk by speaking with relevant regulators and other knowledgeable parties including: the Board of Governors of the Federal Reserve System (Federal Reserve); the Federal Deposit Insurance Corporation (FDIC); the National Credit Union Administration (NCUA); the Office of the Comptroller of the Currency (OCC); the Commodity Futures Trading Commission (CFTC); the Bureau of Consumer Financial Protection, known as the Consumer Financial Protection Bureau (CFPB); the Department of the Treasury (Treasury); the Federal Communications Commission; Federal Trade Commission (FTC); the Financial Industry Regulatory Authority (FINRA), the Securities and Exchange Commission (SEC); and the Small Business Administration.

To obtain state-level perspectives we interviewed representatives of the Conference of State Bank Supervisors (CSBS), National Association of Attorneys General, Money Transmitter Regulators Association, National Association of State Credit Union Supervisors, and the North American Securities Administrators Association. We also interviewed staff from three state financial regulatory agencies in states with active fintech firms and regulatory activities: California, Illinois, and New York.

To assess the regulatory environment and various challenges faced by fintech firms, we identified relevant laws and regulations pertaining to fintech companies within our scope by reviewing prior GAO reports on financial regulation and fintech, interviewed agency staff and industry participants, and analyzed relevant agency documents, including relevant laws and regulations.<sup>1</sup> We also reviewed guidance; final rulemakings; initiatives; and enforcement actions from agencies. To obtain federal regulatory perspectives, we interviewed staff from the Federal Reserve, FDIC, NCUA, OCC, CFTC, CFPB, Treasury, FTC, FINRA, SEC, and SBA.

To determine the steps taken by domestic and other countries' regulators to encourage financial innovation in their countries, we conducted fieldwork—including interviews with regulatory agencies, fintech firms, and industry observers, as well as, observations of fintech programs—in the United Kingdom, Singapore, and Hong Kong. We also conducted interviews with a regulatory organization and fintech firms operating in Canada. We identified and selected countries for our fieldwork through criteria that focused on the extent to which these locations had significant (1) financial services activities, (2) fintech activities, and (3) fintech regulatory approaches. We conducted Internet research, literature searches, and interviews to identify relevant foreign regulators within the selected fieldwork sites. To obtain other countries' regulator perspectives, we interviewed and analyzed agency documents on regulatory efforts and views on fintech innovations within their financial markets from regulators in Hong Kong, Singapore, and the United Kingdom. To obtain the perspective of fintech firms operating in the selected fieldwork sites, we conducted Internet research, literature searches, and interviews to determine relevant fintech firms and foreign trade associations, including recommendations from domestic industry participants and observers.

We conducted this performance audit from initiation August 2016 to March 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for

---

<sup>1</sup>Among other reports, we used the following prior GAO reports to determine relevant financial regulations: GAO, *Financial Technology: Information on Subsectors and Regulatory Oversight*, [GAO-17-361](#) (Washington, D.C.: Apr. 19, 2017), *Financial Regulation: Complex and Fragmented Structure could be Streamlined to Improve Effectiveness*, [GAO-16-175](#), (Washington, D.C.: Feb. 25, 2016), and *Virtual Currencies: Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges*, [GAO-14-496](#), (Washington, D.C.: May 29, 2014).

---

our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

# Appendix II: Interagency Collaborative Efforts That Have Addressed Fintech Issues

---

In this appendix, we present interagency working groups (including task forces and other interagency collaborative bodies) that have discussed fintech issues, and in some cases, taken specific actions. This list includes interagency groups that are dedicated exclusively to fintech as well as those that may discuss fintech as part of their broader financial regulatory focus. Also, it includes interagency groups that operate at both the domestic and international levels (see tables 2 and 3). This list is based on information we obtained from the federal financial regulatory agencies we met with and is not intended to be an exhaustive list.

**Appendix II: Interagency Collaborative Efforts  
That Have Addressed Fintech Issues**

**Table 2: Domestic Interagency Fintech Collaboration Efforts**

<b>Name of group</b>	<b>Participating agencies</b>	<b>Mission/goals</b>	<b>Ways in which group addresses fintech</b>
Interagency Fintech Discussion Forum	The Board of Governors of the Federal Reserve System (Federal Reserve) has convened (no official leader); other members include the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB).	To facilitate information sharing between the heads of the consumer divisions of the federal banking regulators on consumer protection issues as they relate to fintech and to preview related agency actions.	General Fintech. Created in March 2017, this informal group meets every 4 to 6 weeks and discusses the effect of fintech products and services on consumers. For example, the group has discussed the benefits and risks of using alternative data and models in lending, and related compliance management challenges; data aggregation; and bank management of third-party relationships with fintechs.
Federal Reserve Mobile Payments Industry Workgroup	Federal Reserve Banks of Boston and Atlanta convene; in addition to industry participants, meetings with government agencies include CFPB, FDIC, Federal Reserve, the Federal Trade Commission (FTC), the National Credit Union Administration (NCUA), OCC, the Department of the Treasury (Treasury), and the Conference of State Bank Supervisors (CSBS).	To facilitate discussions among the stakeholders as to how a successful mobile payments (as opposed to mobile banking) system could evolve in the United States.	Payments. Created in 2010, the Federal Reserve meets with industry members several times annually to discuss barriers and opportunities in mobile payments in the United States. The group focuses on the regulatory landscape, innovation, and financial inclusion, and has published numerous whitepapers. The group also conducts meetings with regulators that have responsibilities related to mobile payments in order to help keep industry members up to date on regulatory concerns, identify potential regulatory gaps, and educate regulators on mobile technologies.
Federal Reserve Faster Payments Task Force, May 2015 to August 2017	Federal Reserve convened; participants included a large number of market participants and consumer advocates, as well as CFPB, FTC, OCC, and Treasury.	Represented views on future needs for a safe, ubiquitous faster U.S. payments solution; assessed alternative approaches for faster payment capabilities; and addressed other issues deemed important to the successful development of effective approaches.	Payments. Meeting from 2015 through August 2017, this group developed a set of effectiveness criteria and published reports on the need for faster payments solutions, as well as a related assessment of proposed solutions and recommendations for industry next steps. These recommendations would apply to fintech developers and payment system providers.

**Appendix II: Interagency Collaborative Efforts  
That Have Addressed Fintech Issues**

<b>Name of group</b>	<b>Participating agencies</b>	<b>Mission/goals</b>	<b>Ways in which group addresses fintech</b>
Federal Reserve Secure Payments Task Force	Federal Reserve convenes; participants include market participants, as well as CFPB and Treasury.	Provide advice on payment security matters.  Coordinate with the Faster Payments Task Force to identify solutions for any new or modified payments infrastructure so that it is both fast and secure.  Determine areas of focus and priorities for future action to advance payment system safety, security and resiliency.	Payments. Created in 2015, working groups address issues including identity management, information sharing for mitigation of payments risk and fraud, data protection, and legal and regulatory coordination. The task force has studied eight use cases, including mobile wallets and contactless payments, and developed materials that outlined topics including security methods and risks, sensitive payment data and risks, and standards that it has shared with broader industry.
Federal Financial Institutions Examination Council Task Force on Supervision (FFIEC TFOS)	CFPB, FDIC, Federal Reserve, NCUA, OCC, and State Liaison Committee.	FFIEC TFOS coordinates and oversees matters related to safety and soundness supervision and examination of depository institutions.	Payments and Financial Account Aggregation. FFIEC TFOS added an appendix on mobile banking to the Retail Payments booklet of the FFIEC's IT Handbook and offered a related webinar, and has subgroups on IT (information technology), cybersecurity and critical infrastructure, and anti-money laundering (AML). The IT subgroup developed a paper on data aggregation and related consumer compliance issues, including consumer access to data, Electronic Fund Transfer Act (Regulation E), and Fair Credit Reporting Act. The paper was presented to TFOS in August 2017 and to TFCC in September 2017, and two task forces are considering how to best continue discussions on the matter.
FFIEC Task Force on Consumer Compliance (FFIEC TFCC)	CFPB, FDIC, Federal Reserve, NCUA, OCC, and State Liaison Committee.	FFIEC TFCC coordinates on matters related to consumer protection supervision and examination of depository institutions.	General Fintech. The FFIEC TFCC may consider matters related to fintech and other emerging trends, as appropriate. It has drafted updates to the Gramm-Leach-Bliley Act (Regulation P) examination updates, but this is not specific to fintech. In September 2017, members of the FFIEC TFOS IT subgroup also briefed the task force on consumer compliance implications related to data aggregation, and the two task forces are considering how to best continue discussions on the matter.
Interagency Working Group on Marketplace Lending	Treasury convened; participants included CFPB, FDIC, Federal Reserve, FTC, OCC, Small Business Administration (SBA), and Securities and Exchange Commission (SEC).	This group was created to share information, engage industry participants and public interest groups, and evaluate where additional regulatory clarity could protect borrowers and investors.	Fintech Lending. Met 3 times in 2016 to address Treasury's Marketplace Lending White Paper and such issues as the use of alternative data in credit and financial decision making, as well as the proper level of financial disclosures for small business borrowers. This group is not currently active.

Source: GAO analysis of agency information. | GAO-18-254

**Appendix II: Interagency Collaborative Efforts  
That Have Addressed Fintech Issues**

**Table 3: International Interagency Fintech Collaboration Efforts**

<b>Name of group</b>	<b>Participating agencies</b>	<b>Mission / goals</b>	<b>Ways in which group addresses fintech</b>
The Bank for International Settlements, Committee on Payments and Markets Infrastructure and Committee on the Global Financial System	Federal Reserve (committee chair) and the Federal Reserve Bank of New York represent the United States. Other members include other central banks.	Identify and assess potential sources of stress in global financial markets, further the understanding of the structural underpinnings of financial markets, and promote improvements to the functioning and stability of these markets.	Fintech Payments and Lending. From 2014 to February 2017, the Committee on Payments and Markets Infrastructure has published papers on a variety of fintech payments topics including DLT in payments, virtual currencies, faster payments, and nonbanks in retail payments papers. In May 2017, the Committee on the Global Financial System published a white paper (in collaboration with the Financial Stability Board's Financial Innovation Network) on the financial stability impacts of fintech credit.
Basel Committee on Banking Supervision's Task Force on Financial Technology (TFFT)	OCC co-chairs, and FDIC and Federal Reserve also represent the United States. Other participants include central banks and authorities with formal responsibility for the supervision of banking business.	TFFT assesses the risks and supervisory challenges associated with innovation and technological changes affecting banking.	General Fintech. TFFT's work is currently focused on the effect that fintech has on banks and banks' business models, and the implications this has for supervision. In 2016, TFFT drafted an internal paper on fintech issues. In August 2017, TFFT and the Bank for International Settlements jointly issued a consultative document on the implications of fintech developments for banks and bank supervisors.
Financial Action Task Force (FATF) Fintech & Regtech Forums	Treasury (lead), Federal Reserve and OCC represent the United States. Other members include agencies from other jurisdictions and two regional organizations, and associate members include other international and regional organizations.	Conduct industry outreach and provide a platform for a constructive dialogue and support innovation in financial services while addressing the regulatory and supervisory challenges posed by emerging technologies.	General Fintech. In 2017, FATF held three fintech-related events on fintech, regtech, and AML/counter-terrorist financing (CTF) covering topics including: relevance of emerging fintech trends to financial institutions; AML/CTF standards in fintech; how different jurisdictions approach the regulation and supervision of fintech; fintech's effect on AML/CTF-related information availability and exchange; and risk management and mitigation for fintech.
Financial Stability Board Financial Innovation Network	Federal Reserve, Federal Reserve Bank of New York, the Office of Financial Research, SEC, FDIC and OCC represent the United States. Other members include central banks and authorities with formal responsibility for the supervision of banking business..	The Financial Stability Board promotes international financial stability by coordinating national financial authorities and international standard-setting bodies as they work toward developing financial sector policies. The Financial Innovation Network is responsible for understanding emerging trends in financial services and the potential effect on financial stability.	General Fintech. In 2017, published white papers and a report on the financial stability implications of fintech credit (in collaboration with the Committee on the Global Financial System), the use of artificial intelligence (AI) and machine learning in financial services, and fintech supervisory and regulatory issues that merit authorities' attention.

**Appendix II: Interagency Collaborative Efforts  
That Have Addressed Fintech Issues**

<b>Name of group</b>	<b>Participating agencies</b>	<b>Mission / goals</b>	<b>Ways in which group addresses fintech</b>
International Credit Union Regulators Network (ICURN)	NCUA represents the United States. Other members include national and other supervisors of credit unions and financial cooperatives.	ICURN provides training to supervisors of credit unions and financial cooperatives on a variety of topics.	General Fintech. ICURN's July 2017 conference included a panel on understanding fintech and regulation. Discussion covered sectors including payments, lending, digital wealth management, and DLT.
International Organization of Securities Commissions (IOSCO), Committee on Emerging Risks	SEC and CFTC represent the United States. Other members include national and provincial securities regulators.	IOSCO brings together the world's securities regulators and works with the G20 and the Financial Stability Board (FSB) on the global regulatory reform agenda. The Committee on Emerging Risks provides a platform for securities regulators and economists to discuss emerging risks and market developments and to develop and assess tools to assist regulators in reviewing the regulatory environment and identifying, monitoring, and managing systemic risk.	General Fintech. In February 2017, the Committee on Emerging Risks published a research report on fintech, which included sections on fintech lending, digital investment advice, DLT, fintech in emerging markets, and other regulatory considerations. IOSCO also established an Initial Coin Offering Consultation Network, through which members can discuss their experiences and concerns regarding token sales, and has issued related statements to members and the public. In addition, IOSCO and the Bank for International Settlements Committee on Payments and Market Infrastructures have focused on fintech issues through the Joint Working Group on Digital Innovation, which has identified and assessed the implications of DLT and related technologies for post-trade processes such as clearing and settlement.

Source: GAO analysis of agency information. | GAO-18-254



---

# Appendix III: Regulatory Sandbox Examples

---

---

## Summary

Based on our review of the regulatory sandboxes of the United Kingdom (UK), Singapore, and Hong Kong, including interviews with regulators and participating firms and agency document reviews, certain characteristics were similarly present in all of the sandboxes, although some differences did exist. Regulatory sandbox programs in these countries generally included the following elements:

1. firms apply to participate;
2. firms and regulators agree on the parameters of how products or services will be tested, such as the number of consumers or transactions included in the test, the required product disclosures, or the time frame of the test;
3. firms secure the appropriate licenses, if applicable; and
4. firms and regulators interact regularly.
5. Below are descriptions of each jurisdiction's regulatory sandbox.

---

## UK Financial Conduct Authority's Regulatory Sandbox

According to officials, the purpose of the Financial Conduct Authority's (FCA) sandbox is to allow firms to test innovative products, services, or business models in a live market environment, while ensuring that appropriate protections are in place. FCA has stated that its sandbox has (1) reduced the time and cost of getting innovative ideas to market; (2) facilitated access to finance for innovators; (3) enabled products to be tested and introduced to the market; and (4) helped the agency build appropriate consumer protection safeguards into new products and services. The characteristics of the FCA sandbox, according to the agency, are listed below.

- **Eligible Participants:** Currently regulated firms as well as unregulated firms.
- **Eligibility Criteria:** Firms submit an application outlining how they meet the eligibility criteria for testing, which are (1) carrying out or supporting financial services business in the UK; (2) genuinely innovative; (3) identifiable consumer benefit; (4) need for sandbox testing; and (5) ready to test.
- **Testing Parameters:** If a firm is unauthorized it must obtain authorization or restricted authorization prior to participation in the sandbox. Prior to participating in the sandbox a firm must design, and obtain agreement on, the parameters of the sandbox test, including

---

the duration; customer selection; customer safeguards; disclosures; data; and testing plans.

FCA has four ways that it can help firms operate more easily in its sandbox. First, it can provide restricted authorizations that are a tailored authorization process for firms accepted into the sandbox. Any authorization or registration is restricted to allow firms to test only their ideas as agreed upon with agency staff, which is intended to make the process easier for firms to meet requirements and reduce the cost and time to initiate the test, according to the agency. Second, FCA provides individual guidance to firms in the sandbox that are unclear on how the agency's rules apply, whereby FCA will interpret the regulatory requirements in the context of the firm's specific test. Third, in some cases, FCA may be able to waive or modify an unduly burdensome rule for the purposes of the sandbox test, but it cannot waive national or international laws. Finally, FCA can issue no enforcement action letters in cases where they cannot issue individual guidance or waivers but they believe regulatory relief is justified for the circumstances of the sandbox. According to the agency, no enforcement action letters are offered only during the duration of the sandbox test to firms that keep to the agreed-upon testing parameters and that treat customers fairly. Also, no enforcement action letters only apply to FCA disciplinary action and do not limit any liabilities to consumers. Officials we interviewed noted that rule waivers and no enforcement action letters are rarely used tools. As of January 2018, FCA had received more than 200 sandbox applications. Eighteen firms had successfully graduated from the first cohort, 24 firms were preparing to test in the second cohort, and 18 other firms were accepted to test in the third cohort.

---

### Monetary Authority of Singapore's Regulatory Sandbox

Recognizing that when lack of clarity over whether a new financial service complies with legal and regulatory requirements could cause some financial institutions or start-ups to choose not to implement an innovation, the Monetary Authority of Singapore's (MAS) purpose in establishing its sandbox was to encourage such experimentation so that promising innovations could be tested in the market and have a chance for wider adoption, according to the agency. In addition, the agency stated that sandbox tests include safeguards to contain the consequences of failure and maintain the overall safety and soundness of the financial system. The characteristics of the MAS sandbox, according to MAS, are listed below.

- **Eligible Participants:** Firms that are looking to apply technology in an innovative way to provide financial services that are regulated by MAS, including financial institutions, fintech firms, and professional services firms partnering with such firms.
- **Eligibility Criteria:** Firms submit an application outlining how they meet the eligibility criteria for testing, which are that (1) the product uses new technology or existing technology in an innovative way, (2) the product benefits consumers or industry, and (3) the firm intends to deploy the product in Singapore on a broader scale after exiting the sandbox.
- **Testing Parameters:** Firms must define the following testing parameters prior to participating in the sandbox: (1) clearly defined test scenarios and expected outcomes must be established; (2) boundary conditions that facilitate meaningful experiments while sufficiently protecting the interests of consumers and maintaining the safety and soundness of the industry must be in place; (3) the firm assesses and mitigates significant associated risks; and (4) an acceptable exit and transition strategy must be defined.

MAS stated that it will consider relaxing various regulatory requirements for the duration of the sandbox test. However, they emphasized that their sandbox is not intended and cannot be used as a means to circumvent legal and regulatory requirements. MAS staff determines the specific legal and regulatory requirements that they may be willing to relax on a case-by-case basis. According to MAS, some of the regulatory requirements that could be relaxed included maintenance of certain levels of financial soundness, solvency, capital adequacy, and credit ratings as well as licensing fees, board composition requirements, and management experience requirements, among others. However, MAS has also laid out some requirements that it will not consider relaxing, including those regarding consumer information confidentiality, anti-money laundering, and countering terrorist financing. MAS officials said that all firms in the sandbox will receive some form of regulatory relaxation. As of November 2017, MAS had received more than 30 sandbox applications. One firm had successfully graduated, and a few other firms were testing or were in the process of initiating a sandbox test.

## Hong Kong Monetary Authority's Fintech Supervisory Sandbox

According to the Hong Kong Monetary Authority (HKMA), the purpose of the HKMA sandbox is to enable banks and technology firms to gather data and user feedback so that they can make changes to their innovations, thereby expediting the launch of new products and reducing

development costs. HKMA officials stated that the sandbox allows banks and their partnering technology firms to conduct pilot trials of their fintech initiatives involving a limited number of participating customers without the need to achieve full compliance with HKMA's supervisory requirements. The characteristics of the HKMA sandbox, according to the agency, are listed below.

- **Eligible Participants:** Regulated banks and their partnering technology firms.
- **Eligibility Criteria:** Fintech initiatives that are intended to be launched by banks in Hong Kong are eligible for the sandbox.
- **Testing Parameters:** Participating firms must (1) define the scope, phases, timing, and termination of the sandbox test; (2) establish customer protection measures, including disclosures, complaint handling, and compensation for consumer loss; (3) establishing risk management controls; and (4) establish a monitoring program for the sandbox test.

Similar to MAS, HKMA stated that its sandbox should not be used as a means to bypass applicable supervisory requirements; however, HKMA will relax regulatory requirements on a case-by-case basis. As of November 2017, nine banks had participated in 26 HKMA sandbox tests. Twelve of these tests had been completed and banks collaborated with fintech firms in 15 of the tests.

# Appendix IV: Comments from the Consumer Financial Protection Bureau



1700 G Street, N.W., Washington, DC 20552

February 23, 2018

Lawrence L. Evans, Jr.,  
Managing Director, Financial Markets and Community Investment  
Government Accountability Office  
441 G Street, NW  
Washington DC, 20548

Dear Mr. Evans:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report, titled *Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Encourage Responsible Innovation (GAO-18-254)*. We greatly appreciate GAO's work over the course of this engagement and believe the report provides important information regarding, among other things, the benefits and risks of financial technology (fintech) products and regulatory oversight of fintech firms.

The GAO makes one recommendation to the Bureau: "The Director of the Consumer Financial Protection Bureau should engage in collaborative discussions with other relevant financial regulators to help market participants address issues surrounding reimbursement for consumers who use financial account aggregators and experience unauthorized transactions in a group that incorporates leading practices."

The Bureau does not object to the GAO's recommendation. As the GAO is aware, the Bureau in October 2017 published consumer protection principles for financial data sharing and aggregation.<sup>1</sup> Those principles include the Bureau's vision that the consumer-authorized financial data sharing and aggregation market will include reasonable and practical means for consumers to dispute and resolve instances of unauthorized payments conducted in connection with or as a result of either authorized or unauthorized data sharing access. The Bureau also released a Request for Information Regarding Consumer Access to Financial Records in November 2016.<sup>2</sup> A variety of stakeholders, including market participants, provided comments in response to that request. The Bureau will continue to closely monitor developments in the market for consumer financial data sharing and aggregation and will continue to assess how the Bureau's consumer protection principles may best be realized. In doing so, the Bureau will engage in collaborative discussions with the relevant

---

<sup>1</sup> The Bureau's consumer protection principles are available at [http://files.consumerfinance.gov/f/documents/cfpb\\_consumer-protection-principles\\_data-aggregation.pdf](http://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf).

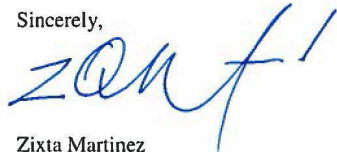
<sup>2</sup> See 81 Fed. Reg. 83,806 (Nov. 22, 2016).

[consumerfinance.gov](http://consumerfinance.gov)

federal financial regulators, including through the Federal Financial Institutions Examination Council, and state regulators.

The Bureau looks forward to continuing to work with GAO as it monitors the Bureau's progress in implementing this recommendation.

Sincerely,



Zixta Martinez  
Associate Director for External Affairs

[consumerfinance.gov](http://consumerfinance.gov)

# Appendix V: Comments from the Commodity Futures Trading Commission



**U.S. Commodity Futures Trading Commission**  
Three Lafayette Centre, 1155 21st Street, NW, Washington, DC 20581  
[www.cftc.gov](http://www.cftc.gov)

J. Christopher Giancarlo  
Chairman

(202) 418-5030  
[jcgiancarlo@cftc.gov](mailto:jcgiancarlo@cftc.gov)

February 15, 2018

Lawrence Evans, Jr.  
Managing Director  
Financial Markets and Community Investment  
United States Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Evans:

Thank you for providing the opportunity to review and comment on the GAO's report entitled *Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Encourage Responsible Innovation* (GAO-18-254). We appreciate GAO's work on the important topic of the development of financial technology (fintech), the current extent of federal oversight of fintech, and opportunities for federal financial regulators to facilitate market-enhancing fintech innovation. We also appreciate the courtesy that you have shown CFTC staff in conducting this engagement.

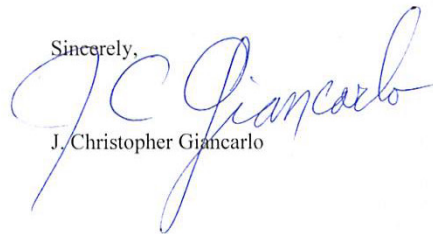
The CFTC concurs in GAO's recommendation to formally evaluate the feasibility and benefits to the CFTC's regulatory capabilities of adopting relevant knowledge building initiatives related to financial innovation. Indeed, the CFTC is either using or exploring the use of some of the knowledge building initiatives identified in the report including regulatory relief in the form of staff no-action letters, innovation competitions, and proofs of concept. The CFTC would be well positioned to conduct proof of concepts, including by potentially leveraging the large amount of data that the Commission already collects, but has concerns that, absent targeted legislative changes, such projects may violate federal procurement laws and gift prohibitions.

As the report indicates, the CFTC's fintech efforts are spearheaded by LabCFTC which was launched in May 2017. LabCFTC manages the CFTC's interface between technological innovation, regulatory modernization, and existing rules and regulations. LabCFTC accomplishes its mission in three ways: (1) engagement with innovators, both startups and

established entities; (2) consideration of, or support for, new technologies, including regulatory technology, which have the potential to allow the Commission to carry out its mission more effectively and efficiently or to improve CFTC markets; and, (3) collaboration with external organizations, including domestic and international regulators, focused on sharing information and best practices related to fintech innovation. These efforts are all consistent with the leading practices identified in GAO's report.

Thank you again for the opportunity to review and comment on the report. GAO's work will assist us in our continuing effort to make the CFTC a 21<sup>st</sup> century regulator that keeps pace with technological innovation in support of America's vital interest in maintaining the world's deepest and most durable, competitive, and vibrant capital and risk transfer markets.

Sincerely,

A handwritten signature in blue ink, appearing to read "JC Giancarlo", is written over the typed name.

J. Christopher Giancarlo



# Appendix VI: Comments from the Conference of State Bank Supervisors



February 23, 2018

Lawrance L. Evans, Jr.  
Director, Financial Markets and Community Investment  
Government Accountability Office  
441 G St., NW  
Washington, DC 20548

Re: GAO-18-254 Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Encourage Responsible Innovation

Dear Mr. Evans,

The Conference of State Bank Supervisors ("CSBS") is pleased to comment on GAO-18-254, *Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Encourage Responsible Innovation* ("Report"). The application of advances in technology to the delivery of financial services has given rise to innovative financial technology ("fintech") solutions that lower costs, enhance convenience, and potentially increase financial inclusion. The benefits and risks of fintech innovation warrants research by policy makers and the Government Accountability Office ("GAO") into the regulatory environment applicable to fintech firms.

To further address the purpose and subject matter of this report, CSBS submits this letter to:

1. Review the state system of regulatory oversight for fintech products and services;
2. Provide analytical insight into fintech that is only available from state regulators;
3. Discuss how state regulators are addressing the challenges posed to fintech firms by the state regulatory system; and
4. Address the recommended approaches for federal regulators to encourage financial innovation.

CSBS welcomes any further discussion with GAO or Congress on state regulatory oversight of fintech companies and consents to GAO using language from this letter to update the Report if GAO deems it prudent. Through engagement with the fintech industry, state regulators have taken note of common regulatory and licensing challenges faced by fintech firms. State regulators share the common goal of fostering prudent financial innovation by enabling fintech firms to operate on a national scale while protecting consumers from predatory products and services and maintaining the strength and resiliency of the broader financial system. Building off this

1129 20<sup>th</sup> Street, N.W. • Ninth Floor • Washington, DC • 20036  
www.csbs.org • 202-296-2840 • FAX 202-296-1928

common goal, state regulators launched Vision 2020, an initiative to modernize state regulation of non-bank financial companies, including fintech firms.

CSBS agrees that greater interagency collaboration and outreach on financial innovation at the state and federal level are important steps that could be taken to improve the regulatory oversight of the fintech industry. CSBS would support federal efforts to enhance collaboration, outreach, and education on financial innovation provided that such efforts respect the role of state regulators as the primary regulators of non-depository financial services providers, including fintech firms.

### State Regulators Actively Oversee Fintech Companies

Defining and describing fintech is a difficult task, which GAO tackles in an effective manner by focusing on products and services leveraging technological advances offered by institutions within the payment, lending, and wealth management sectors. CSBS would like to take the opportunity to expand on products and services reviewed within the payments and lending sectors, including a general overview of the applicability of state financial services regulation and fintech-specific applications.

#### The State Regulatory System

CSBS and its members have first-hand knowledge of the payments and lending products and services identified in the Report as “fintech”, particularly in mobile payments, marketplace lending, and distributed ledger technology (“DLT”) products and services. Most state legislatures have placed responsibility for regulating non-bank financial services industries with the state banking department or sister state agencies. The dual responsibility of bank and non-bank supervision gives the states unique insight into depository and non-depository fintech issues.

Through their nonbank licensing authority, CSBS members function as the primary regulators of non-bank consumer lenders, money services businesses, and mortgage lenders, including those with business models that are fintech in nature.<sup>1</sup> Accordingly, the states actively license and supervise companies engaging in activities identified in the Report as fintech payments and fintech lending. When any non-bank company (including any fintech firm) performs fintech payments and consumer lending activities, the states are responsible for licensing and supervising these activities consistent with state and federal law.

---

<sup>1</sup> Although not discussed in the Report and thus not reviewed in this letter, states actively license and regulate mortgage loan originators, including those deploying fintech innovations. For a general overview of state regulation of mortgage loan originators, please see the CSBS letter in response to the previous GAO report on fintech, available here: <https://www.gao.gov/products/GAO-17-361>.

#### Fintech Lending – Consumer Finance

State consumer finance licensing laws require individuals and businesses to obtain a consumer lending license to lend to consumers in their state. To obtain a license, prospective licensees are required to file an application that typically includes the submission of credit reports, fingerprints, a business plan, financial statements, and a surety bond. The prospective licensee may be required to provide evidence of policies, procedures, and internal controls that will facilitate the organization's compliance with state and federal laws, including disclosure, servicing, and debt collection requirements. Once a license is granted, management is required to maintain compliance with federal and state law which is overseen through periodic reporting and compliance examination requirements. Through licensing, state regulators have the ability to conduct examinations and take enforcement actions for violations of state and federal lending laws or regulatory requirements.

The act of making an unsecured loan to a consumer<sup>2</sup> – on the internet or in person – requires state licensure as a consumer credit provider.<sup>3</sup> Though state product requirements may vary,<sup>4</sup> consumer loans made through the fintech lending models described in the Report—whether person-to-person lending, direct lending, or platform lending—generally are subject to consumer credit licensing. CSBS confirms the finding in the Report that all states and the District of Columbia required lending licenses for consumer lenders operating in their states, despite the table in Appendix II stating that only 31 states license consumer lending. Using examples from the Report, CSBS can confirm that all identified consumer fintech lenders hold state licenses.<sup>5</sup> Though many of these fintech lenders originate through a depository institution, state licensure is still applicable in most situations.

Once licensed, the states supervise fintech lenders through on-site examinations. These exams review the licensee's compliance with both state and federal consumer protection laws in addition to state financial safety and soundness requirements. While federal regulators may have authority to periodically conduct examinations under the Bank Service Company Act (BSCA), the

<sup>2</sup> As in federal law, commercial lending is exempt from most state law protections. However, there are states that regulate commercial loans. See, e.g. North Dakota Money Broker License, available at <http://mortgage.nationwidelicencingsystem.org/slr/PublishedStateDocuments/ND-MB-License-Description.pdf>.

<sup>3</sup> See, e.g. Oregon Consumer Finance License, available at <https://mortgage.nationwidelicencingsystem.org/slr/PublishedStateDocuments/OR-Consumer-Finance-License-Company-Description.pdf>; New Hampshire Small Loan Lender Company License, available at <https://mortgage.nationwidelicencingsystem.org/slr/PublishedStateDocuments/NH-Small-Loan-Lender-Company-Description.pdf>.

<sup>4</sup> Typically, state thresholds vary for interest rate, principal, and term.

<sup>5</sup> Licensing records for SoFi, LendingClub, Prosper, and UpStart can all be found on NMLS Consumer Access at [nmlsconsumeraccess.org](http://nmlsconsumeraccess.org).

states are required to examine licensed consumer credit companies – including fintech lenders – regularly.

#### Fintech Payments – Money Services Businesses

Providers of fintech payments products and services—including mobile wallets, peer-to-peer payments, and peer-to-business payments—are regulated as money transmitters or money services businesses (hereinafter “MSBs”) under state law.<sup>6</sup> Generally, state MSB laws require individuals and companies to obtain an MSB license in order to take, hold, and/or send money for consumers in their state. Despite the use of different terminology in MSB laws, a common set of requirements exists for companies seeking to operate nationally. To operate in 49 states, D.C., and Puerto Rico, a money transmitter must be bonded, maintain permissible investments, and satisfy minimum net worth requirements. While the dollar amount of these requirements varies, the legal requirement to meet these regulatory standards is consistent.

Importantly, the states do not just examine for compliance with state law but also examine for compliance with federal law. Ensuring a licensee’s compliance with the Electronic Funds Transfer Act and Bank Secrecy Act are key components to the state examination process. The states have taken actions against licensed money transmitters for violations of the Bank Secrecy Act, Office of Foreign Asset Control requirements, and other federal requirements.<sup>7</sup>

Since the regulatory requirements are common among the states, industry oversight is in the process of standardization. As of March 2017, 45 states, D.C., and Puerto Rico have signed the Nationwide Cooperative Agreement for MSB Supervision and its companion Protocol for Performing Multi-State Examinations.<sup>8</sup> This Protocol and Agreement establishes the Multi-State MSB Examination Taskforce (“MMET”), a body consisting of representatives from ten participating states tasked with enhancing the state supervisory system for money services businesses supervision and fostering regulatory consistency.<sup>9</sup> Through the MMET, in 2017, the

<sup>6</sup> The core underpinning of NMLS is agreed upon business activity definitions. Despite different statutory language, 36 states apply the following business activity definition for electronic money transmitting, likely covering all mobile wallet providers: “Accepting or instructing to be delivered currency, funds, or other value, such as stored value, that substitutes for currency to another location or person by electronic means, such as mobile-to-mobile payments.” available at <http://mortgage.nationwidelicensingsystem.org/licensees/resources/LicenseeResources/Business%20Activities%20Definitions.pdf>.

<sup>7</sup> See, e.g. *In the Matter of PayPal, Inc.*, Massachusetts Consent Order, Docket No. 2014-005 (28 May 2014). Available at <http://nmlsconsumeraccess.org/EntityDetails.aspx/Artifact/Final%20Order.pdf?q=111350-211164>.

<sup>8</sup> See Nationwide Cooperative Agreement for MSB Supervision (January 2012), available at <https://www.csbs.org/sites/default/files/2017-11/MSB-CooperativeAgreement010512clean.pdf>; Protocol for Performing Multi-state Examinations (January 2012) available at <https://www.csbs.org/sites/default/files/2017-11/MSB-Protocol010512.pdf>.

<sup>9</sup> Under the MMET Operating Procedures, five MMET members are appointed by the CSBS board of directors and five MMET members are appointed by the Money Transmitter Regulators Association (“MTRA”) board of directors. Additionally, the terms of MMET members are limited to two year periods and the composition of the MMET

states coordinated oversight of 165 MSBs that operate in multiple states, including companies listed in the Report. In 2017, the MMET coordinated 64 examinations of multi-state MSBs where teams of examiners from different states conducted coordinated supervision.<sup>10</sup> Notwithstanding varying licensing requirements and oversight mechanisms, this collaboration between states in MSB examination increases efficiency for both the states and industry.

Several fintech business models have emerged in which a digital wallet is provided to customers using distributed ledger virtual currencies. After engagement with industry participants, state and federal regulators, and other stakeholders, CSBS concluded that activities involving third party control of virtual currency should be subject to state licensure and supervision.<sup>11</sup> CSBS produced a model regulatory framework for states to utilize, and continue to work with the states and industry to tailor the regulatory process for licensed activities that occur with virtual currency.

Since the release of the CSBS Virtual Currency Model Regulatory Framework, states have licensed and examined virtual currency mobile wallet providers. In the states' experience, the traditional approach to MSB examination has worked, though unique issues have arisen that warrant further review in the supervisory process. These issues include valuation of virtual currency transactions, fluctuating value of virtual currency, verifying virtual currency ownership, confirming balances, cybersecurity, and the irreversible nature of virtual currency transactions. The MMET is cognizant of these issues and continues to monitor for best practices.

#### Bank-Fintech Partnerships

States are also responsible for chartering and supervising state-chartered banks. In partnering with fintech companies, these banks originate loans through fintech lenders, purchase fintech lender loans, utilize fintech payments solutions, and are actively exploring innovative DLT applications. Drawing from the dual responsibility of state regulators over bank and non-bank supervision, CSBS can confirm the Report's findings that fintech companies generally must comply with bank third-party risk management requirements and/or state licensure and supervision.<sup>12</sup> Only commercial lenders operating independently of banks would avoid both third-party bank oversight and state licensure.

---

membership fluctuates to ensure that the MMET is representative of all participating states. See Multi-state MSB Examination Taskforce Operating Procedures, available at <https://www.mtraweb.org/wp-content/uploads/2012/10/Multi-State-MSB-Examination-Taskforce-MMET-Operating-Procedures-07-16-131.pdf>.

<sup>10</sup> See MMET 2016 Annual Report, available at <https://www.mtraweb.org/exams/multi-state-msb-examination-taskforce-mmet/>.

<sup>11</sup> See <https://www.csbs.org/model-regulatory-framework-virtual-currencies>.

<sup>12</sup> CSBS explains third-party oversight in detail in a 2015 letter to Treasury on marketplace lending, available at <https://www.csbs.org/regulatory/policy/Documents/2015/CSBS-NACCA%20Marketplace%20Lending%20RFI.pdf>.

Increasingly banks are outsourcing a wide variety of critical services to third-party technology service providers (TSPs), some of which may be characterized as fintech in nature. In addition to examining state-licensed nonbank fintech companies, state regulators are also actively supervising and regulating fintech TSPs through their authority to examine the TSPs for state banks. Currently, approximately 37 states are authorized under state law to examine bank TSPs to assess the potential risks they pose to individual client banks and the broader banking system. In supervising TSPs, state regulators coordinate with their federal counterparts that are authorized to examine TSPs under the BSCA. State regulators are actively seeking to improve information sharing between state and federal regulators under the BSCA to promote more efficient supervision and encourage partnerships between banks and fintech firms.

#### NMLS Provides Insight into Fintech

The states developed the NMLS to serve as the system that facilitates compliance with state licensing laws.<sup>13</sup> Through this common structure, the states gather information useful to policy makers, industry, and regulators alike.

Through the NMLS, the states collect a substantial amount of information. Notable data fields for fintech companies include:

- Identifying information, including trade names;
- Financial statements;
- Bank account information;
- Legal status, including corporate formation and state;
- Affiliates and subsidiaries; and
- Control and ownership.

This information is used to inform a view of regulated industries, which can be leveraged for public stakeholders. NMLS also has information specific to the types of fintech companies identified in the Report.

#### NMLS Data – Fintech Payments

As of June 30, 2017, 37 state agencies managed their MSB licenses in NMLS. The NMLS Uniform Authorized Agent Reporting (“UAAR”) functionality, deployed in 2014, permits state-licensed MSBs to upload their authorized agents for reporting to state regulators. As of June 30, 2017, 34 agencies were using the UAAR functionality. From these reports, NMLS data reflects:

- 364 companies hold a total of 3,522 state money transmitter licenses in NMLS;
- 55 percent of the companies are licensed in more than one state;

<sup>13</sup> At the end of 2016, NMLS was the licensing system of record for 62 state agencies, managing a total of 601 different license authorities covering a broad range of non-depository financial services. This is up from 585 at the end of 2015. NMLS manages 327 company, 193 branch, and 81 individual license types.



- 111 companies are licensed in more than 10 states;
- 192 companies report 306,154 Active Authorized Agent relationships in NMLS, and 117 report no agents use (as of 6/30/2017);
- NMLS contains 196,285 Active Agent Locations, with 58,707 used by multiple principals (as of 6/30/2017; and
- 11 companies have uploaded over 5,000 agents (as of 6/30/2017).<sup>14</sup>

From this data, policy makers can extract several trends. First, the MSB industry trends towards multi-state activity. Second, companies without agents likely utilize the internet. Accordingly, the MSB industry has diverging business models: large multi-state companies that engage in electronic money transfer,<sup>15</sup> large multi-state companies that engage in physical money transfer,<sup>16</sup> and specialty MSBs that serve local communities.<sup>17</sup>

The NMLS has also developed functionality for collecting MSB call report information. In the first quarter of 2017, NMLS began collecting company-specific data, including financial condition, state-specific transactions, company-wide transactions, permissible investments, and destination country reporting. This information is a primary source for determining market trends, allocating regulatory resources, and streamlining reporting requirements for companies operating across state lines.

Using licensing, agent, and transaction data, CSBS is able to set parameters to identify fintech payments providers.<sup>18</sup> The table below shows the market share of fintech payments companies in different MSB markets as of the second quarter of 2017.

<sup>14</sup> For more information, see the SRR Annual Report. Available at <http://mortgage.nationwidelicencingsystem.org/about/Documents/2016%20SRR%20AR%20Report%20Web%20Version.pdf>.

<sup>15</sup> Large multi-state companies engaged in electronic money transfer are likely licensed in 10 or more states without agents.

<sup>16</sup> Large multi-state companies engaged in physical money transfer are likely licensed in 10 or more states with a significant number of agents that handle money from customers.

<sup>17</sup> Specialty MSBs are likely licensed in 1-state, often providing services to a particular community.

<sup>18</sup> For the purposes of this letter, a fintech payments provider is identified as a MSB licensed in four or more states and that operates with two or fewer physical agents, based on the assumption that such MSBs must be utilizing technology to conduct business.

Market	Q1 & Q2 Market Sum	0-2 Agents 4 or More Licenses	% of Market
Money Transmission Transactions	\$ 315,600,710,213	\$ 94,399,644,288	30%
Stored Value Transactions	\$ 113,041,580,286	\$ 89,220,787,291	79%
Payment Instruments Issued/Sold	\$ 95,068,052,346	\$ 1,610,298,261	2%
Virtual Currency Transactions	\$ 3,450,656,079	\$ 2,983,269,368	86%
Currency Exchange Transactions	\$ 1,892,373,820	\$ 1,031,922,627	55%
Total:	\$529,053,372,744	\$ 189,245,923,638	36%

The total volume of transactions by fintech payments providers amounted to approximately 36% of the total MSB market through the first half of 2017. This aggregate data covers large mobile wallet and other payments companies like PayPal, Venmo, Amazon, Facebook, Google, and Amazon.

The MSB Call Report will be particularly useful when discussing remittances and access to financial services. Currently, there is no data source for U.S. consumer payments across borders. With the collection and verification of MSB Call Report data, the NMLS will be able to identify where U.S. consumers send money, as well as market trends over time.

#### NMLS Data – Fintech Lenders

When states license any company, financial statements and business plans are required to be submitted to the regulator. When performed through NMLS, a record is created that can be used to determine market conditions and risk profiles of licensed companies. Accordingly, NMLS contains data that might be useful to regulators and policymakers alike. Indeed, CSBS has entered into information sharing agreements with several federal government agencies and offices to govern the sharing of NMLS data, including the Consumer Financial Protection Bureau (CFPB), the Financial Crimes Enforcement Network (FinCEN), the Federal Housing Administration (FHA), the Federal Trade Commission (FTC), and the Office of Financial Research (OFR).

In their letter requesting a fintech study, Senators Brown, Shaheen, and Merkley asked about the size and structure of fintech lending.<sup>19</sup> The Senators stated, “[s]ince many fintech companies are

<sup>19</sup> The letter is available at <http://www.brown.senate.gov/download/160418-sl-gao-fintech>.



privately held, information about the size of their portfolios is often not transparent.” It is true that private companies – including marketplace lenders and mobile wallet providers – are not obligated to release financial details. However, state-licensed companies are required to submit financial information to their regulators. State regulators use this information to make regulatory and supervisory decisions, and are glad to discuss portfolio information upon request.

### Steps Being Taken by State Regulators to Address Challenges to Fintech Firm Posed by State Regulatory Requirements

The Report identifies regulatory approaches taken in other countries that could benefit fintech regulation and innovation and assesses the extent to which federal financial regulatory agencies have adopted similar approaches. Such approaches include interaction-building initiatives, knowledge-building initiatives, and regulatory-coordination initiatives. Since the Report does not discuss the extent to which state financial services regulators have adopted similar efforts, CSBS would like to take this opportunity to outline steps being taken by state regulators to modernize state regulation of the fintech industry through an initiative referred to as Vision 2020.<sup>20</sup>

#### Vision 2020

CSBS recognizes that the emergence of fintech innovations underscores the need for the states to establish a regulatory environment where technological innovation can be developed and regulated in a clear and responsible manner. The challenges posed by numerous state regulatory requirements identified in the Report echo concerns heard by state regulators in conducting outreach with the fintech industry over the course of the past several years. Based on this feedback, state regulators identified several common goals shared between regulators and the industry that will help guide improvements to the state licensing and supervisory process.

State regulators and the fintech industry are in agreement that the state regulatory system should support innovative fintech startups and enable licensees to operate on a national scale while upholding consumer protections and maintaining the resiliency of the financial system. Building off of these shared goals, state regulators launched Vision 2020, a series of initiatives intended to modernize state regulation of non-bank financial companies, including fintech firms, by 2020. Specifically, through Vision 2020, state regulators and CSBS intend to modernize the state regulatory system by: (1) forming a Fintech Advisory Panel, (2) redesigning NMLS, (3) harmonizing multi-state supervision, (4) assisting state banking departments, (5) enabling banks to service non-banks, and (6) improving third party supervision.

<sup>20</sup> For more information on Vision 2020, see <https://www.csbs.org/vision2020>.

As discussed below, the regulatory initiatives taken abroad which the Report suggests for adoption by U.S. federal regulators are currently or imminently underway at the state level.

#### Interaction-Building Initiatives

The Report identifies steps taken by regulators abroad and by U.S. federal regulators to better facilitate interactions with fintech firms so as to address potential confusion among fintech firms regarding which regulations they were subject to, which regulators would oversee their activities, and who should they contact to obtain answers to these questions. Such interaction-building initiatives include establishing innovation offices which would serve as a point of contact for industry, hosting fintech events for industry, and issuing publications on various fintech-related topics.

Although not addressed in the Report, state regulators have undertaken several interaction-building initiatives over the past several years to better facilitate interaction between state regulators and fintech service providers. As early as 2014, the CSBS formed the Emerging Payments and Innovation Task Force (“EPITF”) to study changes in payment systems brought forth by fintech innovations and to serve as a point of contact for fintech industry stakeholders. Since that time the EPITF has held public hearings and forums across the country to enable engagement between fintech industry and state regulators, including an Emerging Payments Stakeholder Hearing, several fintech roundtables, and an upcoming Fintech Forum.

More recently, through Vision 2020, CSBS and state regulators plan to host multiple fintech forums for the fintech payments and fintech lending sectors to enable direct dialogue with state regulators and facilitate the emergence of concrete ideas to make the state regulatory system more streamlined and efficient. Thus, state regulators and CSBS have launched several ongoing interaction-building initiatives to improve interactions with fintech firms similar to those taken by regulators abroad and at the federal level.

#### Knowledge-Building Initiatives

The Report discusses efforts undertaken by regulators abroad and by U.S. federal regulators to help regulators learn about new products and business models in the fintech space. Although not mentioned in the report, state regulators have undertaken several knowledge-building initiatives to help educate state regulators on emerging fintech innovations. In addition to the knowledge gained through the interaction-building initiatives discussed above, state regulators are also actively improving their education programs and standards with respect to non-bank supervision under the auspices of Vision 2020.

One major initiative within Vision 2020 calls on CSBS to help state regulators identify knowledge gaps, develop and allocate expertise where it is most needed, compare regulatory approaches with other state regulators for educational purposes, and validate higher

performance through enhanced state agency accreditation standards. Assisting state regulators through this knowledge-building initiative is intended to improve the state licensing and supervisory process for fintech service providers and build recognition of common regulatory standards across state lines.

Another major initiative within Vision 2020 is the formation of a Fintech Industry Advisory Panel (“FIAP”) comprised of representatives of state regulators and companies within the fintech payments and fintech lending sectors.<sup>21</sup> Through FIAP, state regulators are actively learning about new fintech products and services, identifying points of regulatory friction in licensing, multi-state nonbank regulation, and the regulation of bank-fintech partnerships. Additionally, the upcoming CSBS Fintech Forum discussed above will be an opportunity for state regulators to continue to build their knowledge and understanding of a variety of fintech business models and of developments related to cryptocurrency and blockchain technology.

Thus, several knowledge-building initiatives have been launched by state regulators and CSBS to facilitate education around fintech products and services and how they fit within the fabric of the state regulatory system.

#### Regulatory-Coordination Initiatives

The Report addresses efforts by regulators abroad and by U.S. federal regulators to enhance coordination between regulatory bodies with oversight authority over fintech. For many years, State regulators have been actively engaged in regulatory coordination with federal financial regulatory agencies through multiple interagency bodies, including the Federal Financial Institutions Examination Council (FFIEC) and the Federal Stability Oversight Council (FSOC). Additionally, although not discussed in the Report, CSBS and state regulators have taken steps to enhance regulatory coordination and collaboration among state regulators in licensing, supervising, and regulating fintech service providers.

In fact, most of the initiatives within Vision 2020 are intended to enable greater regulatory coordination and/or result in more coordinated, consistent regulatory and supervisory processes. For instance, the FIAP is intended to identify actionable steps for improving state licensing, regulation, and non-depository supervision and for supporting innovation in financial services. Additionally, a coordinated, consistent multi-state approach to licensing is currently being developed through another Vision 2020 initiative—the redesign of NMLS. The redesigned NMLS, or NMLS 2.0, is intended to enhance the role of NMLS as a common platform for state licensing. NMLS 2.0 will launch in early 2019 and operate in real time, standardize information collection, establish a common framework, automate that which is manual and routine, and

<sup>21</sup> For more information on the FIAP, see <https://www.csbs.org/csbs-fintech-industry-advisory-panel>.

operate at the highest levels of data security. Through enhanced regulatory technology features, NMLS will improve compliance with state licensing requirements.<sup>22</sup>

Another regulatory-coordination initiative underway through Vision 2020 is the development of the State Examination System (SES), a new technology platform for state examinations and other supervisory activities. SES will harmonize multi-state supervision by fostering greater collaboration and information sharing between regulators from different states, enhancing uniformity in examinations and enforcement, and improving states' ability to risk-focus their supervisory activities. Together NMLS 2.0 and SES will also enhance the efficiency of state examinations by enabling greater risk-scoping for purposes of examination resource allocation.<sup>23</sup>

More recently, seven states have agreed to a multi-state agreement that seeks to standardize key elements of the licensing process for money services businesses.<sup>24</sup> The seven states consist of Georgia, Illinois, Kansas, Massachusetts, Tennessee, Texas and Washington. Under the agreement, if one participating state has reviewed key elements of a company's operations in connection with the company's application for a money transmitter license (IT, cybersecurity, business plan, background check, and compliance with the federal Bank Secrecy Act), the other participating states will accept that state's findings.

Not only are state regulators actively involved in efforts to enhance coordination with one another, but CSBS and state regulators are also pushing for greater regulatory coordination between state and federal regulators. Specifically, through CSBS, state regulators continue to support federal legislation to amend the BSCA to allow state and federal regulators to better coordinate supervision of TSPs and, in turn, produce a more effective supervisory experience for fintech firms and other nonbanks. Thus, several regulatory-coordination initiatives have been launched by state regulators and CSBS to modernize state regulation of nonbank and fintech companies.

### Recommended Approaches to Federal Financial Regulators to Improve Fintech Regulation and Encourage Financial Innovation

CSBS appreciates the GAO's consideration of regulatory approaches abroad to assess their relevance to the U.S. regulatory structure. CSBS agrees that greater interagency collaboration and outreach on financial innovation at the federal level are important steps that could be

<sup>22</sup> For more information on NMLS 2.0, see <http://mortgage.nationwidelicensingsystem.org/Pages/NMLS20Information.aspx>.

<sup>23</sup> For more information on SES, see <https://new.nmls.org/ses>.

<sup>24</sup> See Press Release: State Regulators Take First Step to Standardize Licensing Practices for Fintech Payments, available at <https://www.csbs.org/state-regulators-take-first-step-standardize-licensing-practices-fintech-payments>.

taken to improve the regulatory oversight of the fintech industry. In fact, CSBS believes the GAO should have gone farther in its recommendations by recommending that federal regulators consistently invite state regulators to participate in fintech-related interagency collaborative groups. CSBS would support and eagerly participate in federal efforts to enhance collaboration, outreach, and education on financial innovation provided that such efforts respect the role of state regulators as the primary regulators of non-depository financial services providers, including fintech firms.

While CSBS appreciates suggestions of greater regulatory coordination and industry outreach, we do not support any recommendation that federal regulators adopt knowledge-building initiatives in the form of regulatory sandboxes, pilot programs or similar arrangements that would preempt state consumer protection and licensing laws for fintech payments providers and fintech lenders. The Report characterizes such mechanisms as “knowledge-building” because, according to the Report, they “help innovators develop products in limited risk environments.”

CSBS cautions that federal “knowledge-building” initiatives which carry with them the preemption of state law would amount to a dangerous experiment that could create profound risks for consumers. Perhaps such risks are more limited in Hong Kong and Singapore given that the populations of these countries are roughly equal to the populations of Washington and Wisconsin, respectively. Even the economy of United Kingdom, the fifth largest in the world, is roughly the size of that of a single U.S. state, California. Accordingly, taking into account economic context, regulatory approaches that may pose limited risks in other countries would pose significantly greater risk if applied to the U.S. as a whole through federal preemption.

### Benefits of the State Regulatory System for Fintech Companies, Consumers, and the Broader Financial System

The state regulatory system is the foundation upon which the fintech industry has emerged and remains the superior regulatory structure for ensuring that ground-breaking innovation in the financial services industry continues to emerge on the basis of competitive equality and regulatory impartiality. Financial innovation among nonbank fintech firms can only emerge in a regulatory structure that is tailored to the unique risk profile of nonbank financial services providers and that subjects such providers to a degree of regulatory scrutiny commensurate with their risk to consumers. Although it is not without its flaws and it is certainly capable of improvement, the state regulatory system enables states to strike that balance in a prudent and accountable fashion.

A recent federal initiative mentioned in the Report to create a special purpose national charter for nonbank financial service providers would upset that balance by creating a regulatory

structure which is not only divorced from any accountability to consumers but that would also heap competitive advantages on a select few firms in an impartial manner. CSBS believes that financial innovation would not continue emerge at its current pace if such a federal regulatory paradigm were to become a reality.

Maintaining the primary role of state regulators in licensing and supervising fintech firms is also essential to ensuring the continued resiliency of the financial system. The regulatory perimeter established by state regulation of nonbank financial service providers is a critical component to ensuring that the federal safety net is not extended beyond the banking industry. Recent federal initiatives which threaten to redefine what it means to be a bank by regulatory fiat would upend traditional commitments to a bank-centric payment system and the separation of banking and commerce. The end result of such a drastic redefinition would be the extension of the federal safety net well beyond its intended scope with the American public left to pay for the costs of dangerous regulatory experimentation.<sup>25</sup>

Thus, CSBS urges caution and candor on the part of federal financial regulators as they contemplate alternative regulatory approaches to encourage innovation in the financial services industry and improve fintech regulation.


### Conclusion

CSBS appreciates the opportunity to review the Report and submit this overview of the state regulatory system and steps being taken to improve the state regulatory system. Between the supervision actively occurring at licensed fintech companies and the modernization of state regulation occurring through Vision 2020, the states are actively engaged in tackling the challenges posed by emerging financial innovation and its interaction with state regulation. CSBS welcomes any opportunity to follow up on this Report or provide information that may be relevant to analysis of the fintech industry.

Sincerely,

<sup>25</sup> While the Report and other sources seem to draw some parallel between the OCC special purpose national charter and the ILC charter, any comparison is flawed and misplaced. Congress explicitly exempted ILCs from coverage under the Bank Holding Company Act (BHCA) and, in so doing, limited ILCs' access to the Fed payments system and applied antitrust restrictions to ILCs to mitigate concerns prompted by the intermingling of banking and commerce. Since Congress provided no explicit exemption from BHCA coverage for the OCC special purpose national charter, the limits on payments system access and anticompetitive practices would seemingly not apply based on the language of the BHCA. Furthermore, ILCs are insured depository institutions regulated at the state and federal level and, as a consequence of obtaining deposit insurance, are able to export interest rates across state lines. In contrast, the OCC special purpose national charter would be regulated solely by the OCC and seek to export interest rates nationwide without obtaining deposit insurance and thereby establish an unprecedented level of preemption of state usury laws.

15



John W. Ryan  
President & CEO

# Appendix VII: Comments from the Federal Communications Commission



Federal Communications Commission  
Washington, D.C. 20554

February 26, 2018

Lawrance L. Evans, Jr.  
Managing Director  
Financial Markets and Community Investment  
Government Accountability Office  
441 G Street NW  
Washington, DC 20548

Dear Mr Evans:

We have reviewed GAO's draft report, "FINANCIAL TECHNOLOGY: Additional Steps by Regulators Could Better Protect Consumers and Encourage Responsible Innovation".

The report recommends that, "The Chairman of the Federal Communications Commission (FCC) should discuss with the Presidents of the Federal Reserve Banks of Atlanta and Boston whether the topics of the 2018- 2019 biennial regulators meeting of the Federal Reserve's Mobile Payments Industry Working Group would make FCC participation beneficial to the FCC or the group, and take steps accordingly."

We agree with the recommendation. FCC will reach out to the Federal Reserve Banks of Atlanta and Boston to determine the topics of the 2018- 2019 biennial regulators meeting of the Federal Reserve's Mobile Payments Industry Working Group. We will then decide whether FCC participation would be beneficial, and take steps accordingly.

Sincerely,

A handwritten signature in black ink, appearing to read "G. Patrick Webre", is written over the word "Sincerely,".

G. Patrick Webre  
Acting Chief  
Consumer and Governmental Affairs Bureau



# Appendix VIII: Comments from the Federal Deposit Insurance Corporation



**Federal Deposit Insurance Corporation**  
550 17th Street NW, Washington, D.C. 20429-9990

Division of Risk Management Supervision  
Division of Depositor and Consumer Protection

February 21, 2018

Mr. Lawrence I. Evans, Jr., Managing Director  
Financial Markets and Community Investment  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, D.C. 20548

Dear Mr. Evans:

The Federal Deposit Insurance Corporation (FDIC) appreciates the opportunity to review the GAO draft report *Financial Technology – Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight* (Report) (GAO-18-254). The Report summarized the GAO's study of certain aspects of fintech activities: (1) fintech benefits and risks; (2) regulatory oversight of fintech firms; (3) regulatory challenges for fintech firms; and (4) other countries' oversight and innovation efforts, and their potential relevance in the United States.

The Report contains three recommendations to the FDIC, along with recommendations to other regulators. First, the Report recommends that the Chairman of the FDIC engage in collaborative discussions with other relevant financial regulators to help market participants address issues surrounding reimbursement for consumers who use financial aggregators and experience unauthorized transactions in a group that incorporates leading practices. The FDIC recognizes the benefits of engaging in collaborative discussions with other relevant regulators. As the Report details, the FDIC has been involved in ongoing collaborative discussions with other financial regulators about financial account aggregation through existing interagency frameworks and will continue to do so. In particular, the FDIC will engage in collaborative discussions regarding liability for unauthorized transactions and consumer reimbursement.

The Report also recommends that the Chairman of the FDIC formally evaluate the feasibility and benefit of establishing an Office of Innovation or clear contact point, with a dedicated website, email address, and staff. The FDIC acknowledges this recommendation and will conduct such an evaluation. However, it should be recognized that the FDIC has a long history of engaging in open dialogue with any party interested in discussing matters related to the FDIC's mission and responsibilities, regardless of the business model or status of the interested party. In its evaluation, the FDIC would be cautious that establishing such specific contacts for a particular industry or segment of a market not suggest an endorsement on the part of the FDIC of that industry or market segment versus others.

The Report also recommends that the Chairman of the FDIC formally evaluate the feasibility and benefits to their regulatory capacities of adopting relevant knowledge building initiatives related to financial innovation. The FDIC recognizes the importance of knowledge building and has developed a framework and implemented initiatives to facilitate knowledge building. The FDIC has established a Technology Steering Committee, comprised of senior

- 2 -

FDIC executives, to oversee FDIC monitoring and evaluation of technology industry developments and their implications for financial institutions and consumers. The Technology Steering Committee directs the work of two interdisciplinary working groups that are building knowledge along wholesale and retail aspects of Technology.

Among other things, one of the Technology Steering Committee's objectives is gaining an understanding of current technology activities and trends and evaluating the potential impact to banks, the deposit insurance system, effective supervisory oversight, economic inclusion, and consumer protection. To achieve those objectives, the FDIC is taking a multi-pronged approach in building knowledge to:

- meet with industry stakeholders and attend conferences to educate the working group about innovations being adopted;
- use case scenarios and perform deep dive analysis to assess potential implications to safety and soundness, consumer protection, and resolutions;
- implement experimental pilots utilizing innovative technology to allow staff to become familiar with new technologies;
- read research reports to understand technologies, innovations, implementation, and potential implications;
- review bank usage of technologies and bank engagement with financial technology partners during supervisory examinations; and
- monitor news to identify financial innovations and adoption of financial innovation.

Relying on the knowledge built within the working groups utilizing this approach, the working groups began developing reference materials on various innovative technologies that FDIC staff across the Corporation can use as a resource. The FDIC will continue ongoing efforts to build knowledge related to financial innovation and will consider other relevant knowledge building initiatives, as appropriate.

In addition to the recommendations, we observed that the Report notes questions raised by certain providers regarding fair lending considerations when using alternative data or modeling. The FDIC, along with the other FFIEC agencies, has longstanding information regarding compliance with fair lending laws and regulations. For example, the Interagency Fair Lending Examination Procedures is a publicly available framework by which the FDIC conducts its fair lending reviews. These procedures include guidance on how to evaluate automated underwriting and credit scoring models. The agencies have issued additional guidance on fair lending, such as the Interagency Policy Statement on Discrimination in Lending. These frameworks for fair lending consideration are broadly applicable to traditional and non-traditional modeling techniques and data sources. In addition, the FDIC and other agencies have

- 3 -

guidance on model risk management that provide additional information to institutions regarding the use of models in the conduct of banking activities.

Finally, as noted in the Report, the FDIC has also been exploring ways in which mobile financial services (MFS) can help better engage unbanked and underbanked households in the banking system. Mobile devices, such as smartphones and tablets, have emerged as technology with the potential to change the way consumers interact with banks. In response, banks are rapidly making MFS available to their customers. In a 2014 white paper, the FDIC suggested that MFS provided by banks offered the potential to improve underserved consumers' access to, sustainability of, and growth in banking relationships. In 2016, the FDIC released a qualitative evaluation of the value consumers saw in mobile financial services, focused on bank-provided MFS. While neither report addressed "fintech accounts" described in the Report, the 2016 report concluded that MFS has the potential to be implemented in ways that address the specific financial needs of the underserved and help draw them more comprehensively into sustainable banking relationships, thus expanding the number of individuals who obtain financial services safely and securely.

Thank you for your efforts and if you have any questions or need additional follow-up information, please do not hesitate to contact us.

Sincerely



Doreen R. Eberley  
Director  
Division of Risk Management Supervision



Mark Pearce  
Director  
Division of Depositor and Consumer Protection

# Appendix IX: Comments from the Board of Governors of the Federal Reserve System



BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM  
WASHINGTON, D. C. 20551

DIVISION OF  
SUPERVISION AND REGULATION

February 23, 2018

Lawrance Evans, Jr.  
Managing Director  
Financial Markets and Community Investment  
United States Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Evans:

Thank you for providing the Board of Governors of the Federal Reserve System ("Federal Reserve" or "Board") with an opportunity to review the final draft of the Government Accountability Office ("GAO") report titled: *Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight* (GAO-18-254). We appreciate the report's recognition of the steps the Federal Reserve has taken, in coordination with other federal and state regulators, to facilitate discussions and information-sharing among financial technology ("fintech") industry stakeholders.

Almost all fintech innovations rely on connections to traditional financial institutions for services such as access to consumer deposits or related account data; access to the payment system; or credit origination. Accordingly, the Federal Reserve's general approach to fintech developments is that, first and foremost, we have a responsibility to ensure that the institutions subject to our supervision are operated safely and soundly and that they comply with applicable statutes and regulations. Within that framework, we have a strong interest in permitting socially beneficial innovations to flourish, while ensuring the risks that they may present are appropriately managed. Our goal is to avoid unnecessarily

[www.federalreserve.gov](http://www.federalreserve.gov)

2

restricting innovations that can benefit consumers and small businesses through expanded access to financial services or greater efficiency, convenience, and reduced transaction costs.

The GAO's report makes five recommendations to the Federal Reserve:

- The Chair of the Board of Governors of the Federal Reserve System should invite NCUA to participate in the Interagency Fintech Discussion Forum.
- The President of the Federal Reserve Bank of Atlanta should discuss with the Chairman of the FCC and the President of the Federal Reserve Banks of Boston whether the topics of the 2018-2019 biennial regulators meeting of the Federal Reserve's Mobile Payments Industry Working Group would make FCC participation beneficial to the FCC or the group, and take steps accordingly.
- The President of the Federal Reserve Bank of Boston should discuss with the Chairman of the FCC and the President of the Federal Reserve Banks of Atlanta whether the topics of the 2018-2019 biennial regulators meeting of the Federal Reserve's Mobile Payments Industry Working Group would make FCC participation beneficial to the FCC or the group, and take steps accordingly.
- The Chair of the Board of Governors of the Federal Reserve System should engage in collaborative discussions with other relevant financial regulators to help market participants address issues surrounding reimbursement for consumers who use financial account aggregators and experience unauthorized transactions in a group that incorporates leading practices.
- The Chair of the Board of Governors of the Federal Reserve System should formally evaluate the feasibility and benefits to their regulatory capacities of adopting relevant knowledge building initiatives related to financial innovation.

*Invite NCUA to Participate in the Interagency Fintech Discussion Forum*

With regard to the report's recommendation that the Board invite the *National Credit Union Administration* ("NCUA") to participate in the Interagency Fintech Discussion Forum, we agree that the NCUA's oversight of credit unions provides it with experiences and perspectives that are relevant to the group's collaborative work on fintech consumer protection issues. Accordingly, Board staff will invite relevant contacts at the NCUA to take part in future meetings of the Interagency Fintech Discussion Forum.

*Coordinate with the Federal Communications Commission concerning their participation in the 2018-2019 Federal Reserve's Mobile Payments Industry Working Group*

With respect to the GAO's second and third recommendations, staff at the Federal Reserve Banks of Atlanta and Boston will discuss with appropriate contacts at the Federal Communications Commission ("FCC") the benefits of the FCC's participation in the 2018-2019 Federal Reserve's Mobile Payments Industry Working Group ("MPIW") and will take any additional necessary steps to involve the FCC in any relevant upcoming work of the MPIW.

*Engage in collaborative discussions regarding financial account aggregation*

With regard to the GAO's recommendation that the Federal Reserve System engage in discussions with other regulators to help market participants address issues arising from financial account aggregators, the Federal Reserve recognizes the importance of working together when determining how best to encourage socially beneficial innovation in the marketplace, while ensuring that consumers' interests are protected. As reflected in your report, the Federal Reserve and other regulators have already committed to coordinating on these issues in a variety of fora, including the Federal Financial Institutions Examination Council ("FFIEC") Task Force on Supervision, the FFIEC Task Force on Consumer Compliance, and the Interagency Fintech Discussion Forum. This calendar year, the Federal Reserve has also organized a number of meetings with industry actors, trade associations, and consumer advocates in a variety of fintech areas, including financial account aggregation, which have included joint participation from a number of relevant regulators, like the OCC, FDIC, CFPB, and several Federal Reserve Banks. We will continue to

R5

4

facilitate and engage in collaborative discussions with other relevant financial regulators in these and other settings to help market participants address the important issues surrounding reimbursement for consumers who use financial account aggregators and experience unauthorized transactions.

*Evaluate the feasibility and benefits to regulatory capacities of adopting relevant knowledge building initiatives related to financial innovation.*

With respect to the GAO's recommendation that the Federal Reserve formally evaluate the feasibility and benefits to its regulatory capacities of adopting relevant knowledge building initiatives related to financial innovation, the Federal Reserve recognizes the importance of formally increasing its knowledge base as it relates to financial innovation. Among other efforts that focus on financial innovation, the Federal Reserve System has recently organized a nation-wide team of experts, tasked with monitoring fintech and related emerging technology trends as they relate to our supervisory mandates. The new organization includes representation from all of the Federal Reserve System's Reserve Banks and is co-led by the Board's Division of Supervision and Regulation and the Division of Consumer and Community Affairs. The team's critical objectives will include ensuring that fintech-related supervisory information is shared across the Federal Reserve System and informs relevant supervisory, policy, and outreach strategies.

I have consulted with the Director of the Division of Reserve Bank Operations and Payment Systems, the Director of the Division of Consumer and Community Affairs, the General Counsel of the Board, the President of the Federal Reserve Bank of Atlanta, and the President of the Federal Reserve Bank of Boston on this reply to your report, and they concur in this response. We appreciate the GAO's review of the Federal Reserve's collaborative efforts in the fintech space, for their professional approach to the review, and for the opportunity to comment.

Sincerely,

A handwritten signature in blue ink, appearing to read "Mike Gibson".

Michael S. Gibson  
Director



# Appendix X: Comments from the National Credit Union Administration



National Credit Union Administration  
Office of the Executive Director

February 22, 2018

**SENT BY E-MAIL**

Lawrence L. Evans, Jr.  
Director, Financial Markets and Community Investment  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548  
[evansl@gao.gov](mailto:evansl@gao.gov)

Dear Mr. Evans:

We reviewed GAO's draft report entitled *Financial Technology – Additional Steps by Regulators Could Better Protect Consumers and Encourage Responsible Innovation (GAO-18-254)*. We acknowledge the growth of the financial technology (Fintech) industry provides benefits as well as risks to consumers. We concur with the report's recommendations and will continue to collaborate with the other federal regulators to address risk issues.

Because NCUA does not have vendor authority like the other federal banking regulators, evaluations of Fintech activities are challenging. We will continue to monitor risks posed by Fintech firms to the credit union industry by working with the banking regulators. Thank you for the opportunity to comment.

Sincerely,

A handwritten signature in black ink, which appears to read "Mark Treichel", is positioned above the printed name and title.

Mark Treichel  
Executive Director

1775 Duke Street – Alexandria, VA 22314-3428 – 703-518-6320



# Appendix XI: Comments from the Office of the Comptroller of the Currency



Office of the Comptroller of the Currency

Washington, DC 20219

March 1, 2018

Mr. Lawrence L. Evans, Jr.  
Director, Financial Markets and Community Investment  
U. S. Government Accountability Office  
Washington, DC 20548

Dear Mr. Evans:

The Office of the Comptroller of the Currency (OCC) has received and reviewed the Government Accountability Office's (GAO) draft report titled "Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Encourage Responsible Innovation" (Report). The Report examined: (1) the benefits and risks financial services pose to consumers, (2) the regulatory environment, (3) the various challenges faces by fintech firms; and (4) the steps taken by domestic and other countries' regulators to encourage financial innovation within their countries.

As the prudential regulator of the federal banking system, the OCC supports the ability of national banks and federal savings associations to continue to fulfill their vital role of providing financial services to consumers, businesses, and their communities through innovation that is responsive to those evolving needs. Encouraging responsible innovation in the banking sector promotes efficiencies and effectiveness that supports long lasting economic growth and ensures that financial institutions remains not only relevant but also a vibrant part of the financial system.

As noted in your Report, the OCC has already taken many steps to encourage responsible innovation by national banks and federal savings associations as well as the fintech firms that partner with these banks. In the fall of 2016, the OCC announced the creation of a framework to support responsible innovation.<sup>1</sup> The components of that framework address many of the matters discussed in your report including outreach and collaboration with other regulators. In addition, the OCC established an Office of Innovation (Office), which began operating in January 2017. The Office's primary purpose is to make certain that institutions with federal charters have a regulatory framework that is receptive to responsible innovation and the supervision needed to support it. Part of that mission is to assist banks and nonbanks, including fintech firms, with understanding our expectations regarding safe and sound operations, fair access, and fair treatment of customers. The Office serves as a clearinghouse for innovation-related matters and a central point of contact for OCC staff, banks, fintech firms, and other industry stakeholders. The Office has published guides and reference materials for community banks, as well as fintech

<sup>1</sup> "OCC Issues Responsible Innovation Framework" (October 2016), available at <https://occ.gov/news-issuances/news-releases/2016/nr-occ-2016-135.html>.

firms and nonbank institutions.<sup>2</sup> It has also conducted significant outreach to establish a more open and continuous dialogue regarding innovation.<sup>3</sup>

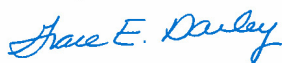
Within our agency, the Office has worked to raise awareness and understanding of industry trends and issues. We want to make sure that our staff understands the latest industry developments including the use of artificial intelligence and machine learning, the newest payment developments, the evolution of lending, and bank-fintech partnerships. This familiarity will allow staff, and examiners in particular, to have meaningful and helpful conversations with the banks we regulate.

As part of the Report, the GAO makes one recommendation for the OCC. The GAO recommends that the OCC should engage in collaborative discussions with other relevant financial regulators to help market participants address issues surrounding reimbursement for consumers who use financial account aggregators and experience unauthorized transactions in a group that incorporates leading practices.

The OCC appreciates the concern raised by the GAO and understands the importance and the benefit of this recommendation. The OCC, as well as the other federal banking agencies and the Consumer Financial Protection Bureau, have met with a variety of stakeholders, including fintech firms, financial account aggregators, banks, consumer groups and trade associations, regarding issues arising from data aggregation. The OCC has also participated in interagency meetings with these stakeholders and has discussed these matters with other regulators in forums such as the Federal Financial Institutions Examination Council's Task Forces on Supervision and Consumer Compliance and the Interagency Fintech Discussion Group. Going forward, the OCC will continue to facilitate, engage, and participate in discussions with applicable industry groups and other regulators on matters regarding data aggregation, including issues surrounding reimbursement for consumers who experience harm from unauthorized transactions.

If you need additional information, please contact Beth Knickerbocker, Chief Innovation Officer, (202) 649-7820.

Sincerely,



Grace E. Dailey  
Senior Deputy Comptroller and Chief National Bank Examiner

<sup>2</sup> See "Responsible Innovation" on occ.gov (<https://www.occ.gov/topics/responsible-innovation/index-innovation.html>).

<sup>3</sup> For example, the Office has engaged in "Office Hours" in San Francisco and New York and intends to hold Office Hours in Chicago, Illinois on March 21 and 22, 2018.

# Appendix XII: Comments from the Securities and Exchange Commission



UNITED STATES  
SECURITIES AND EXCHANGE COMMISSION  
WASHINGTON, D.C. 20549

February 23, 2018

Lawrance L. Evans, Jr.  
Managing Director  
Financial Markets and Community Investment  
United States Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Evans:

I appreciate the opportunity to respond to your report titled, "Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Encourage Responsible Innovation" GAO-18-254 ("draft report"). The SEC appreciates having the benefit of the GAO's views on how best to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation in the emerging financial technology ("fintech") environment.

In its report, the GAO recommends that the SEC formally evaluate the feasibility and benefits to their regulatory capacities of adopting relevant knowledge-building initiatives related to financial innovation. I support the GAO's recommendation.

The SEC has a very strong track record of active participation in significant knowledge-building initiatives with industry participants and fellow regulators – both domestically and internationally. The agency has been actively engaged in the fintech space since as early as 2013, with the creation of an internal Distributed Ledger Technology (DLT) Working Group to build expertise, identify emerging risk areas, and coordinate efforts among the SEC's divisions and offices. In 2016, the Commission hosted a Fintech Forum and announced the creation of an agency-wide Fintech Working Group to evaluate emerging areas in fintech. The agency has also established a central point of contact (FinTech@sec.gov) to receive inquiries from market participants and investors on fintech issues. This past fall, the SEC also announced the creation of a new Cyber Unit within the Division of Enforcement to work closely with the Commission's DLT Working Group.

The SEC is committed to continue active participation and engagement in its knowledge-building initiatives, and plans to continue, among other things, to coordinate with our federal and state counterparts, including the Commodity Futures Trading Commission, the Department of Treasury, Department of Justice, and state attorneys general and securities regulators. The Commission is also committed to participate and engage in knowledge-building initiatives on the international front. The Commission is an active member of the Financial Stability Board and International Organization of Securities Commissions ("IOSCO"). In these contexts, the

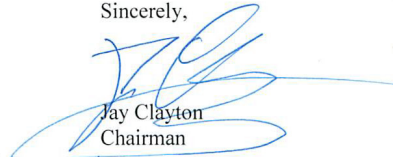
Lawrance L. Evans, Jr.  
Page 2

Commission staff routinely monitors international developments regarding fintech issues and extensively coordinates with foreign regulators. For example, the Commission staff initiated, and participates in, among others, IOSCO's Initial Coin Offering ("ICO") Consultation Network, through which IOSCO members can discuss their experiences and bring their concerns regarding ICOs, including any cross-border issues, to the attention of fellow regulators.

As the SEC assesses the merits of potential additional knowledge-building initiatives related to financial innovation, the agency will, of course, continue to coordinate with our fellow regulators in this effort.

Thank you again for your work on this important issue.

Sincerely,



Jay Clayton  
Chairman

---

# Appendix XIII: GAO Contact and Staff Acknowledgments

---

---

## GAO Contact

Lawrance L. Evans, Jr., (202) 512-8678 or [evansl@gao.gov](mailto:evansl@gao.gov).

---

## Staff Acknowledgements

In addition to the contact named above, Cody Goebel (Assistant Director); Chloe Brown (Analyst-in-Charge); Chris Ross; Davis Judson; Ian P. Moloney; and Bethany Benitez made key contributions to this report. Also contributing to this report were Joanna Berry; Timothy Bober; Richard Hung; Pamela Davidson; Tovah Rom; Cynthia Saunders; and Jena Sinkfield.

---

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<https://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <https://www.gao.gov> and select "E-mail Updates."

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).  
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#).  
Visit GAO on the web at <https://www.gao.gov>.

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <https://www.gao.gov/fraudnet/fraudnet.htm>

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Orice Williams Brown, Managing Director, [WilliamsO@gao.gov](mailto:WilliamsO@gao.gov), (202) 512-4400,  
U.S. Government Accountability Office, 441 G Street NW, Room 7125,  
Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

---

## Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, [spel@gao.gov](mailto:spel@gao.gov), (202) 512-4707  
U.S. Government Accountability Office, 441 G Street NW, Room 7814,  
Washington, DC 20548



Please Print on Recycled Paper.

# Tab 13

**SECURITIES AND EXCHANGE COMMISSION**

**17 CFR Part 275**

**Release No. IA-4889; File No. S7-09-18**

**RIN: 3235-AM36**

**Proposed Commission Interpretation Regarding Standard of Conduct for Investment  
Advisers; Request for Comment on Enhancing Investment Adviser Regulation**

**AGENCY:** Securities and Exchange Commission.

**ACTION:** Proposed interpretation; request for comment.

**SUMMARY:** The Securities and Exchange Commission (the “SEC” or the “Commission”) is publishing for comment a proposed interpretation of the standard of conduct for investment advisers under the Investment Advisers Act of 1940 (the “Advisers Act” or the “Act”). The Commission also is requesting comment on: licensing and continuing education requirements for personnel of SEC-registered investment advisers; delivery of account statements to clients with investment advisory accounts; and financial responsibility requirements for SEC-registered investment advisers, including fidelity bonds.

**DATES:** Comments should be received on or before August 7, 2018.

**ADDRESSES:** Comments may be submitted by any of the following methods:

Electronic Comments:

- Use the Commission’s Internet comment form (<http://www.sec.gov/rules/interp.shtml>); or
- Send an e-mail to [rule-comments@sec.gov](mailto:rule-comments@sec.gov). Please include File Number S7-09-18 on the subject line.



Paper Comments:

- Send paper comments to Brent J. Fields, Secretary, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549-1090.

All submissions should refer to File Number S7-09-18. This file number should be included on the subject line if e-mail is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's Internet website (<http://www.sec.gov/rules/interp.shtml>). Comments also are available for website viewing and printing in the Commission's Public Reference Room, 100 F Street, NE, Washington, DC 20549, on official business days between the hours of 10:00 am and 3:00 pm. All comments received will be posted without change. Persons submitting comments are cautioned that we do not redact or edit personal identifying information from comment submissions. You should submit only information that you wish to make publicly available.

Studies, memoranda or other substantive items may be added by the Commission or staff to the comment file during this rulemaking. A notification of the inclusion in the comment file of any such materials will be made available on the Commission's website. To ensure direct electronic receipt of such notifications, sign up through the "Stay Connected" option at [www.sec.gov](http://www.sec.gov) to receive notifications by e-mail.

**FOR FURTHER INFORMATION CONTACT:** Jennifer Songer, Senior Counsel, or Sara Cortes, Assistant Director, at (202) 551-6787 or [IArules@sec.gov](mailto:IArules@sec.gov), Investment Adviser Regulation Office, Division of Investment Management, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549-8549.

**SUPPLEMENTARY INFORMATION:** The Commission is publishing for comment a

proposed interpretation of the standard of conduct for investment advisers under the Advisers Act [15 U.S.C. 80b].<sup>1</sup>

## TABLE OF CONTENTS

- II. INVESTMENT ADVISERS' FIDUCIARY DUTY
  - A. **Duty of Care**
    - i. **Duty to Provide Advice that is in the Client's Best Interest**
    - ii. **Duty to Seek Best Execution**
    - iii. **Duty to Act and to Provide Advice and Monitoring over the Course of the Relationship**
  - B. **Duty of Loyalty**
  - C. **Request for Comment**
- III. ECONOMIC CONSIDERATIONS
  - A. **Background**
  - B. **Economic Impacts**
- IV. REQUEST FOR COMMENT REGARDING AREAS OF ENHANCED INVESTMENT ADVISER REGULATION
  - A. **Federal Licensing and Continuing Education**
  - B. **Provision of Account Statements**
  - C. **Financial Responsibility**

## I. INTRODUCTION

An investment adviser is a fiduciary, and as such is held to the highest standard of conduct and must act in the best interest of its client.<sup>2</sup> Its fiduciary obligation, which includes an

---

<sup>1</sup> 15 U.S.C. 80b. Unless otherwise noted, when we refer to the Advisers Act, or any paragraph of the Advisers Act, we are referring to 15 U.S.C. 80b of the United States Code, at which the Advisers Act is codified, and when we refer to rules under the Advisers Act, or any paragraph of these rules, we are referring to title 17, part 275 of the Code of Federal Regulations [17 CFR 275], in which these rules are published.

<sup>2</sup> *SEC v. Capital Gains Research Bureau, Inc.*, 375 U.S. 180, 194 (1963) ("SEC v. Capital Gains"). *See also infra* notes 26 - 32 and accompanying text; Investment Adviser Codes of Ethics, Investment Advisers Act Release No. 2256 (July 2, 2004); Compliance Programs of Investment Companies and Investment Advisers, Investment Advisers Act Release No. 2204 (Dec. 17, 2003) ("Compliance Programs Release"); Electronic Filing by Investment Advisers; Proposed Amendments to Form ADV, Investment Advisers Act

affirmative duty of utmost good faith and full and fair disclosure of all material facts, is established under federal law and is important to the Commission’s investor protection efforts.<sup>3</sup> The Commission also regulates broker-dealers, including the obligations that broker-dealers owe to their customers. Investment advisers and broker-dealers provide advice and services to retail investors and are important to our capital markets and our economy more broadly. Broker-dealers and investment advisers have different types of relationships with their customers and clients and have different models for providing advice, which provide investors with choice about the levels and types of advice they receive and how they pay for the services that they receive.

Today, the Commission is proposing a rule that would require all broker-dealers and natural persons who are associated persons of broker-dealers to act in the best interest of retail customers<sup>4</sup> when making a recommendation of any securities transaction or investment strategy involving securities to retail customers (“Regulation Best Interest”).<sup>5</sup> We are also proposing to require registered investment advisers and registered broker-dealers to deliver to retail investors a relationship summary, which would provide these investors with information about the relationships and services the firm offers, the standard of conduct and the fees and costs associated with those services, specified conflicts of interest, and whether the firm and its

---

Release No. 1862 (Apr. 5, 2000). We acknowledge that investment advisers also have antifraud liability with respect to prospective clients under section 206 of the Advisers Act.

<sup>3</sup> See SEC v. Capital Gains, *supra* note 2.

<sup>4</sup> An investment adviser has a fiduciary duty to all of its clients, whether or not the client is a retail investor.

<sup>5</sup> Regulation Best Interest, Exchange Act Release No. 34-83062 (April 18, 2018) (“Regulation Best Interest Proposal”).

financial professionals currently have reportable legal or disciplinary events.<sup>6</sup> In light of the comprehensive nature of our proposed set of rulemakings, we believe it would be appropriate and beneficial to address in one release<sup>7</sup> and reaffirm – and in some cases clarify – certain aspects of the fiduciary duty that an investment adviser owes to its clients under section 206 of the Advisers Act.<sup>8</sup>

An investment adviser’s fiduciary duty is similar to, but not the same as, the proposed obligations of broker-dealers under Regulation Best Interest.<sup>9</sup> While we are not proposing a uniform standard of conduct for broker-dealers and investment advisers in light of their different relationship types and models for providing advice, we continue to consider whether we can improve protection of investors through potential enhancements to the legal obligations of investment advisers. Below, in addition to our interpretation of advisers’ existing fiduciary obligations, we request comment on three potential enhancements to their legal obligations by considering areas where the current broker-dealer framework provides investor protections that may not have counterparts in the investment adviser context.

---

<sup>6</sup> Form CRS Relationship Summary; Amendments to Form ADV; Required Disclosures in Retail Communications and Restrictions on the use of Certain Names or Titles, Investment Advisers Act Release No. IA-4888 (April 18, 2018) (“Form CRS Proposal”).

<sup>7</sup> This Release is intended to highlight the principles relevant to an adviser’s fiduciary duty. It is not, however, intended to be the exclusive resource for understanding these principles.

<sup>8</sup> The Commission recognizes that many advisers provide impersonal investment advice. *See, e.g.*, Advisers Act rule 203A-3 (defining “impersonal investment advice” in the context of defining “investment adviser representative” as “investment advisory services provided by means of written material or oral statements that do not purport to meet the objectives or needs of specific individuals or accounts”). This Release does not address the extent to which the Advisers Act applies to different types of impersonal investment advice.

<sup>9</sup> Regulation Best Interest Proposal, *supra* note 5. In addition to the obligations proposed in Regulation Best Interest, broker-dealers have a variety of existing specific obligations, including, among others, suitability, best execution, and fair and reasonable compensation. *See, e.g., Hanly v. SEC*, 415 F.2d 589, 596-97 (2d Cir. 1969) (“A securities dealer occupies a special relationship to a buyer of securities in that by his position he implicitly represents that he has an adequate and reasonable basis for the opinions he renders.”); and FINRA rules 2111 (Suitability), 5310 (Best Execution and Interpositioning), and 2121 (Fair Prices and Commissions)).

## II. INVESTMENT ADVISERS' FIDUCIARY DUTY

The Advisers Act establishes a federal fiduciary standard for investment advisers.<sup>10</sup> This fiduciary standard is based on equitable common law principles and is fundamental to advisers' relationships with their clients under the Advisers Act.<sup>11</sup> The fiduciary duty to which advisers are subject is not specifically defined in the Advisers Act or in Commission rules, but reflects a Congressional recognition "of the delicate fiduciary nature of an investment advisory relationship" as well as a Congressional intent to "eliminate, or at least to expose, all conflicts of interest which might incline an investment adviser – consciously or unconsciously – to render advice which was not disinterested."<sup>12</sup> An adviser's fiduciary duty is imposed under the Advisers Act in recognition of the nature of the relationship between an investment adviser and a client and the desire "so far as is presently practicable to eliminate the abuses" that led to the enactment of the Advisers Act.<sup>13</sup> It is made enforceable by the antifraud provisions of the

---

<sup>10</sup> *Transamerica Mortgage Advisors, Inc. v. Lewis*, 444 U.S. 11, 17 (1979) ("Transamerica Mortgage v. Lewis") ("§ 206 establishes federal fiduciary standards to govern the conduct of investment advisers.") (quotation marks omitted); *Santa Fe Industries, Inc. v. Green*, 430 U.S. 462, 471, n.11 (1977) (in discussing SEC v. Capital Gains, stating that the Supreme Court's reference to fraud in the "equitable" sense of the term was "premised on its recognition that Congress intended the Investment Advisers Act to establish federal fiduciary standards for investment advisers"); SEC v. Capital Gains, *supra* note 2; Amendments to Form ADV, Investment Advisers Act Release No. 3060 (July 28, 2010) ("Investment Advisers Act Release 3060") ("Under the Advisers Act, an adviser is a fiduciary whose duty is to serve the best interests of its clients, which includes an obligation not to subrogate clients' interests to its own," citing Proxy Voting by Investment Advisers, Investment Advisers Act Release No. 2106 (Jan. 31, 2003) ("Investment Advisers Act Release 2106")).

<sup>11</sup> See SEC v. Capital Gains, *supra* note 2 (discussing the history of the Advisers Act, and how equitable principles influenced the common law of fraud and changed the suits brought against a fiduciary, "which Congress recognized the investment adviser to be").

<sup>12</sup> See SEC v. Capital Gains, *supra* note 2.

<sup>13</sup> See SEC v. Capital Gains, *supra* note 2 ("The Advisers Act thus reflects a congressional recognition 'of the delicate fiduciary nature of an investment advisory relationship,' as well as a congressional intent to eliminate, or at least to expose, all conflicts of interest which might incline an investment adviser -- consciously or unconsciously -- to render advice which was not disinterested." and also noting that the "declaration of policy" in the original bill, which became the Advisers Act, declared that "the national public interest and the interest of investors are adversely affected when the business of investment advisers is so conducted as to defraud or mislead investors, or to enable such advisers to relieve themselves of their fiduciary obligations to their clients. It [sic] is hereby declared that the policy and purposes of this title, in

Advisers Act.<sup>14</sup>

An investment adviser's fiduciary duty under the Advisers Act comprises a duty of care and a duty of loyalty. Several commenters responding to Chairman Clayton's June 2017 request for public input<sup>15</sup> on the standards of conduct for investment advisers and broker-dealers acknowledged these duties.<sup>16</sup> This fiduciary duty requires an adviser "to adopt the principal's goals, objectives, or ends."<sup>17</sup> This means the adviser must, at all times, serve the best interest of its clients and not subordinate its clients' interest to its own.<sup>18</sup> The federal fiduciary duty is

---

accordance with which the provisions of this title shall be interpreted, are to mitigate and, so far as is presently practicable to eliminate the abuses enumerated in this section" (citing S. 3580, 76th Cong., 3d Sess., § 202 and Investment Trusts and Investment Companies, Report of the Securities and Exchange Commission, Pursuant to Section 30 of the Public Utility Holding Company Act of 1935, on Investment Counsel, Investment Management, Investment Supervisory, and Investment Advisory Services, H.R. Doc. No. 477, 76<sup>th</sup> Cong. 2d Sess., 1, at 28). *See also* In the Matter of Arleen W. Hughes, Exchange Act Release No. 4048 (Feb. 18, 1948) ("Arleen Hughes") (discussing the relationship of trust and confidence between the client and a dual registrant and stating that the registrant was a fiduciary and subject to liability under the antifraud provisions of the Securities Act of 1933 and the Securities Exchange Act).

<sup>14</sup> SEC v. Capital Gains, *supra* note 2; Transamerica Mortgage v. Lewis, *supra* note 10 ("[T]he Act's legislative history leaves no doubt that Congress intended to impose enforceable fiduciary obligations.").

<sup>15</sup> Public Comments from Retail Investors and Other Interested Parties on Standards of Conduct for Investment Advisers and Broker-Dealers, Chairman Jay Clayton (June 1, 2017), *available at* <https://www.sec.gov/news/public-statement/statement-chairman-clayton-2017-05-31> ("Chairman Clayton's Request for Public Input").

<sup>16</sup> *See, e.g.*, Comment letter of the Investment Adviser Association (Aug. 31, 2017) ("IAA Letter") ("The well-established fiduciary duty under the Advisers Act, which incorporates both a duty of loyalty and a duty of care, has been applied consistently over the years by courts and the SEC."); Comment letter of the Consumer Federation of America (Sept. 14, 2017) ("an adviser's fiduciary obligation 'divides neatly into the duty of loyalty and the duty of care.' The duty of loyalty is designed to protect against 'malfeasance,' or wrongdoing, on the part of the adviser, while the duty of care is designed to protect against 'nonfeasance,' such as neglect.").

<sup>17</sup> Arthur B. Laby, *The Fiduciary Obligations as the Adoption of Ends*, 56 Buffalo Law Review 99 (2008). *See also* Restatement (Third) of Agency, §2.02 Scope of Actual Authority (2006) (describing a fiduciary's authority in terms of the fiduciary's reasonable understanding of the principal's manifestations and objectives).

<sup>18</sup> Investment Advisers Act Release 3060, *supra* footnote 10 (adopting amendments to Form ADV and stating that "under the Advisers Act, an adviser is a fiduciary whose duty is to serve the best interests of its clients, which includes an obligation not to subrogate clients' interests to its own," citing Investment Advisers Act Release 2106 *supra* note 10); SEC v. Tambone, 550 F.3d 106, 146 (1st Cir. 2008) ("Section 206 imposes a fiduciary duty on investment advisers to act at all times in the best interest of the fund and its investors."); SEC v. Moran, 944 F. Supp. 286 (S.D.N.Y. 1996) ("Investment advisers are entrusted with the responsibility and duty to act in the best interest of their clients.").

imposed through the antifraud provisions of the Advisers Act.<sup>19</sup> The duty follows the contours of the relationship between the adviser and its client, and the adviser and its client may shape that relationship through contract when the client receives full and fair disclosure and provides informed consent.<sup>20</sup> Although the ability to tailor the terms means that the application of the fiduciary duty will vary with the terms of the relationship, the relationship in all cases remains that of a fiduciary to a client. In other words, the investment adviser cannot disclose or negotiate away, and the investor cannot waive, the federal fiduciary duty.<sup>21</sup> We discuss our views<sup>22</sup> on an

---

<sup>19</sup> See *supra* note 14.

<sup>20</sup> See *infra* note 40 and accompanying text for a discussion of informed consent.

<sup>21</sup> As an adviser's federal fiduciary obligations are enforceable through section 206 of the Act, we would view a waiver of enforcement of section 206 as implicating section 215(a) of the Act, which provides that "any condition, stipulation or provision binding any person to waive compliance with any provision of this title. . . shall be void." Some commenters on Chairman Clayton's Request for Public Input and other Commission requests for comment also stated that an adviser's fiduciary duty could not be disclosed away. See, e.g., IAA Letter *supra* note 16 ("While disclosure of conflicts is crucial, it cannot take the place of the overarching duty of loyalty. In other words, an adviser is still first and foremost bound by its duty to act in its client's best interest and disclosure does not relieve an adviser of this duty."); Comment letter of AARP (Sept. 6, 2017) ("Disclosure and consent alone do not meet the fiduciary test."); Financial Planning Coalition Letter (July 5, 2013) responding to SEC Request for Data and Other Information, Duties of Brokers, Dealers, and Investment Advisers, Exchange Act Release No. 69013 (Mar. 1, 2013) ("Financial Planning Coalition 2013 Letter") ("[D]isclosure alone is not sufficient to discharge an investment adviser's fiduciary duty; rather, the key issue is whether the transaction is in the best interest of the client.") (internal citations omitted). See also Restatement (Third) of Agency, § 8.06 Principal's Consent (2006) ("The law applicable to relationships of agency as defined in § 1.01 imposes mandatory limits on the circumstances under which an agent may be empowered to take disloyal action. These limits serve protective and cautionary purposes. Thus, an agreement that contains general or broad language purporting to release an agent in advance from the agent's general fiduciary obligation to the principal is not likely to be enforceable. This is because a broadly sweeping release of an agent's fiduciary duty may not reflect an adequately informed judgment on the part of the principal; if effective, the release would expose the principal to the risk that the agent will exploit the agent's position in ways not foreseeable by the principal at the time the principal agreed to the release. In contrast, when a principal consents to specific transactions or to specified types of conduct by the agent, the principal has a focused opportunity to assess risks that are more readily identifiable."); Tamar Frankel, Arthur Laby & Ann Schwing, *The Regulation of Money Managers*, (updated 2017) ("The Regulation of Money Managers") ("Disclosure may, but will not always, cure the fraud, since a fiduciary owes a duty to deal fairly with clients.").

<sup>22</sup> In various circumstances, other regulators, including the U.S. Department of Labor, and other legal regimes, including state securities law, impose obligations on investment advisers. In some cases, these standards may differ from the standard imposed and enforced by the Commission.

investment adviser's fiduciary duty in more detail below.<sup>23</sup>

### **A. Duty of Care**

As fiduciaries, investment advisers owe their clients a duty of care.<sup>24</sup> The Commission has discussed the duty of care and its components in a number of contexts.<sup>25</sup> The duty of care includes, among other things: (i) the duty to act and to provide advice that is in the best interest of the client, (ii) the duty to seek best execution of a client's transactions where the adviser has the responsibility to select broker-dealers to execute client trades, and (iii) the duty to provide advice and monitoring over the course of the relationship.

#### **i. Duty to Provide Advice that is in the Client's Best Interest**

We have addressed an adviser's duty of care in the context of the provision of personalized investment advice. In this context, the duty of care includes a duty to make a reasonable inquiry into a client's financial situation, level of financial sophistication, investment

---

<sup>23</sup> The interpretations discussed in this Release also apply to automated advisers, which are often colloquially referred to as "robo-advisers." Robo-advisers, like all SEC-registered investment advisers, are subject to all of the requirements of the Advisers Act, including the requirement that they provide advice consistent with the fiduciary duty they owe to their clients. The staff of the Commission has issued guidance regarding how robo-advisers can meet their obligations under the Advisers Act, given the unique challenges and opportunities presented by their business models. *See Division of Investment Management, SEC, Staff Guidance on Robo Advisers*, (February 2017), available at <https://www.sec.gov/investment/im-guidance-2017-02.pdf>.

<sup>24</sup> *See* Investment Advisers Act Release No. 2106, *supra* note 10 (stating that under the Advisers Act, "an adviser is a fiduciary that owes each of its clients duties of care and loyalty with respect to all services undertaken on the client's behalf, including proxy voting," which is the subject of the release, and citing *SEC v. Capital Gains* *supra* note 2, to support this point). *See also* Restatement (Third) of Agency, § 8.08 (discussing the duty of care that an agent owes its principal as a matter of common law); *The Regulation of Money Managers*, *supra* note 21 ("Advice can be divided into three stages. The first determines the needs of the particular client. The second determines the portfolio strategy that would lead to meeting the client's needs. The third relates to the choice of securities that the portfolio would contain. The duty of care relates to each of the stages and depends on the depth or extent of the advisers' obligation towards their clients.").

<sup>25</sup> *See, e.g.*, Suitability of Investment Advice Provided by Investment Advisers; Custodial Account Statements for Certain Advisory Clients, Investment Advisers Act Release No. 1406 (Mar. 16, 1994) ("Investment Advisers Act Release 1406") (stating that advisers have a duty of care and discussing advisers' suitability obligations); Securities; Brokerage and Research Services, Exchange Act Release No. 23170 (Apr. 23, 1986) ("Exchange Act Release 23170") ("an adviser, as a fiduciary, owes its clients a duty of obtaining the best execution on securities transactions."). We highlight certain contexts in which the Commission has addressed the duty of care but we note that there are others; for example, voting proxies when an adviser undertakes to do so. Investment Advisers Act Release 2106, *supra* note 10.



experience, and investment objectives (which we refer to collectively as the client’s “investment profile”) and a duty to provide personalized advice that is suitable for and in the best interest of the client based on the client’s investment profile.<sup>26</sup>

An adviser must, before providing any personalized investment advice and as appropriate thereafter, make a reasonable inquiry into the client’s investment profile. The nature and extent of the inquiry turn on what is reasonable under the circumstances, including the nature and extent of the agreed-upon advisory services, the nature and complexity of the anticipated investment advice, and the investment profile of the client. For example, to formulate a comprehensive financial plan for a client, an adviser might obtain a range of personal and financial information about the client, including current income, investments, assets and debts, marital status, insurance policies, and financial goals.<sup>27</sup>

An adviser must update a client’s investment profile in order to adjust its advice to reflect any changed circumstances.<sup>28</sup> The frequency with which the adviser must update the information in order to consider changes to any advice the adviser provides would turn on many factors, including whether the adviser is aware of events that have occurred that could render inaccurate or incomplete the investment profile on which it currently bases its advice. For

---

<sup>26</sup> In 1994, the Commission proposed a rule that would make express the fiduciary obligation of investment advisers to make only suitable recommendations to a client. Investment Advisers Act Release 1406, *supra* note 25. Although never adopted, the rule was designed, among other things, to reflect the Commission’s interpretation of an adviser’s existing suitability obligation under the Advisers Act. We believe that this obligation, when combined with an adviser’s fiduciary duty to act in the best interest of its client, requires an adviser to provide investment advice that is suitable for *and in the best interest of* its client.

<sup>27</sup> Investment Advisers Act Release 1406, *supra* note 25. After making a reasonable inquiry into the client’s investment profile, it generally would be reasonable for an adviser to rely on information provided by the client (or the client’s agent) regarding the client’s financial circumstances, and an adviser should not be held to have given advice not in its client’s best interest if it is later shown that the client had misled the adviser.

<sup>28</sup> We note that this would not be done for a one-time financial plan or other investment advice that is not provided on an ongoing basis. *See also infra* note 37.

example, a change in the relevant tax law or knowledge that the client has retired or experienced a change in marital status might trigger an obligation to make a new inquiry.

An investment adviser must also have a reasonable belief that the personalized advice is suitable for and in the best interest of the client based on the client's investment profile. A reasonable belief would involve considering, for example, whether investments are recommended only to those clients who can and are willing to tolerate the risks of those investments and for whom the potential benefits may justify the risks.<sup>29</sup> Whether the advice is in a client's best interest must be evaluated in the context of the portfolio that the adviser manages for the client and the client's investment profile. For example, when an adviser is advising a client with a conservative investment objective, investing in certain derivatives may be in the client's best interest when they are used to hedge interest rate risk in the client's portfolio, whereas investing in certain directionally speculative derivatives on their own may not. For that same client, investing in a particular security on margin may not be in the client's best interest, even if investing in that same security may be in the client's best interest. When advising a financially sophisticated investor with a high risk tolerance, however, it may be consistent with the adviser's duties to recommend investing in such directionally speculative derivatives or investing in securities on margin.

The cost (including fees and compensation) associated with investment advice would generally be one of many important factors—such as the investment product's or strategy's investment objectives, characteristics (including any special or unusual features), liquidity, risks

---

<sup>29</sup> We note that Item 8 of Part 2A of Form ADV requires an investment adviser to describe its methods of analysis and investment strategies and disclose that investing in securities involves risk of loss which clients should be prepared to bear. This item also requires that an adviser explain the material risks involved for each significant investment strategy or method of analysis it uses and particular type of security it recommends, with more detail if those risks are significant or unusual.

and potential benefits, volatility and likely performance in a variety of market and economic conditions—to consider when determining whether a security or investment strategy involving a security or securities is in the best interest of the client. Accordingly, the fiduciary duty does not necessarily require an adviser to recommend the lowest cost investment product or strategy. We believe that an adviser could not reasonably believe that a recommended security is in the best interest of a client if it is higher cost than a security that is otherwise identical, including any special or unusual features, liquidity, risks and potential benefits, volatility and likely performance. For example, if an adviser advises its clients to invest in a mutual fund share class that is more expensive than other available options when the adviser is receiving compensation that creates a potential conflict and that may reduce the client’s return, the adviser may violate its fiduciary duty and the antifraud provisions of the Advisers Act if it does not, at a minimum, provide full and fair disclosure of the conflict and its impact on the client and obtain informed client consent to the conflict.<sup>30</sup> Furthermore, an adviser would not satisfy its fiduciary duty to provide advice that is in the client’s best interest by simply advising its client to invest in the least expensive or least remunerative investment product or strategy without any further analysis of other factors in the context of the portfolio that the adviser manages for the client and the client’s investment profile. For example, it might be consistent with an adviser’s fiduciary duty to advise a client with a high risk tolerance and significant investment experience to invest in a private equity fund with relatively high fees if other factors about the fund, such as its diversification and potential performance benefits, cause it to be in the client’s best interest. We believe that a reasonable belief that investment advice is in the best interest of a client also

---

<sup>30</sup> See *infra* notes 48 – 52 and accompanying text (discussing an adviser’s duties related to disclosure and consent).

requires that an adviser conduct a reasonable investigation into the investment sufficient to not base its advice on materially inaccurate or incomplete information.<sup>31</sup> We have brought enforcement actions where an investment adviser did not independently or reasonably investigate securities before recommending them to clients.<sup>32</sup> This obligation to provide advice that is suitable and in the best interest applies not just to potential investments, but to all advice the investment adviser provides to clients, including advice about an investment strategy or engaging a sub-adviser and advice about whether to rollover a retirement account so that the investment adviser manages that account.

## **ii. Duty to Seek Best Execution**

We have addressed an investment adviser's duty of care in the context of trade execution where the adviser has the responsibility to select broker-dealers to execute client trades (typically in the case of discretionary accounts). We have said that, in this context, an adviser has the duty to seek best execution of a client's transactions.<sup>33</sup> In meeting this obligation, an adviser must seek to obtain the execution of transactions for each of its clients such that the client's total cost or proceeds in each transaction are the most favorable under the circumstances. An adviser fulfills this duty by executing securities transactions on behalf of a client with the goal of

---

<sup>31</sup> See, e.g., Concept Release on the U.S. Proxy System, Investment Advisers Act Release No. 3052 (July 14, 2010) (stating "as a fiduciary, the proxy advisory firm has a duty of care requiring it to make a reasonable investigation to determine that it is not basing its recommendations on materially inaccurate or incomplete information").

<sup>32</sup> See *In the Matter of Larry C. Grossman*, Investment Advisers Act Release No. 4543 (Sept. 30, 2016) (Commission opinion) (imposing liability on a principal of a registered investment adviser for recommending offshore private investment funds to clients without a reasonable independent basis for his advice).

<sup>33</sup> See Commission Guidance Regarding Client Commission Practices Under Section 28(e) of the Securities Exchange Act of 1934, Exchange Act Release No. 54165 (July 18, 2006) (stating that investment advisers have "best execution obligations"); Investment Advisers Act Release 3060, *supra* note 10 (discussing an adviser's best execution obligations in the context of directed brokerage arrangements and disclosure of soft dollar practices). See also Advisers Act rule 206(3)-2(c) (referring to adviser's duty of best execution of client transactions).

maximizing value for the client under the particular circumstances occurring at the time of the transaction. As noted below, maximizing value can encompass more than just minimizing cost. When seeking best execution, an adviser should consider “the full range and quality of a broker’s services in placing brokerage including, among other things, the value of research provided as well as execution capability, commission rate, financial responsibility, and responsiveness” to the adviser.<sup>34</sup> In other words, the determinative factor is not the lowest possible commission cost but whether the transaction represents the best qualitative execution. Further, an investment adviser should “periodically and systematically” evaluate the execution it is receiving for clients.<sup>35</sup>

### **iii. Duty to Act and to Provide Advice and Monitoring over the Course of the Relationship**

An investment adviser’s duty of care also encompasses the duty to provide advice and monitoring over the course of a relationship with a client.<sup>36</sup> An adviser is required to provide advice and services to a client over the course of the relationship at a frequency that is both in the

---

<sup>34</sup> Exchange Act Release 23170, *supra* note 25.

<sup>35</sup> *Id.* The Advisers Act does not prohibit advisers from using an affiliated broker to execute client trades. However, the adviser’s use of such an affiliate involves a conflict of interest that must be fully and fairly disclosed and the client must provide informed consent to the conflict.

<sup>36</sup> See SEC v. Capital Gains, *supra* note 2 (describing advisers’ “basic function” as “furnishing to clients on a personal basis competent, unbiased, and continuous advice regarding the sound management of their investments” (quoting Investment Trusts and Investment Companies, Report of the Securities and Exchange Commission, Pursuant to Section 30 of the Public Utility Holding Company Act of 1935, on Investment Counsel, Investment Management, Investment Supervisory, and Investment Advisory Services, H.R. Doc. No. 477, 76<sup>th</sup> Cong. 2d Sess., 1, at 28)). Cf. Barbara Black, *Brokers and Advisers-What’s in a Name?*, 32 Fordham Journal of Corporate and Financial Law XI (2005) (“[W]here the investment adviser’s duties include management of the account, [the adviser] is under an obligation to monitor the performance of the account and to make appropriate changes in the portfolio.”); Arthur B. Laby, *Fiduciary Obligations of Broker-Dealers and Investment Advisers*, 55 Villanova Law Review 701, at 728 (2010) (“Laby Villanova Article”) (“If an adviser has agreed to provide continuous supervisory services, the scope of the adviser’s fiduciary duty entails a continuous, ongoing duty to supervise the client’s account, regardless of whether any trading occurs. This feature of the adviser’s duty, even in a non-discretionary account, contrasts sharply with the duty of a broker administering a non-discretionary account, where no duty to monitor is required.”) (internal citations omitted).

best interest of the client and consistent with the scope of advisory services agreed upon between the investment adviser and the client. The duty to provide advice and monitoring is particularly important for an adviser that has an ongoing relationship with a client (for example, a relationship where the adviser is compensated with a periodic asset-based fee or an adviser with discretionary authority over client assets). Conversely, the steps needed to fulfill this duty may be relatively circumscribed for the adviser and client that have agreed to a relationship of limited duration via contract (for example, a financial planning relationship where the adviser is compensated with a fixed, one-time fee commensurate with the discrete, limited-duration nature of the advice provided).<sup>37</sup> An adviser's duty to monitor extends to all personalized advice it provides the client, including an evaluation of whether a client's account or program type (for example, a wrap account) continues to be in the client's best interest.

## **B. Duty of Loyalty**

The duty of loyalty requires an investment adviser to put its client's interests first. An investment adviser must not favor its own interests over those of a client or unfairly favor one client over another.<sup>38</sup> In seeking to meet its duty of loyalty, an adviser must make full and fair disclosure to its clients of all material facts relating to the advisory relationship.<sup>39</sup> In addition, an

---

<sup>37</sup> See Laby Villanova Article, *supra* note 36, at 728 (2010) (stating that the scope of an adviser's activity can be altered by contract and that an adviser's fiduciary duty would be commensurate with the scope of the relationship).

<sup>38</sup> See Investment Advisers Act Release 3060 ("Under the Advisers Act, an adviser is a fiduciary whose duty is to serve the best interests of its clients, which includes an obligation not to subrogate clients' interests to its own," citing Investment Advisers Act Release 2106 *supra* note 9). See also Staff of the U.S. Securities and Exchange Commission, *Study on Investment Advisers and Broker-Dealers As Required by Section 913 of the Dodd-Frank Wall Street Reform and Consumer Protection Act* (Jan. 2011), available at <https://www.sec.gov/news/studies/2011/913studyfinal.pdf> ("913 Study").

<sup>39</sup> Investment Advisers Act Release 3060, *supra* note 6 ("as a fiduciary, an adviser has an ongoing obligation to inform its clients of any material information that could affect the advisory relationship"). See also General Instruction 3 to Part 2 of Form ADV ("Under federal and state law, you are a fiduciary and must make full disclosure to your *clients* of all material facts relating to the advisory relationship.").

adviser must seek to avoid conflicts of interest with its clients, and, at a minimum, make full and fair disclosure of all material conflicts of interest that could affect the advisory relationship. The disclosure should be sufficiently specific so that a client is able to decide whether to provide informed consent to the conflict of interest.<sup>40</sup> We discuss each of these aspects of the duty of loyalty below.

Because an adviser must serve the best interests of its clients, it has an obligation not to subordinate its clients' interests to its own. For example, an adviser cannot favor its own interests over those of a client, whether by favoring its own accounts or by favoring certain client accounts that pay higher fee rates to the adviser over other client accounts.<sup>41</sup> Accordingly, the duty of loyalty includes a duty not to treat some clients favorably at the expense of other clients. Thus, we believe that in allocating investment opportunities among eligible clients, an adviser

---

<sup>40</sup> Arleen Hughes, *supra* note 13, at 4 and 8 (stating, “[s]ince loyalty to his trust is the first duty which a fiduciary owes to his principal, it is the general rule that a fiduciary must not put himself into a position where his own interests may come in conflict with those of his principal. To prevent any conflict and the possible subordination of this duty to act solely for the benefit of his principal, a fiduciary at common law is forbidden to deal as an adverse party with his principal. An exception is made, however, where the principal gives his informed consent to such dealings,” and adding that, “[r]egistrant has an affirmative obligation to disclose all material facts to her clients in a manner which is clear enough so that a client is fully apprised of the facts and is in a position to give his informed consent.”). *See also Hughes v. Securities and Exchange Commission*, 174 F.2d 969 (1949) (affirming the SEC decision in Arleen Hughes).

*See also* General Instruction 3 to Part 2 of Form ADV (stating that an adviser's disclosure obligation “requires that [the adviser] provide the client with sufficiently specific facts so that the client is able to understand the conflicts of interest [the adviser has] and the business practices in which [the adviser] engage[s], and can give informed consent to such conflicts or practices or reject them”); Investment Advisers Act Release 3060, *supra* note 10 (same); Restatement (Third) of Agency §8.06 (“Conduct by an agent that would otherwise constitute a breach of duty as stated in §§ 8.01, 8.02, 8.03, 8.04, and 8.05 [referencing the fiduciary duty] does not constitute a breach of duty if the principal consents to the conduct, provided that (a) in obtaining the principal's consent, the agent (i) acts in good faith, (ii) discloses all material facts that the agent knows, has reason to know, or should know would reasonably affect the principal's judgment unless the principal has manifested that such facts are already known by the principal or that the principal does not wish to know them, and (iii) otherwise deals fairly with the principal; and (b) the principal's consent concerns either a specific act or transaction, or acts or transactions of a specified type that could reasonably be expected to occur in the ordinary course of the agency relationship”)

<sup>41</sup> The Commission has brought numerous enforcement actions against advisers that unfairly allocated trades to their own accounts and allocated less favorable or unprofitable trades to their clients' accounts. *See, e.g., SEC v. Strategic Capital Management, LLC and Michael J. Breton*, Litigation Release No. 23867 (June 23, 2017) (partial settlement) (adviser placed trades through a master brokerage account and then allocated profitable trades to adviser's account while placing unprofitable trades into the client accounts.).

must treat all clients fairly.<sup>42</sup> This does not mean that an adviser must have a *pro rata* allocation policy, that the adviser's allocation policies cannot reflect the differences in clients' objectives or investment profiles, or that the adviser cannot exercise judgment in allocating investment opportunities among eligible clients. Rather, it means that an adviser's allocation policies must be fair and, if they present a conflict, the adviser must fully and fairly disclose the conflict such that a client can provide informed consent.

An adviser must seek to avoid conflicts of interest with its clients, and, at a minimum, make full and fair disclosure to its clients of all material conflicts of interest that could affect the advisory relationship.<sup>43</sup> Disclosure of a conflict alone is not always sufficient to satisfy the adviser's duty of loyalty and section 206 of the Advisers Act.<sup>44</sup> Any disclosure must be clear and detailed enough for a client to make a reasonably informed decision to consent to such conflicts and practices or reject them.<sup>45</sup> An adviser must provide the client with sufficiently specific facts so that the client is able to understand the adviser's conflicts of interest and

---

<sup>42</sup> See also Barry Barbash and Jai Massari, *The Investment Advisers Act of 1940; Regulation by Accretion*, 39 Rutgers Law Journal 627 (2008) (stating that under section 206 of the Advisers Act and traditional notions of fiduciary and agency law an adviser must not give preferential treatment to some clients or systematically exclude eligible clients from participating in specific opportunities without providing the clients with appropriate disclosure regarding the treatment).

<sup>43</sup> See *SEC v. Capital Gains*, *supra* note 2 (advisers must fully disclose all material conflicts, citing Congressional intent "to eliminate, or at least expose, all conflicts of interest which might incline an investment adviser—consciously or unconsciously—to render advice which was not disinterested"). See also Investment Advisers Act Release 3060, *supra* note 9.

<sup>44</sup> See *SEC v. Capital Gains*, *supra* note 2 (in discussing the legislative history of the Advisers Act, citing ethical standards of one of the leading investment counsel associations, which provided that an investment counsel should remain "as free as humanly possible from the subtle influence of prejudice, conscious or unconscious" and "avoid any affiliation, or any act which subjects his position to challenge in this respect" and stating that one of the policy purposes of the Advisers Act is "to mitigate and, so far as is presently practicable to eliminate the abuses" that formed the basis of the Advisers Act). Separate and apart from potential liability under the antifraud provisions of the Advisers Act enforceable by the Commission for breaches of fiduciary duty in the absence of full and fair disclosure, investment advisers may also wish to consider their potential liability to clients under state common law, which may vary from state to state.

<sup>45</sup> See Arlene Hughes, *supra* at 13 (in finding that registrant had not obtained informed consent, citing to testimony indicating that "some clients had no understanding at all of the nature and significance" of the disclosure).



business practices well enough to make an informed decision.<sup>46</sup> For example, an adviser disclosing that it “may” have a conflict is not adequate disclosure when the conflict actually exists.<sup>47</sup> A client’s informed consent can be either explicit or, depending on the facts and circumstances, implicit. We believe, however, that it would not be consistent with an adviser’s fiduciary duty to infer or accept client consent to a conflict where either (i) the facts and circumstances indicate that the client did not understand the nature and import of the conflict, or (ii) the material facts concerning the conflict could not be fully and fairly disclosed.<sup>48</sup> For example, in some cases, conflicts may be of a nature and extent that it would be difficult to provide disclosure that adequately conveys the material facts or the nature, magnitude and potential effect of the conflict necessary to obtain informed consent and satisfy an adviser’s fiduciary duty. In other cases, disclosure may not be specific enough for clients to understand whether and how the conflict will affect the advice they receive. With some complex or

---

<sup>46</sup> See General Instruction 3 to Part 2 of Form ADV. Cf. Arleen Hughes, *supra* note 13 (Hughes acted simultaneously in the dual capacity of investment adviser and of broker and dealer and conceded having a fiduciary duty. In describing the fiduciary duty and her potential liability under the antifraud provisions of the Securities Act and the Exchange Act, the Commission stated she had “an affirmative obligation to disclose all material facts to her clients in a manner which is clear enough so that a client is fully apprised of the facts and is in a position to give his informed consent.”).

<sup>47</sup> We have brought enforcement actions in such cases. See, e.g., In the Matter of The Robare Group, Ltd., et al., Investment Advisers Act Release No. 4566 (Nov. 7, 2016) (Commission Opinion) (appeal docketed) (finding, among other things, that adviser’s disclosure was inadequate because it stated that the adviser *may* receive compensation from a broker as a result of the facilitation of transactions on client’s behalf through such broker-dealer and that these arrangements *may* create a conflict of interest when adviser *was*, in fact, receiving payments from the broker and *had* such a conflict of interest).

<sup>48</sup> See Arleen Hughes, *supra* note 13 (“Registrant cannot satisfy this duty by executing an agreement with her clients which the record shows some clients do not understand and which, in any event, does not contain the essential facts which she must communicate.”) Some commenters on Commission requests for comment agreed that full and fair disclosure and informed consent are important components of an adviser’s fiduciary duty. See, e.g., Financial Planning Coalition 2013 Letter, *supra* note 21 (“[C]onsent is only informed if the customer has the ability fully to understand and to evaluate the information. Many complex products ... are appropriate only for sophisticated and experienced investors. It is not sufficient for a fiduciary to make disclosure of potential conflicts of interest with respect to such products. The fiduciary must make a reasonable judgment that the customer is fully able to understand and to evaluate the product and the potential conflicts of interest that it presents – and then the fiduciary must make a judgment that the product is in the best interests of the customer.”).

extensive conflicts, it may be difficult to provide disclosure that is sufficiently specific, but also understandable, to the adviser's clients. In all of these cases where full and fair disclosure and informed consent is insufficient, we expect an adviser to eliminate the conflict or adequately mitigate the conflict so that it can be more readily disclosed.

Full and fair disclosure of all material facts that could affect an advisory relationship, including all material conflicts of interest between the adviser and the client, can help clients and prospective clients in evaluating and selecting investment advisers. Accordingly, we require advisers to deliver to their clients a "brochure," under Part 2A of Form ADV, which sets out minimum disclosure requirements, including disclosure of certain conflicts.<sup>49</sup> Investment advisers are required to deliver the brochure to a prospective client at or before entering into a contract so that the prospective client can use the information contained in the brochure to decide whether or not to enter into the advisory relationship.<sup>50</sup> In a concurrent release, we are proposing to require all investment advisers to deliver to retail investors before or at the time the adviser enters into an investment advisory agreement a relationship summary which would include a summary of certain conflicts of interest.<sup>51</sup>

---

<sup>49</sup> Investment Advisers Act Release 3060, *supra* note 10; General Instruction 3 to Part 2 of Form ADV ("Under federal and state law, you are a fiduciary and must make full disclosure to your clients of all material facts relating to the advisory relationship. As a fiduciary, you also must seek to avoid conflicts of interest with your clients, and, at a minimum, make full disclosure of all material conflicts of interest between you and your clients that could affect the advisory relationship. This obligation requires that you provide the client with sufficiently specific facts so that the client is able to understand the conflicts of interest you have and the business practices in which you engage, and can give informed consent to such conflicts or practices or reject them.").

<sup>50</sup> Investment Advisers Act rule 204-3. Investment Advisers Act Release 3060, *supra* note 10 (adopting amendments to Form ADV and stating that "A client may use this disclosure to select his or her own adviser and evaluate the adviser's business practices and conflicts on an ongoing basis. As a result, the disclosure clients and prospective clients receive is critical to their ability to make an informed decision about whether to engage an adviser and, having engaged the adviser, to manage that relationship.").

<sup>51</sup> Form CRS Proposal, *supra* note 6.

### **C. Request for Comment**

The Commission requests comment on our proposed interpretation regarding certain aspects of the fiduciary duty under section 206 of the Advisers Act.

- Does the Commission's proposed interpretation offer sufficient guidance with respect to the fiduciary duty under section 206 of the Advisers Act?
- Are there any significant issues related to an adviser's fiduciary duty that the proposed interpretation has not addressed?
- Would it be beneficial for investors, advisers or broker-dealers for the Commission to codify any portion of our proposed interpretation of the fiduciary duty under section 206 of the Advisers Act?

## **III. ECONOMIC CONSIDERATIONS**

The Commission is sensitive to the potential economic effects of the proposed interpretation provided above.<sup>52</sup> In this section we discuss how the proposed Commission interpretation may benefit investors and reduce agency problems by reaffirming and clarifying the fiduciary duty an investment adviser owes to its clients. We also discuss some potential broader economic effects on the market for investment advice.

### **A. Background**

The Commission's interpretation of the standard of conduct for investment advisers under the Advisers Act set forth in this Release would affect investment advisers and their associated persons as well as the clients of those investment advisers, and the market for

---

<sup>52</sup> The Commission, where possible, has sought to quantify the economic impacts expected to result from the proposed interpretations. However, as discussed more specifically below, the Commission is unable to quantify certain of the economic effects because it lacks information necessary to provide reasonable estimates.

financial advice more broadly.<sup>53</sup> There are 12,659 investment advisers registered with the Commission with over \$72 trillion in assets under management as well as 17,635 investment advisers registered with states and 3,587 investment advisers who submit Form ADV as exempt reporting advisers.<sup>54</sup> As of December 2017, there are approximately 36 million client accounts advised by SEC-registered investment advisers.

These investment advisers currently incur ongoing costs related to their compliance with their legal and regulatory obligations, including costs related to their understanding of the standard of conduct. We believe, based on the Commission's experience, that the interpretations we are setting forth in this Release are generally consistent with investment advisers' current understanding of the practices necessary to comply with their fiduciary duty under the Advisers Act; however, we recognize that there may be certain current investment advisers who have interpreted their fiduciary duty to require something less, or something more, than the Commission's interpretation. We lack data to identify which investment advisers currently understand the practices necessary to comply with their fiduciary duty to be different from the standard of conduct in the Commission's interpretation. Based on our experience, however, we generally believe that it is not a significant portion of the market.

## **B. Economic Impacts**

Based on our experience as the long-standing regulator of the investment adviser industry, the Commission's interpretation of the fiduciary duty under section 206 of the Advisers

---

<sup>53</sup> See Form CRS Proposal, *supra* note 6, at Section IV.A (discussing the market for financial advice generally).

<sup>54</sup> See Form CRS Proposal, *supra* note 6, at Section IV.A.1.b (discussing SEC-registered investment advisers). Note, however, that because we are interpreting advisers' fiduciary duties under section 206 of the Advisers Act, this interpretation would be applicable to both SEC- and state-registered investment advisers, as well as other investment advisers that are exempt from registration or subject to a prohibition on registration under the Advisers Act.

Act described in this Release generally reaffirms the current practices of investment advisers. Therefore, we expect there to be no significant economic impacts from the interpretation. We do acknowledge, however, to the extent certain investment advisers currently understand the practices necessary to comply with their fiduciary duty to be different from those discussed in this interpretation, there could be some potential economic effects, which we discuss below.

*Clients of investment advisers*

The typical relationship between an investment adviser and a client is a principal-agent relationship, where the principal (the client) hires an agent (the investment adviser) to perform some service (investment advisory services) on the client's behalf.<sup>55</sup> Because investors and investment advisers are likely to have different preferences and goals, the investment adviser relationship is subject to agency problems: that is, investment advisers may take actions that increase their well-being at the expense of investors, thereby imposing agency costs on investors.<sup>56</sup> A fiduciary duty, such as the duty investment advisers owe their clients, can mitigate these agency problems and reduce agency costs by deterring agents from taking actions that expose them to legal liability.<sup>57</sup>

To the extent the Commission's interpretation of investment adviser fiduciary duty would cause a change in behavior of those investment advisers, if any, who currently interpret their fiduciary duty to require something different from the Commission's interpretation, we expect a

---

<sup>55</sup> See, e.g., James A. Brickley, Clifford W. Smith, Jr., Jerold L. Zimmerman, *Managerial Economics and Organizational Architecture* (2004), at 265 ("An agency relationship consists of an agreement under which one party, the principal, engages another party, the agent, to perform some service on the principal's behalf."). See also Michael C. Jensen and William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, *Journal of Financial Economics*, Vol. 3, 305-360 (1976).

<sup>56</sup> See, e.g., Jensen and Meckling, *supra* note 55. See also the discussion on agency problems in the market for investment advice in Section IV.B. of the Regulation Best Interest Proposal, *supra* note 5.

<sup>57</sup> See, e.g., Frank H. Easterbrook and Daniel R. Fischel, *Contract and Fiduciary Duty*, *Journal of Law & Economics*, Vol. 36, 425-46 (1993).

potential reduction in agency problems and, consequently, a reduction of agency costs to the client. The extent to which agency costs would be reduced is difficult to assess given that we are unable to ascertain whether any investment advisers currently interpret their fiduciary duty to be something different from the Commission's interpretation, and consequently we are not able to estimate the agency costs these advisers, if any, currently impose on investors. However, we believe that there may be potential benefits for clients of those investment advisers, if any, to the extent the Commission's interpretation is effective at strengthening investment advisers' understanding of their obligations to their clients. For example, to the extent that the Commission's interpretation enhances the understanding of any investment advisers of their duty of care, it may potentially raise the quality of investment advice given and that advice's fit with a client's individual profile and preferences or lead to increased compliance with the duty to provide advice and monitoring over the course of the relationship.

Additionally, to the extent the Commission's interpretation enhances the understanding of any investment advisers of their duty of loyalty it may potentially benefit the clients of those investment advisers. Specifically, to the extent this leads to a higher quality of disclosures about conflicts for clients of some investment advisers, the nature and extent of such conflict disclosures would help investors better assess the quality of the investment advice they receive, therefore providing an important benefit to investors.

Further, to the extent that the interpretation causes some investment advisers to properly identify circumstances in which disclosure alone cannot cure a conflict of interest, the proposed interpretation may lead those investment advisers to take additional steps to mitigate or eliminate the conflict. The interpretation may also cause some investment advisers to conclude in some circumstances that even if disclosure would be enough to meet their fiduciary duty, such

disclosure would have to be so expansive or complex that they instead voluntarily mitigate or eliminate the conflicts of interest. Thus, to the extent the Commission's interpretation would cause investment advisers to better understand their obligations as part of their fiduciary duty and therefore to make changes to their business practices in ways that reduce the likelihood of conflicted advice or the magnitude of the conflicts, it may ameliorate the agency conflict between investment advisers and their clients and, in turn, may improve the quality of advice that the clients receive. This less-conflicted advice may therefore produce higher overall returns for clients and increase the efficiency of portfolio allocation. However, as discussed above, we would generally expect these effects to be minimal. Finally, this interpretation would also benefit clients of investment advisers to the extent it assists the Commission in its oversight of investment advisers' compliance with their regulatory obligations.

*Investment advisers and the market for investment advice*

In general, we expect the Commission's interpretation of an investment adviser's fiduciary duty would affirm investment advisers' understanding of the obligations they owe their clients, reduce uncertainty for advisers, and facilitate their compliance. Furthermore, by addressing in one release certain aspects of the fiduciary duty that an investment adviser owes to its clients, the Commission's interpretation could reduce the costs associated with comprehensively assessing their compliance obligations. We acknowledge that, as with other circumstances in which the Commission speaks to the legal obligations of regulated entities, affected firms, including those whose practices are consistent with the Commission's interpretation, incur costs to evaluate the Commission's interpretation and assess its applicability to them. Moreover, as discussed above, there may be certain investment advisers who currently understand the practices necessary to comply with their fiduciary duty to be different from the

standard of conduct in the Commission's interpretation. Those investment advisers if any, would experience an increase in their compliance costs as they change their systems, processes and behavior, and train their supervised persons, to align with the Commission's interpretation.

Moreover, to the extent any investment advisers that understood their fiduciary obligation to be different from the Commission's interpretation change their behavior to align with this interpretation, there could potentially also be some economic effects on the market for investment advice. For example, any improved compliance may not only reduce agency costs in current investment advisory relationships and increase the value of those relationships to current clients, it may also increase trust in the market for investment advice among all investors, which may result in more investors seeking advice from investment advisers. This may, in turn, benefit investors by improving the efficiency of their portfolio allocation. To the extent it is costly or difficult, at least in the short term, to expand the supply of investment advisory services to meet an increase in demand, any such new demand for investment adviser services could potentially put some upward price pressure on fees. At the same time, however, if any such new demand increases the overall profitability of investment advisory services, then we expect it would encourage entry by new investment advisers – or hiring of new representatives, by current investment advisers – such that competition would increase over time. Indeed, we recognize that the recent growth in the investment adviser segment of the market, both in terms of firms and number of representatives,<sup>58</sup> may suggest that the costs of expanding the supply of investment advisory services are currently relatively low.

Additionally, we acknowledge that to the extent certain investment advisers recognize, due to the Commission's interpretation, that their obligations to clients are stricter than how they

---

<sup>58</sup> See Form CRS Proposal, *supra* note 6, at Section IV.A.1.d.



currently interpret their fiduciary duty, it could potentially affect competition. Specifically, the Commission's interpretation of certain aspects of the standard of conduct for investment advisers may result in additional compliance costs to meet their fiduciary obligation under the Commission's interpretation. This increase in compliance costs, in turn, may discourage competition for client segments that generate lower revenues, such as clients with relatively low levels of financial assets, which could reduce the supply of investment adviser services and raise fees for these client segments. However, the investment advisers who already are complying with the understanding of their fiduciary duty reflected in the Commission's interpretation, and may therefore currently have a comparative cost disadvantage, could potentially find it more profitable to compete for the customers of those investment advisers who would face higher compliance costs as a result of the proposed interpretation, which would mitigate negative effects on the supply of investment adviser services. Furthermore, as noted above, there has been a recent growth trend in the supply of investment advisory services, which is likely to mitigate any potential negative supply effects from the Commission's interpretation.<sup>59</sup>

Finally, to the extent the proposed interpretation would cause some investment advisers to reassess their compliance with their disclosure obligations, it could lead to a reduction in the expected profitability of certain products associated with particularly conflicted advice for which

---

<sup>59</sup> Beyond having an effect on competition in the market for investment adviser services, it is possible that the Commission's interpretation could affect competition between investment advisers and other providers of financial advice, such as broker-dealers, banks, and insurance companies. This may be the case if certain investors base their choice between an investment adviser and another provider of financial advice, at least in part, on their perception of the standards of conduct each owes to their customers. To the extent that the Commission's interpretation increases investors' trust in investment advisers' overall compliance with their standard of conduct, certain of these investors may become more willing, to hire an investment adviser rather than one of their non-investment adviser competitors. As a result, investment advisers as a group may increase their competitive situation compared to that of other types of providers of financial advice. On the other hand, if the Commission's interpretation raises costs for investment advisers, they could become less competitive with other financial services providers.

compliance costs would increase following the reassessment.<sup>60</sup> As a result, the number of investment advisers willing to advise a client to make these investments may be reduced. A decline in the supply of investment adviser advice on these investments could potentially reduce the efficiency of portfolio allocation of those investors who might otherwise benefit from investment adviser advice on these investments.

#### **IV. REQUEST FOR COMMENT REGARDING AREAS OF ENHANCED INVESTMENT ADVISER REGULATION**

In 2011, the Commission issued the staff's 913 Study, pursuant to section 913 of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, in which the staff recognized several areas for potential harmonization of broker-dealer and investment adviser regulation.<sup>61</sup> We have identified a few discrete areas where the current broker-dealer framework provides investor protections that may not have counterparts in the investment adviser context, and request comment on those areas. The Commission intends to consider these comments in connection with any future proposed rules or other proposed regulatory actions with respect to these matters.

---

<sup>60</sup> For example, such products could include highly complex, high cost products with risk and return characteristics that are hard to fully understand for retail investors or mutual funds or fund share classes that may pay higher compensation to investment advisers that are dual registrants, or that the investment adviser and its representatives may receive through payments to an affiliated broker-dealer or third party broker-dealer with which representatives of the investment adviser are associated.

<sup>61</sup> The staff made two primary recommendations in the 913 Study. The first recommendation was that we engage in rulemaking to implement a uniform fiduciary standard of conduct for broker-dealers and investment advisers when providing personalized investment advice about securities to retail customers. The second recommendation was that we consider harmonizing certain regulatory requirements of broker-dealers and investment advisers where such harmonization appears likely to enhance meaningful investor protection, taking into account the best elements of each regime. In the 913 Study, the areas the staff suggested the Commission consider for harmonization included, among others, licensing and continuing education requirements for persons associated with firms. The staff stated that the areas identified were not intended to be a comprehensive or exclusive listing of potential areas of harmonization. *See* 913 Study *supra* note 38.

## A. Federal Licensing and Continuing Education

Associated persons of broker-dealers that effect securities transactions are required to be registered with the Financial Industry Regulatory Authority (“FINRA”),<sup>62</sup> and must meet qualification requirements, which include passing a securities qualification exam and fulfilling continuing education requirements.<sup>63</sup> The federal securities laws do not require investment adviser representatives to become licensed or to meet qualification requirements, but most states impose registration, licensing, or qualification requirements on investment adviser representatives who have a place of business in the state, regardless of whether the investment adviser is registered with the Commission or the state.<sup>64</sup> These qualification requirements typically mandate that investment adviser representatives register and pass certain securities exams or hold certain designations (such as Chartered Financial Analyst credential).<sup>65</sup> The staff recommended in the 913 Study that the Commission consider requiring investment adviser representatives to be subject to federal continuing education and licensing requirements.<sup>66</sup>

---

<sup>62</sup> Generally, all registered broker-dealers that deal with the public must become members of FINRA, a registered national securities association, and may choose to become exchange members. *See* Exchange Act section 15(b)(8) and Exchange Act rule 15b9-1. FINRA is the sole national securities association registered with the SEC under section 15A of the Exchange Act.

<sup>63</sup> *See* NASD Rule 1021 (“Registration Requirements”); NASD Rule 1031 (“Registration Requirements”); NASD Rule 1041 (“Registration Requirements for Assistant Representatives”); FINRA Rule 1250 (“Continuing Education Requirements”).

<sup>64</sup> *See* 913 Study, *supra* note 38, at 86. *See also* Advisers Act rule 203A-3(a) (definition of “investment adviser representative”).

<sup>65</sup> *See* 913 Study, *supra* note 38, at 86-87, 138. The North American Securities Administrators Association (“NASAA”) is considering a potential model rule that would require that investment adviser representatives meet a continuing education requirement in order to maintain their state registrations. An internal survey of NASAA’s membership identified strong support for such a requirement along with significant regulatory need. NASAA is now conducting a nationwide survey of relevant stakeholders to get their input and views on such a requirement. For more information, see <http://www.nasaa.org/industry-resources/investment-advisers/nasaa-survey-regarding-continuing-education-for-investment-adviser-representatives/>.

<sup>66</sup> Several commenters, cited in the 913 Study, suggested that this was a gap that should be addressed. *See* 913 Study, *supra* note 38, at 138 (citing letters from AALU, Bank of America, FSI, Hartford, LPL, UBS, and Woodbury).

We request comment on whether there should be federal licensing and continuing education requirements for personnel of SEC-registered investment advisers. Such requirements could be designed to address minimum and ongoing competency requirements for the personnel of SEC-registered advisers.<sup>67</sup>

- Should investment adviser representatives be subject to federal continuing education and licensing requirements?
- Which advisory personnel should be included in these requirements? For example, should persons whose functions are solely clerical or ministerial be excluded, similar to the exclusion in the FINRA rules regarding broker-dealer registered representatives? Should a subset of registered investment adviser personnel (such as supervised persons, individuals for whom an adviser must deliver a Form ADV brochure supplement, “investment adviser representatives” as defined in the Advisers Act, or some other group) be required to comply with such requirements?
- How should the continuing education requirement be structured? How frequent should the certification be? How many hours of education should be required? Who should determine what qualifies as an authorized continuing education class?
- How could unnecessary duplication of any existing continuing education requirement be avoided?
- Should these individuals be required to register with the Commission? What information should these individuals be required to disclose on any registration form? Should the registration requirements mirror the requirements of existing Form U4 or require additional information? Should such registration requirements apply to individuals who

---

<sup>67</sup> See 913 Study, *supra* note 38, at 138.

provide advice on behalf of SEC-registered investment advisers but fall outside the definition of “investment adviser representative” in rule 203A-3 (because, for example, they have five or fewer clients who are natural persons, they provide impersonal investment advice, or ten percent or less of their clients are individuals other than qualified clients)? Should these individuals be required to pass examinations, such as the Series 65 exam required by most states, or to hold certain designations, as part of any registration requirements? Should other steps be required as well, such as a background check or fingerprinting? Would a competency or other examination be a meritorious basis upon which to determine competency and proficiency? Would a competency or other examination requirement provide a false sense of security to advisory clients of competency or proficiency?

- If continuing education requirements are a part of any licensing requirements, should specific topics or types of training be required? For example, these individuals could be required to complete a certain amount of training dedicated to ethics, regulatory requirements or the firm’s compliance program.
- What would the expected benefits of continuing education and licensing be? Would it be an effective way to increase the quality of advice provided to investors? Would it provide better visibility into the qualifications and education of personnel of SEC-registered investment advisers?
- What would the expected costs of continuing education and licensing be? How expensive would it be to obtain the continuing education or procure the license? Do those costs scale, or would they fall more heavily on smaller advisers? Would these

requirements result in a barrier to entry that could decrease the number of advisers and advisory personnel (and thus potentially increase the cost of advice)?

- What would the effects be of continuing education and licensing for investment adviser personnel in the market for investment advice (*i.e.*, as compared to broker-dealers)?
- What other types of qualification requirements should be considered, such as minimum experience requirements or standards regarding an individual's fitness for serving as an investment adviser representative?

## **B. Provision of Account Statements**

Fees and costs are important to retail investors,<sup>68</sup> but many retail investors are uncertain about the fees they will pay.<sup>69</sup> The relationship summary that we are proposing in a concurrent release would discuss certain differences between advisory and brokerage fees to provide investors more clarity concerning the key categories of fees and expenses they should expect to pay, but would not require more complete, specific or personalized disclosures or disclosures about the amount of fees and expenses.<sup>70</sup> We believe that delivery of periodic account statements, if they specified the dollar amounts of fees and expenses, would allow clients to readily see and understand the fees and expenses they pay for an adviser's services. Clients would receive account statements close in time to the assessment of periodic account fees, which

---

<sup>68</sup> See Staff of the Securities and Exchange Commission, *Study Regarding Financial Literacy Among Investors as required by Section 917 of the Dodd-Frank Wall Street Reform and Consumer Protection Act* (Aug. 2012), at iv, available at <https://www.sec.gov/news/studies/2012/917-financial-literacy-study-part1.pdf> ("With respect to financial intermediaries, investors consider information about fees, disciplinary history, investment strategy, conflicts of interest to be absolutely essential.").

<sup>69</sup> See Angela A. Hung, et al., RAND Institute for Civil Justice, *Investor and Industry Perspectives on Investment Advisers and Broker-Dealers* (2008), at xix, available at [https://www.sec.gov/news/press/2008/2008-1\\_randiabreport.pdf](https://www.sec.gov/news/press/2008/2008-1_randiabreport.pdf) ("In fact, focus-group participants with investments acknowledged uncertainty about the fees they pay for their investments, and survey responses also indicate confusion about the fees.").

<sup>70</sup> See Form CRS Proposal, *supra* note 6, at Section II.B.4.

could be an effective way for clients to understand and evaluate the cost of the services they are receiving from their advisers.

Broker-dealers are required to provide confirmations of transactions with detailed information concerning commissions and certain other remuneration, as well as account statements containing a description of any securities positions, money balances or account activity during the period since the last statement was sent to the customer.<sup>71</sup> Broker-dealers generally must provide account statements no less than once every calendar quarter. Brokerage customers must receive periodic account statements even when not receiving immediate trade confirmations.<sup>72</sup> Although we understand that many advisers do provide clients with account statements, advisers are not directly required to provide account statements under the federal securities laws. Notably, however, the custody rule requires advisers with custody of a client's assets to have a reasonable basis for believing that the qualified custodian sends an account statement at least quarterly.<sup>73</sup> In addition, in any separately managed account program relying on rule 3a-4 under the Investment Company Act of 1940, the program sponsor or another person designated by the sponsor must provide clients statements at least quarterly containing specified information.<sup>74</sup>

We request comment on whether we should propose rules to require registered investment advisers to provide account statements, either directly or via the client's custodian, regardless of whether the adviser is deemed to have custody of client assets under Advisers Act

---

<sup>71</sup> See, e.g., NASD Rule 2340; FINRA Rule 2232; MSRB Rule G-15. See also Exchange Act rule 15c3-2 (account statements); Exchange Act rule 10b-10 (confirmation of transactions).

<sup>72</sup> See Confirmation of Transactions, Securities Exchange Act Release No. 34962 (November 10, 1994).

<sup>73</sup> Advisers Act rule 206(4)-2(a)(3) (custody rule). The Commission also has stated that an adviser's policies and procedures, at a minimum, should address the accuracy of disclosures made to investors, clients, and regulators, including account statements.

<sup>74</sup> Investment Company Act of 1940 [15 U.S.C. 80a-1 et seq.] ("Investment Company Act") rule 3a-4(a)(4).

Rule 206(4)-2 or the adviser is a sponsor (or a designee of a sponsor) of a managed account program relying on the safe harbor in Investment Company Act rule 3a-4.

- To what extent do retail clients of registered investment advisers already receive account statements? To what extent do those account statements specify the dollar amounts charged for advisory fees and other fees (*e.g.*, brokerage fees) and expenses? Would retail clients benefit from a requirement that they receive account statements from registered investment advisers? If clients are uncertain about what fees and expenses they will pay, would they benefit from a requirement that, before receiving advice from a registered investment adviser, they enter into a written (including electronic) agreement specifying the fees and expenses to be paid?
- What information, in addition to fees and expenses, would be most useful for retail clients to receive in account statements? Should any requirement to provide account statements have prescriptive requirements as to presentation, content, and delivery? Should they resemble the account statements required to be provided by broker-dealers, under NASD Rule 2340 with the addition of fee disclosure?
- How often should clients receive account statements?
- How costly would it be to provide account statements? Does that cost depend on how those account statements could be delivered (*e.g.*, via U.S. mail, electronic delivery, notice and access)? Are there any other factors that would impact cost?

### **C. Financial Responsibility**

Broker-dealers are subject to a comprehensive financial responsibility program. Pursuant to Exchange Act rule 15c3-1 (the net capital rule), broker-dealers are required to maintain minimum levels of net capital designed to ensure that a broker-dealer under financial stress has



sufficient liquid assets to satisfy all non-subordinated liabilities without the need for a formal liquidation proceeding.<sup>75</sup> Exchange Act rule 15c3-3 (the customer protection rule) requires broker-dealers to segregate customer assets and maintain them in a manner designed to ensure that should the broker-dealer fail, those assets are readily available to be returned to customers.<sup>76</sup> Broker-dealers are also subject to extensive recordkeeping and reporting requirements, including an annual audit requirement as well as a requirement to make their audited balance sheets available to customers.<sup>77</sup> Broker-dealers are required to be members of the Securities Investor Protection Corporation (“SIPC”), which is responsible for overseeing the liquidation of member broker-dealers that close due to bankruptcy or financial trouble and customer assets are missing. When a brokerage firm is closed and customer assets are missing, SIPC, within certain limits, works to return customers’ cash, stock, and other securities held by the firm. If a firm closes, SIPC protects the securities and cash in a customer’s brokerage account up to \$500,000, including up to \$250,000 protection for cash in the account.<sup>78</sup> Finally, FINRA rules require that broker-dealers obtain fidelity bond coverage from an insurance company.<sup>79</sup>

Under Advisers Act rule 206(4)-2, investment advisers with custody must generally maintain client assets with a “qualified custodian,” which includes banks and registered broker-dealers, and must comply with certain other requirements.<sup>80</sup> In 2009 the Commission adopted amendments to the custody requirements for investment advisers that, among other

---

<sup>75</sup> See Exchange Act rule 15c3-1.

<sup>76</sup> See Exchange Act rule 15c3-3.

<sup>77</sup> See Exchange Act rules 17a-3, 17a-4, and 17a-5.

<sup>78</sup> See Securities Investor Protection Act of 1970, Public Law No. 91-598, 84 Stat. 1636 (Dec. 30, 1970), 15 U.S.C. § 78aaa through 15 U.S.C. § 78lll.

<sup>79</sup> See FINRA Rule 4360, (“Fidelity Bonds”).

<sup>80</sup> See Advisers Act rule 206(4)-2.

enhancements, required all registered investment advisers with custody of client assets to undergo an annual surprise examination by an independent public accountant. SEC-registered investment advisers, however, are not subject to any net capital requirements comparable to those applicable to broker-dealers, although they must disclose any material financial condition that impairs their ability to provide services to their clients.<sup>81</sup> Many investment advisers have relatively small amounts of capital, particularly compared to the amount of assets that they have under management.<sup>82</sup> When we discover a serious fraud by an adviser, often the assets of the adviser are insufficient to compensate clients for their loss. In addition, investment advisers are not required to obtain fidelity bonds, unlike many other financial service providers that have access to client assets.<sup>83</sup>

In light of these disparities, we request comment on whether SEC-registered investment advisers should be subject to financial responsibility requirements along the lines of those that apply to broker-dealers.

- What is the frequency and severity of client losses due to investment advisers' inability to satisfy a judgment or otherwise compensate a client for losses due to the investment adviser's wrongdoing?
- Should investment advisers be subject to net capital or other financial responsibility requirements in order to ensure they can meet their obligations, including compensation

---

<sup>81</sup> See Form ADV. Many states have imposed fidelity bonding and/or net capital requirements on state-registered investment advisers. Rule 17g-1 under the Investment Company Act of 1940 requires registered investment companies to obtain fidelity bonds covering their officers and employees who may have access to the investment companies' assets.

<sup>82</sup> See Custody of Funds or Securities of Clients by Investment Advisers, Investment Advisers Act Release No. 2968 (Dec. 30, 2009).

<sup>83</sup> Fidelity bonds are required to be obtained by broker-dealers (FINRA Rule 4360; New York Stock Exchange Rule 319; American Stock Exchange Rule 330); transfer agents (New York Stock Exchange Rule Listed Company Manual §906); investment companies (17 CFR 270.17g-1); national banks (12 CFR 7.2013); federal savings associations (12 CFR 563.190).

for clients if the adviser becomes insolvent or advisory personnel misappropriate clients' assets?<sup>84</sup> Do the custody rule and other rules<sup>85</sup> under the Advisers Act adequately address the potential for misappropriation of client assets and other financial responsibility concerns for advisers? Should investment advisers be subject to an annual audit requirement?

- Should advisers be required to obtain a fidelity bond from an insurance company? If so, should some advisers be excluded from this requirement?<sup>86</sup> Is there information or data

---

<sup>84</sup> We note that Congress and the Commission have considered such requirements in the past. In 1973, a Commission advisory committee recommended that Congress authorize the Commission to adopt minimum financial responsibility requirements for investment advisers, including minimum capital requirements. *See* Report of the Advisory Committee on Investment Management Services for Individual Investors, Small Account Investment Management Services, Fed. Sec. L. Rep. (CCH) No. 465, Pt. III, 64-66 (Jan. 1973) ("Investment Management Services Report"). Three years later, in 1976, the Senate Committee on Banking, Housing and Urban Affairs considered a bill that, among other things, would have authorized the Commission to adopt rules requiring investment advisers (i) with discretionary authority over client assets, or (ii) that advise registered investment companies, to meet financial responsibility standards. S. Rep. No. 94-910, 94th Cong. 2d Sess. (May 20, 1976) (reporting favorably S. 2849). S.2849 was never enacted. In 1992, both the Senate and House of Representatives passed bills that would have given the Commission the explicit authority to require investment advisers with custody of client assets to obtain fidelity bonds. S.226, 102d Cong., 2d Sess. (Aug. 12, 1992) and H.R. 5726, 102d Cong. Ed (Sept. 23, 1992). Differences in these two bills were never reconciled and thus neither became law. In 2003, the Commission requested comment on whether to require a fidelity bonding requirement for advisers as a way to increase private sector oversight of the compliance by funds and advisers with the federal securities laws. The Commission decided not to adopt a fidelity bonding requirement at that time, but noted that it regarded such a requirement as a viable option should the Commission wish to further strengthen compliance programs of funds and advisers. Compliance Programs of Investment Companies and Investment Advisers, Investment Company Act Release No. 25925 (Feb. 5, 2003).

<sup>85</sup> *See, e.g.*, Advisers Act rule 206(4)-7 (requires each investment adviser registered or required to be registered with the Commission to adopt and implement written policies and procedures reasonably designed to prevent violations of the Advisers Act and Advisers Act rules, review those policies and procedures annually, and designate an individual to serve as a chief compliance officer).

<sup>86</sup> As noted above, the 1992 legislation would have given us the explicit authority to require bonding of advisers that have custody of client assets or that have discretionary authority over client assets. Section 412 of ERISA [29 U.S.C. 1112] and related regulations (29 CFR 2550.412-1 and 29 CFR 2580) generally require that every fiduciary of an employee benefit plan and every person who handles funds or other property of such a plan shall be bonded. Registered investment advisers exercising investment discretion over assets of plans covered by title I of ERISA are subject to this requirement; it does not apply to advisers who exercise discretion with respect to assets in an individual retirement account or other non-ERISA retirement account. In 1992, only approximately three percent of Commission registered advisers had discretionary authority over client assets; as of March 31, 2018, according to data collected on Form ADV, 91 percent of Commission registered advisers have that authority.

that demonstrates fidelity bonding requirements provide defrauded clients with recovery, and if so what amount or level of recovery is evidenced?

- Alternatively, should advisers be required to maintain a certain amount of capital that could be the source of compensation for clients?<sup>87</sup> What amount of capital would be adequate?<sup>88</sup>
- What would be the expected cost of either maintaining some form of reserve capital or purchasing a fidelity bond? Specifically, in addition to setting aside the initial sum or purchasing the initial bond, what would be the ongoing cost and the opportunity cost for investment advisers? Would one method or the other be more feasible for certain types of investment advisers (particularly, smaller advisers)?
- Would the North American Securities Administrators Association Minimum Financial Requirements For Investment Advisers Model Rule 202(d)-1<sup>89</sup> (which requires, among other things, an investment adviser who has custody of client funds or securities to maintain at all times a minimum net worth of \$35,000 (with some exceptions), an adviser who has discretionary authority but not custody over client funds or securities to maintain at all times a minimum net worth of \$10,000, and an adviser who accepts prepayment of more than \$500 per client and six or more months in advance to maintain at all times a positive net worth), provide an appropriate model for a minimum capital requirement? Why or why not?

---

<sup>87</sup> See *supra* note 84.

<sup>88</sup> Section 412 of ERISA provides that the bond required under that section must be at least ten percent of the amount of funds handled, with a maximum required amount of \$500,000 (increased to \$1,000,000,000 for plans that hold securities issued by an employer of employees covered by the plan).

<sup>89</sup> NASAA Minimum Financial Requirements For Investment Advisers Model Rule 202(d)-1 (Sept. 11, 2011), available at <http://www.nasaa.org/wp-content/uploads/2011/07/IA-Model-Rule-Minimum-Financial-Requirements.pdf>.

- Although investment advisers are required to report specific information about the assets that they manage on behalf of clients, they are not required to report specific information about their own assets.<sup>90</sup> Should advisers be required to obtain annual audits of their own financials and to provide such information on Form ADV? Would such a requirement raise privacy concerns for privately held advisers?

By the Commission.

Dated: April 18, 2018.

Brent J. Fields  
Secretary

---

<sup>90</sup> Form ADV only requires that advisers with significant assets (at least \$1 billion) report the approximate amount of their assets within one of the three ranges (\$1 billion to less than \$10 billion, \$10 billion to less than \$50 billion, and \$50 billion or more). Item 1.O of Part 1A of Form ADV.

Tab 14



---

## **PROMOTING INNOVATION IN FINANCIAL SERVICES**

April 6, 2018

---

---

## TABLE OF CONTENTS

---

I. Introduction.....	1
II. General Principles and Executive Summary.....	3
III. Discussion of Recommendations .....	7
Recommendation One.....	8
The FSOC should create an FSOC Fintech Subcommittee with the mandate to drive pro-innovation practices at the financial agencies.....	8
A. The FSOC Fintech Subcommittee should create a framework for activities-based fintech regulation and assist the agencies in adopting that framework.....	9
B. The FSOC Fintech Subcommittee should develop a regulatory sandbox to help financial institutions and fintech companies engage in responsible innovation. ....	11
C. The FSOC Fintech Subcommittee should take steps to ensure that the agencies enhance their technical capacity and increase their understanding of new technologies.....	12
D. The FSOC Fintech Subcommittee should build on Treasury’s existing efforts to harmonize federal and state regulatory standards with respect to vendor risk and should collaborate with financial institutions to understand the risks that such relationships present and the ways in which financial institutions oversee those relationships.....	14
E. The FSOC Fintech Subcommittee should identify outmoded regulations, make recommendations for the agencies to modify or rescind those regulations where appropriate and, if necessary, recommend legislative changes to current laws that inhibit responsible innovation. ....	15
(i) EGRPRA and Regulatory Review.....	15
(ii) New Product Guidance and Supervision .....	16
(iii) Laws Related to the Intersection of Technology and Consumer Protection.....	17
(iv) E-SIGN Act and UETA .....	18
(v) Digital Books and Records .....	19
F. The FSOC Fintech Subcommittee should create a framework for the agencies to issue appropriate and consistent no-action letters or interpretive relief.....	20
G. The FSOC Fintech Subcommittee should encourage coordination between state regulators and facilitate the establishment of uniform, national data breach notification requirements..	21
H. The FSOC Fintech Subcommittee should facilitate international coordination on fintech issues and the adoption, with appropriate modifications, of international best practices in the fintech space.....	22
Recommendation Two.....	23
Regulators should assure that all parties that have access to sensitive consumer information, including data aggregators adopt and follow appropriate minimum data access, data handling, and data security standards, and act in a safe and responsible way. ....	23



A. Use of Data.....	24
B. Data Aggregation .....	24
Recommendation Three .....	26
The federal banking agencies should revisit and modify as appropriate their current interpretations of certain banking statutes, including with respect to the meaning of control under the BHC Act and the business of banking under the National Bank Act in order to ensure that such interpretations do not impede investments in fintech innovation.....	26
A. “Control” Under the BHC Act .....	26
B. Permissible Incidental or Financial Activities Under the BHC Act.....	27
C. The Business of Banking Under the National Bank Act.....	28
D. Brokered Deposits .....	29
Recommendation Four.....	30
The SEC should reexamine rules that may unnecessarily inhibit the growth of both traditional and digital forms of advice and should revisit rules that govern how documents must be delivered.....	30
A. Digital Investment Advice .....	31
B. Required Deliveries of Fund Investment and Disclosure Documents .....	32
Recommendation Five .....	34
To resolve the uncertainty created by the <i>Madden v. Midland Funding, LLC</i> decision and to assure the smooth functioning of our financial markets, the Administration should promote a legislative solution to the court challenges to the valid-when-made doctrine. ....	34
Recommendation Six.....	36
The agencies should foster the responsible adoption of distributed ledger technologies by updating regulations that impede their use. ....	36
Recommendation Seven .....	37
In the field of cloud computing, the agencies should draw upon the expertise of industry groups and look wherever possible to harmonize standards across jurisdictions. ....	37
Recommendation Eight.....	38
The Administration should work to discourage other jurisdictions from adopting unreasonable data localization requirements. ....	38
Recommendation Nine .....	39
Treasury and the agencies should facilitate the implementation of artificial intelligence tools that could facilitate compliance and should also support wider adoption of machine learning technologies. ....	39
A. Machine Readable Solutions.....	40
B. Industry’s Use of Artificial Intelligence and Machine Learning .....	40
IV. Appendix A – International Approaches to Fintech Regulation.....	42

## I. INTRODUCTION

## Introduction

---

The Treasury Secretary's pending report on innovation and financial technology, or fintech, is an important opportunity to assess the existing financial regulatory and supervisory framework with an eye towards reform that would promote responsible innovation, enhance the delivery of financial products and services to our communities and thus foster economic growth and development.

President Trump's Core Principles for Regulating the United States Financial System should guide the report. In our view, certain aspects of our current regulatory environment unnecessarily hinder the development and implementation of products and services that could “empower Americans to make independent financial decisions and informed choices in the marketplace, save for retirement, and build individual wealth,” “foster economic growth and vibrant financial markets,” and “enable American companies to be competitive with foreign firms in domestic and foreign markets.” Addressing these regulatory frictions would further the principles to “make regulation efficient, effective, and appropriately tailored,” and “rationalize the Federal financial regulatory framework.”

This White Paper covers general principles and topic areas related to innovation and fintech where the Securities Industry and Financial Markets Association (“**SIFMA**”) <sup>1</sup> membership has recommendations that it believes, if adopted, would promote innovation and consumer choice as well as spur job creation and economic growth while protecting both consumers and the integrity of the financial system.

---

<sup>1</sup> SIFMA is the voice of the U.S. securities industry. We represent the broker-dealers, banks and asset managers whose nearly 1 million employees provide access to the capital markets, raising over \$2.5 trillion for businesses and municipalities in the U.S., serving clients with over \$20 trillion in assets and managing more than \$67 trillion in assets for individual and institutional clients including mutual funds and retirement plans. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit [www.sifma.org](http://www.sifma.org).

## II. GENERAL PRINCIPLES AND EXECUTIVE SUMMARY

## General Principles and Executive Summary

---

The financial services industry is rapidly evolving in new and exciting ways, and financial institutions will use innovation to better serve and protect customers, improve the security of the fintech ecosystem, compete with other providers of financial services (both bank and non-bank), and enhance compliance with regulations. Regulators should encourage responsible innovation by financial institutions that protects consumers and guards against abusive or unsafe practices. To foster such innovation, regulators will need to rethink how existing concepts and principles apply to financial services delivered through new technologies and acknowledge that innovation does not pose a material risk to safety and soundness if properly managed and overseen.

While all innovation carries uncertainty and some risk, these risks are dwarfed by the broader threat to the competitiveness and stability of the U.S. financial system if financial institutions do not keep pace with international competition, changing technology, and customer demand. The strength of the U.S. financial system depends upon a regulatory system that balances the need to mitigate the risks of innovation with the tremendous opportunities that innovation can bring to the U.S. economy.

We believe that the following general principles should guide regulators in their efforts to reform financial regulation to promote innovation:

- Innovation in the financial industry is essential to its success and must be encouraged. Regulators should therefore ensure flexibility of the regulatory framework to encourage and support innovation without compromising consumer protection or the safety and soundness of the financial system.
- Regulations and supervisory practices should be principles-based and technology-agnostic to accommodate future innovation without requiring regulatory reforms each time that new technology is created. New regulations are not necessary in many cases.
- Innovation and customer protection are optimized when regulation is based on function or activity (rather than the type of entity or regulated status) and applied in a consistent manner. This requires a rethinking of our current entity-based regulatory framework in addition to coordination and commitment among regulators with different jurisdictional interests at both the federal and state levels.
- Regulatory policy should encourage collaboration among federal and state regulators, financial institutions, and technology companies—in each case both domestically and internationally—to maximize knowledge-sharing.

- Regulators should have advanced technological expertise to evaluate changing technologies.

With these general principles in mind, regulators should, through regulation as well as through supervisory practices,<sup>1</sup> encourage responsible innovation by financial institutions while at the same time ensuring consumer protection. To do so, regulators should use appropriate tools to protect consumers from abusive or unsafe practices while taking care not to frustrate responsible innovation through the misguided application of outmoded concepts and principles. When properly calibrated, regulation can better promote innovation and allow financial institutions to effectively and competitively implement technology that benefits and is embraced by consumers.

Accordingly, we make specific recommendations to Treasury as it formulates its pending report.

**Recommendation One:** The Financial Stability Oversight Council (“**FSOC**” or the “**Council**”) should create a special subcommittee of appropriate members with the mandate to drive pro-innovation practices at the financial agencies (an “**FSOC Fintech Subcommittee**”). Once established, the FSOC Fintech Subcommittee should:

- Create a framework for activities-based fintech regulation and assist the agencies in adopting that framework.
- Develop a regulatory sandbox to help financial institutions and fintech companies engage in responsible innovation.
- Take steps to ensure that the agencies enhance their technical capacity and increase their understanding of new technologies
- Build on Treasury’s existing efforts to harmonize federal and state regulatory standards with respect to vendor risk and collaborate with financial institutions to understand the risks that such relationships present and the ways in which financial institutions oversee those relationships.
- Identify outmoded regulations, make recommendations for the agencies to modify or rescind those regulations where appropriate and, if necessary, recommend legislative changes to current laws that inhibit responsible innovation.
- Create a framework for the agencies to issue appropriate and consistent no-action letters or interpretive relief.

---

<sup>1</sup> See Federal Financial Institutions Examination Council (“**FFIEC**”), Joint Report to Congress: Economic Growth and Regulatory Paperwork Reduction Act 82 Fed. Reg. 15900, 15903 (Mar. 30, 2017) ([link](#)) [hereinafter FFIEC Joint Report] (“The agencies are aware that regulatory burden does not emanate only from statutes and regulations, but often comes from processes and procedures related to examinations and supervisory oversight.”).

- Encourage coordination between state regulators and facilitate the establishment of uniform, national data breach notification requirements.
- Facilitate international coordination on fintech issues and the adoption, with appropriate modifications, of international best practices in the fintech space.

**Recommendation Two:** Regulators should assure that all parties that have access to sensitive consumer information, including data aggregators adopt and follow appropriate minimum data access, data handling, and data security standards, and act in a safe and responsible way.

**Recommendation Three:** The federal banking agencies should revisit and modify as appropriate their current interpretations of certain banking statutes, including the meaning of control under the Bank Holding Company Act of 1956 (“**BHC Act**”) and the business of banking under the National Bank Act in order to ensure that such interpretations do not impede investments in fintech innovation.

**Recommendation Four:** The Securities and Exchange Commission (“**SEC**”) should reexamine rules that may unnecessarily inhibit the growth of both traditional and digital forms of advice and should revisit rules that govern how documents must be delivered.

**Recommendation Five:** To resolve the uncertainty created by the *Madden v. Midland Funding, LLC* decision and to assure the smooth functioning of our financial markets, the Administration should promote a legislative solution to the court challenges to the valid-when-made doctrine.

**Recommendation Six:** The agencies should foster the responsible adoption of distributed ledger technologies (“**DLT**”) by updating regulations that impede their use.

**Recommendation Seven:** In the field of cloud computing, the agencies should draw upon the expertise of industry groups and look wherever possible to harmonize standards across jurisdictions.

**Recommendation Eight:** The Administration should work to discourage other jurisdictions from adopting unreasonable data localization requirements.

**Recommendation Nine:** The agencies should facilitate the implementation of artificial intelligence tools that could facilitate compliance and should also support wider adoption of machine learning technologies.

### III. DISCUSSION OF RECOMMENDATIONS



## Recommendation One

---

### The FSOC should create an FSOC Fintech Subcommittee with the mandate to drive pro-innovation practices at the financial agencies.

As recognized by the Government Accountability Office (“GAO”), the current regulatory framework governing financial institutions is rigid and fragmented,<sup>1</sup> and this has particular implications for fintech.<sup>2</sup> The fragmented nature of our financial regulatory system has led to regulatory obstacles that have frustrated the adoption of new technologies which could provide greater convenience, lower costs, increased financial inclusion, faster services, and improved security.<sup>3</sup>

To avoid the regulatory fragmentation that pervades our financial system, to enhance collaboration<sup>4</sup> and to ensure consistency of application across financial regulators, the Administration should support and direct the creation of an FSOC Fintech Subcommittee with the mandate to drive pro-innovation practices at the financial agencies, including by developing a U.S. regulatory sandbox to help financial institutions and fintech companies engage in responsible innovation.

Once established, the FSOC Fintech Subcommittee should eliminate unnecessary regulatory barriers to fintech innovation, facilitate information sharing and coordination among its member agencies and among other federal and state agencies and thereby enhance the safety and soundness of the financial system in a number of areas<sup>5</sup> regarding policy development, rulemaking, examinations, and other matters. This would be entirely consistent with FSOC’s

---

<sup>1</sup> GAO, Financial Regulation: Complex and Fragmented Structure Could Be Streamlined to Improve Effectiveness (Feb. 2016) ([link](#)).

<sup>2</sup> GAO, Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight (Mar. 2018) ([link](#)) [hereinafter GAO Fintech Report] (“The U.S. regulatory structure poses challenges to fintech firms. With numerous regulators, fintech firms noted that identifying the applicable laws and how their activities will be regulated can be difficult.”).

<sup>3</sup> Id. at 13.

<sup>4</sup> See GAO Fintech Report at 48 (“Although a few fintech market participants and observers we interviewed told us that they thought regulatory collaboration on fintech was sufficient, the majority of market participants and observers we interviewed who commented on interagency collaboration said that it could generally be improved.”).

<sup>5</sup> The FSOC Fintech Subcommittee’s role in encouraging the states to coordinate on the elimination of barriers to innovation imposed by state regulators, including state banking supervisors and state securities commissioners, could be of particular importance. As the GAO noted recently, “complying with fragmented state licensing and reporting requirements can be expensive and time-consuming . . . fintech firms may spend a lot of time on state examinations because state exam requirements vary and numerous states may examine a fintech firm in 1 year. For example, staff from a state regulatory association said that states may examine fintech firms subject to coordinated multistate exams 2 or 3 times per year, and as many as 30 different state regulators per year may examine firms that are subject to state-by-state exams.” GAO Fintech Report at 45.

statutory mission.<sup>6</sup> At least one senior regulator has already signaled his support for FSOC playing this role.<sup>7</sup> We strongly support the goals noted by Commissioner Behnam, and agree that FSOC is best-placed to accomplish these goals, but we recognize that there may be other alternatives. For example, an interagency working group that includes relevant state regulatory representatives dedicated to fintech regulatory issues could undertake the FSOC Fintech Subcommittee work we have outlined in this White Paper.

An FSOC Fintech Subcommittee dedicated to creating a coordinated regulatory approach for fintech could leverage the United States' unique regulatory structure. The FSOC Fintech Subcommittee would bring together technically savvy staff from each agency and representatives from relevant state regulators in order to facilitate coordination between those agencies, financial institutions, and fintech companies to ensure a robust regulatory regime that encourages innovation, identifies risks and emerging threats, ascertains the overall impact of proposed regulatory recommendations and positions the United States as a global leader in fintech innovation. We offer the following specific recommendations to the FSOC Fintech Subcommittee.

#### A. The FSOC Fintech Subcommittee should create a framework for activities-based fintech regulation and assist the agencies in adopting that framework.

---

Banks, securities firms, and money transmitters all engage in the transmission of money at the request of consumers, yet banks must submit to the full panoply of capital, liquidity, and prudential standards applicable to banks, securities firms have their own regulatory requirements, and non-bank and non-securities firm money transmitters must comply with the multitude of state money transmitter statutes. There are differing costs and burdens associated with each regulatory structure. The same is true for lending services, advisory services, and a multitude of other activities that both financial services firms and other entities provide to their consumers.

---

<sup>6</sup> See 12 U.S.C. § 5322 (2)(D)-(E); (M). (“The Council shall . . . monitor domestic and international financial regulatory proposals and developments, including insurance and accounting issues, and to advise Congress and make recommendations in such areas that will enhance the integrity, efficiency, competitiveness, and stability of the U.S. financial markets . . . facilitate information sharing and coordination among the member agencies and other Federal and State agencies regarding domestic financial services policy development, rulemaking, examinations, reporting requirements, enforcement actions . . . provide a forum for—(i) discussion and analysis of emerging market developments and financial regulatory issues; and (ii) resolution of jurisdictional disputes among the members of the Council.”).

<sup>7</sup> Rostin Behnam, Commissioner, Commodity Futures Trading Commission (“CFTC”), Remarks at the FIA Boca 2018 International Futures Industry 43rd Annual Conference, Boca Raton, Florida (Mar. 15, 2018) ([link](#)) [hereinafter Behnam Remarks] (“[T]he authority granted to the FSOC in Dodd-Frank is the perfect means to execute the following: (i) convening member bodies; (ii) foster extensive discussions regarding, among other things, oversight responsibility, jurisdiction, and general policy approach of each regulatory body; (iii) engaging stakeholders, market participants, public interest groups, and foreign regulators; and (iv) delivering a detailed roadmap of policy findings and possibly legislative proposals to the Congress.”).

Consider, for example, the Federal Deposit Insurance Corporation (“**FDIC**”) 2016 Examination Guidance for Third-Party Lending.<sup>8</sup> This guidance broadly states that FDIC-regulated institutions that “engage in new or significant lending activities through third parties will generally receive increased supervisory attention.”<sup>9</sup> No explicit guidance has been provided by the FDIC, however, as to the standard of care required from banks when they partner with non-bank companies, such as fintech companies, to provide liquidity by purchasing loans, and, whatever the FDIC’s expectations may be, they do not apply equally to institutions engaging in similar activities but not subject to regulation by the FDIC.<sup>10</sup>

Inconsistencies such as these can do real harm to consumers. By regulating firms based on charter and not by activities, some firms are, merely by virtue of their charter, subject to extensive requirements while others escape similar regulatory scrutiny, potentially to the detriment of consumers.

As noted recently by Counselor to the Treasury Secretary Craig Phillips, fintech company innovation should be encouraged but regulators should seek to reduce regulatory asymmetries between fintech companies and regulated financial institutions.<sup>11</sup> A reduction in these regulatory asymmetries would even the playing field and address consumer protection concerns. It would be entirely appropriate for the FSOC Fintech Subcommittee to focus on assuring that regulation appropriately addresses the real risks associated with any particular financial activity, and that all participants are subject to appropriate minimum standards that adequately address the risks of that activity.

For example, regulators should ensure that providers of a financial service that raises risks comparable to those that the Bank Secrecy Act (“**BSA**”) and anti-money laundering (“**AML**”) laws seek to combat should be subject to appropriate minimum BSA/AML requirements that are tailored to the provision of that service. Other, non-exclusive areas where appropriate, activity-based minimum standards should be required include know-your-customer (“**KYC**”) rules, data privacy and security requirements, and restrictions on unfair trade practices. Further, these appropriate, activity-based minimum standards should also apply to international participants doing business in the United States.

---

<sup>8</sup> FDIC, Examination Guidance for Third-Party Lending (July 29, 2016) ([link](#)).

<sup>9</sup> Id. at 1.

<sup>10</sup> As explained below, the core concern of our membership may be addressed by moving to a system of activities-based regulation. In the interim, however, the FDIC should provide explicit guidance on the standard of care that banks need to use when partnering with non-bank companies to provide liquidity by purchasing loans.

<sup>11</sup> John Heltman, Treasury report to weigh in on fintech regulation, American Banker (Mar. 5, 2018) ([link](#)).

## B. The FSOC Fintech Subcommittee should develop a regulatory sandbox to help financial institutions and fintech companies engage in responsible innovation.

---

Banks may only engage in bank-permissible activities as determined by their regulators. Bank holding companies (“**BHCs**”) are constrained by the limitations of the BHC Act. Other financial institutions face similar regulatory constraints. Moving past legacy activity parameters requires evaluation by the agencies, including a review of statutory guidelines, past precedents, potential safety and soundness concerns, and the precedential impact of any decision. This process can be slow and expensive, and, most importantly, it can frustrate a financial institution’s ability to compete with less regulated entities by limiting that institution’s ability to improve the customer experience and deliver innovative products and services. Nowhere are these limitations more apparent than in the rapidly changing world of technology.

The FSOC Fintech Subcommittee should foster the creation of a single U.S. regulatory “sandbox” — a space where a company may experiment by making its latest innovations available to a limited number of participants while providing regulators with appropriate visibility into the experiment. A sandbox should have clear rules, subject to notice and comment, that all participants must follow, and all relevant regulators should participate and coordinate to promote regulatory certainty, efficiency, and shared learning.

While certainly each agency could create its own sandbox, individual sandboxes are inefficient and run the risk of adverse or precipitous action by other agencies that may have jurisdiction over some aspect of the activity. Individual sandboxes would exacerbate the very fragmentation that we recommend that Treasury take steps to address. Further, many states are considering their own laws and regulations related to fintech innovations. Thus, we believe that the FSOC Fintech Subcommittee would play a critical role in the creation of a single sandbox cutting across federal and state regulatory jurisdictions.

The creation of such a sandbox would not require new or additional regulation; rather, it would require a single regulatory will to align and coordinate, in a controlled and regulated environment, the full array of regulations on experimental activities that pose no real dangers to the public or the financial system.

With the FSOC Fintech Subcommittee’s sandbox granting relevant regulators appropriate visibility into their experiments, companies can test new ideas and products on a limited number of participants for a limited period of time, gain experience and feedback, and adapt the product or service accordingly. Consistent with the sandbox approach, the regulators should be in a position to give early and frequent feedback to the experimenter. The relevant regulators can assure safety, soundness, and consumer protection, and quickly halt activities that raise particular concerns. Where the normal regulatory evaluation of a project typically occurs when a pilot or

prototype has been completed or during the exam cycle, if the agencies are properly and actively involved in the sandbox, they can provide more real-time guidance as to issues, obstacles, and challenges. Such early feedback can allow all participants to tailor their activities in a way that optimizes the deployment of time, energy, and capital.

Indeed, conducting such activities within a framework where there is appropriate regulatory oversight would be a substantial improvement over our current system where some technology companies occasionally appear focused on gaining market share rather than worrying about compliance obligations. The FSOC Fintech Subcommittee should establish appropriate minimum standards that must be met for firms to participate in the sandbox. These appropriate minimum standards, if properly tailored, could extend the scope of the existing regulatory perimeter to encompass those organizations that are not currently adequately regulated and supervised to ensure the protection of consumers and the safety and soundness of the financial system according to consistently applied activities-based regulation discussed above.

The sandbox could, for example, be used to enable financial services companies to provide broader—yet still responsible—access to credit in a more efficient manner. Board of Governors of the Federal Reserve System (“**Federal Reserve**”) Vice Chair for Supervision Quarles supported this notion when recently stating that “online origination platforms and more sophisticated algorithms may enable credit to be underwritten and delivered in a manner that is still prudent but with greater efficiency, convenience, and lower processing costs.”<sup>12</sup> Currently, there is tremendous reliance on credit bureau variables, such as a consumer’s FICO score, when determining whether to provide a consumer with credit. Allowing financial services companies to test whether alternate data sources could be used when determining to provide a consumer with credit, in addition to a consumer’s FICO score, could be beneficial to growing the overall economy. Specifically, the use of alternative data could expand consumers’ access to credit in order to better determine the risk profiles of potential consumers. New and innovative data sources would enable financial institutions to extend credit to a broader population (such as those with a “thin” credit file, i.e., those who are young or new to obtaining credit) and to offer better pricing for the existing population.

### C. The FSOC Fintech Subcommittee should take steps to ensure that the agencies enhance their technical capacity and increase their understanding of new technologies.

---

We applaud the efforts of the financial regulators to encourage innovation. The Office of the Comptroller of the Currency (“OCC”) has established an Office of Innovation, and has appointed a Chief Innovation Officer. It has invited banking and technology companies to visit

---

<sup>12</sup> Randal K. Quarles, Vice Chair for Supervision, Federal Reserve, The Roles of Consumer Protection and Small Business Access to Credit in Financial Inclusion (Mar. 26, 2018) ([link](#)).

and exchange information, with the hope of educating financial institutions, technology companies, and the OCC on developments and fostering responsible innovation. The Federal Reserve and various Federal Reserve Banks have likewise taken steps to encourage financial services and technology firms to bring ideas and explore how financial services companies might better use technology and how technology firms can navigate the regulatory environment.<sup>13</sup> The CFTC has established LabCFTC with the goals of promoting “responsible FinTech innovation to improve the quality, resiliency, and competitiveness of our markets;” and accelerating “CFTC engagement with FinTech and RegTech solutions that may enable the CFTC to carry out its mission responsibilities more effectively and efficiently.”<sup>14</sup>

While these are useful steps, more should be done given our complex and fragmented regulatory environment. Bank chartering authority is dispersed among the OCC and the states, authority to provide deposit insurance is vested with the FDIC, and holding company regulation and access to essential parts of our payments system is under the control of the Federal Reserve. Thus, discussions with a single agency are insufficient to obtain useful insight and guidance. The SEC, the CFTC, and the Consumer Financial Protection Bureau (“CFPB”) also have roles in various financial products, and, further still, state securities and insurance regulators have additional oversight over the asset management and insurance sectors which could create conflicts between federal and state regulations addressing financial services regulation. This additional regulatory fragmentation makes the need for a more coordinated and comprehensive approach to enhancing technical capacity even more apparent. The optimal outcome is a shared, consistent, activities-based approach across regulators.

The FSOC Fintech Subcommittee should insist that key representatives from applicable regulators participate in the workings of the FSOC Fintech Subcommittee. Knowledge gained and decisions reached by the FSOC Fintech Subcommittee should be shared with the individual agencies and used to drive consistency in policy across those agencies. As the Basel Committee on Banking Supervision has noted, supervisory staff at each agency must have sufficient familiarity with emerging fintech issues to be able to understand and implement the FSOC Fintech Subcommittee’s recommendations.<sup>15</sup> For example, it would be useful for each agency to establish a central point of contact for fintech issues with sufficient authority and stature to ensure that the FSOC Fintech Subcommittee’s recommendations are put into practice. The central point of contact should have sufficient technical knowledge to answer questions posed by

<sup>13</sup> See GAO Fintech Report at 64 (providing an overview and comparison of fintech knowledge-building initiatives at the federal financial regulators).

<sup>14</sup> See U.S. Commodity Futures Trading Commission, LabCFTC Overview ([link](#)).

<sup>15</sup> See Basel Committee on Banking Supervision, Sound Practices: Implications of fintech developments for banks and bank supervisors at 34 (Feb. 2018) ([link](#)) (“Safety and soundness could be enhanced by bank supervisors assessing their current staffing and training programmes to ensure that the knowledge, skills and tools of their staff remain relevant and effective in supervising the risks of new technologies and innovative business models. Supervisors may need to consider the addition of staff with specialised skills to complement existing expertise.”).



firms under the relevant agency's oversight. Furthermore, each agency should ensure that its onsite supervisory staff are aligned with its views and policies consistent with the views and policies expressed by the FSOC Fintech Subcommittee.

**D. The FSOC Fintech Subcommittee should build on Treasury's existing efforts to harmonize federal and state regulatory standards with respect to vendor risk and should collaborate with financial institutions to understand the risks that such relationships present and the ways in which financial institutions oversee those relationships.**

---

Financial regulators define and enforce requirements as to how financial institutions should manage the risks associated with third party relationships.<sup>16</sup> In order to protect their assets, employees, and clients, and to satisfy regulatory requirements, financial institutions have established internal programs to manage risks associated with third parties and assessment protocols to ensure that third parties can manage those risks.

Financial institutions commonly segment third parties into tiers, based on the complexity and risk levels associated with each relationship. Each third party carries a variety of potential risks (e.g., cybersecurity, operational, financial, performance). The depth and frequency by which financial institutions assess third parties is commensurate with the risk tier. In addition to established suppliers, there are always new companies seeking to offer new services, solutions, and technologies to the financial services industry.

Regulatory requirements related to third party risk management vary between agencies. Inconsistencies in how regulators interpret and enforce that guidance create a bureaucratic burden that distracts financial institutions from core risk management activities. Companies offering new services, solutions or technologies find it difficult to comprehend and comply with the complex oversight requirements of financial institutions. This lack of clarity creates a barrier to entry that could stifle innovation and reduce competitiveness.<sup>17</sup>

Building on processes that are already in place, including those recommendations that industry groups have already submitted to Treasury, the FSOC Fintech Subcommittee should work with financial institutions and their regulators to harmonize vendor risk oversight requirements. As

---

<sup>16</sup> For example, the OCC has issued guidance regarding third-party vendor engagement with national banks. See OCC Bulletin 2013-29, Third-Party Relationships: Risk Management Guidance (Oct. 30, 2013) ([link](#)); OCC Bulletin 2017-21, Frequently Asked Questions to Supplement OCC Bulletin 2013-29 (June 7, 2017) ([link](#)).

<sup>17</sup> See GAO Fintech Report at 59 ("Banks, fintech firms, and market observers we interviewed told us that bank due diligence can also lead to lengthy delays in establishing partnerships, which can put fintech firms at risk of going out of business if they do not have sufficient funding and are not able to access new customers through a bank partner.").

part of this effort, financial institutions and regulators should develop, through notice and comment, educational guidance that for companies that are positioning themselves to become suppliers to the financial sector. The FSOC Fintech Subcommittee should take in active role in promoting the guidance and in addressing the industry groups' recommendations.

**E. The FSOC Fintech Subcommittee should identify outmoded regulations, make recommendations for the agencies to modify or rescind those regulations where appropriate and, if necessary, recommend legislative changes to current laws that inhibit responsible innovation.**

---

Many existing regulations and supervisory practices were developed decades ago and these regulations and practices developed in a different era have not kept up with the evolution and pace of technological change. New technologies are unlikely to fit squarely into old rules. Regulatory reforms are necessary to foster innovation while maintaining financial stability and consumer protection.

The FSOC Fintech Subcommittee should encourage the agencies to comprehensively review their regulations and supervisory practices, provide a public report with the results of that review, and eliminate or modify regulations and practices that are outdated. Such a review and update would benefit the agencies by improving the supervisory process as well as the financial institutions that they regulate by encouraging innovation and reducing costs.

We believe that the agencies should issue public statements that emphasize that pursuing innovation and adapting new technologies is critical to a competitive and well-functioning financial institution, that innovation has risks but these risks can be appropriately managed and mitigated, and that examiners should in general provide institutions with the freedom to test and pilot new products.

The following subsections contain specific recommendations regarding regulations, guidance and supervisory practices that we believe can be eliminated or updated to foster innovation, reduce costs and improve efficiency without sacrificing financial stability or consumer protection.

***(i) EGRPRA and Regulatory Review***

---

Under the Economic Growth and Regulatory Paperwork Reduction Act of 1996 (“**EGRPRA**”), the FFIEC, OCC, FDIC, and Federal Reserve are directed to conduct a joint review of their regulations every ten years and consider whether any of those regulations are outdated,



unnecessary, or unduly burdensome.<sup>18</sup> Given the current pace of technology, a once-a-decade review is far from sufficient.

The FSOC Fintech Subcommittee should, even in the absence of Congressional revisions to EGRPRA,<sup>19</sup> encourage all of the agencies to conduct an assessment of existing regulations, guidance, and supervisory practices directly or indirectly affecting financial innovation—at a minimum, every three years, or more often as needed—and update or eliminate outdated regulations, guidance, and supervisory practices to foster innovation, reduce costs and improve efficiency.

### *(ii) New Product Guidance and Supervision*

---

Currently, the agencies often hinder financial innovation by not providing any feedback until the end of the product or activity design process or by scrutinizing the details of an institution's new products or activities, requiring constant communication with the agency before the activity is tested or launched rather than relying on the institution's risk management function to identify and mitigate risks appropriately. For example, the OCC's guidance on new products focuses only on the risks of innovating (without considering the costs and risks of *not* innovating), suggests full-scale compliance management processes even for small pilot tests affecting few consumers, and adds an extra requirement not codified in law that national banks should discuss every new activity with examiners before launch, generating examiner scrutiny and significantly slowing down innovation.<sup>20</sup> Regulatory guidance and supervisory practices in other areas, such as vendor risk management,<sup>21</sup> should also take into account the benefits of innovation and encourage beneficial relationships with fintech companies.

We believe the establishment of an FSOC Fintech Subcommittee could alleviate many of these concerns by serving as a single, coordinated point of engagement for new product and services development. The FSOC Fintech Subcommittee should facilitate discussion between the agencies and companies that are exploring offering new products and should provide a forum for the relevant agencies to offer early feedback to that company. The FSOC Fintech Subcommittee should also recommend that the agencies' new product guidance and supervision focuses not only on the risks of innovating, but also on the potential benefits and should encourage the OCC

---

<sup>18</sup> FFIEC Joint Report at 3.

<sup>19</sup> The House of Representatives recently passed a bill that would add the CFPB to the ranks of those regulators who must conduct the EGRPRA review. H.R. 4607, Comprehensive Regulatory Review Act, (115th Cong., 2d Sess., 2018) ([link](#)). H.R. 4607 would also require that such review be conducted every seven years, rather than every ten years.

<sup>20</sup> OCC Bulletin 2017-43, New, Modified, or Expanded Bank Products and Services (Oct. 20, 2017) ([link](#)) ("Management should discuss plans with its OCC portfolio manager, examiner-in-charge, or supervisory office before developing and implementing new activities...").

<sup>21</sup> See Recommendation One – F.

to revisit its guidance on new products. The agencies must also ensure that supervisory teams cease overly conservative practices as part of the examination process.

### *(iii) Laws Related to the Intersection of Technology and Consumer Protection*

---

The Fair Debt Collection Practices Act (“**FDCPA**”), enacted in 1977, does not specifically bar forms of communication such as email and text messaging. Even so, continued uncertainty surrounding the use of electronic means to communicate with consumers constrains the current use of these technologies. Most problematic is the FDCPA requirement that debt collectors, in connection with the collection of any debt, do not communicate with any person other than the consumer or certain other limited third parties (e.g., the consumer’s attorney).<sup>22</sup> Because consumers may share email addresses or may have their email monitored (e.g., by an employer), regulated firms may be deterred from sending email communications to consumers—even if consumers do most of their communicating by email and would likely prefer that method of communication.

Similarly, the Telephone Consumer Protection Act (“**TCPA**”), enacted in 1991, limits the use of modern communication technology often requested by consumers, such as text messages, by requiring consumer consent before communications may be sent to the consumer. Text messaging is a particularly important means of communication for low-income consumers, yet TCPA compliance costs and litigation risk have deterred some financial institutions from widespread use of text messages as a means of communication.

We strongly support the principle behind the FDCPA that consumers should be shielded from abusive, deceptive and unfair debt collection practices, but we just as strongly support an updated FDCPA rulemaking to clarify an older law for modern times. The CFPB should provide a reasonably tailored safe harbor under the FDCPA to permit communication with consumers by email or another digital means when the consumer has provided an email address or other means of contact for that purpose. This would by no means undermine or be inconsistent with the purpose of the FDCPA and would be consistent with how modern-day consumers communicate.

Similarly, the members of the FSOC Fintech Subcommittee should work with and assist the FCC to update and modernize the FCC’s TCPA regulations to reflect consumer use of text messages and other electronic means of communication. The D.C. Circuit’s recent decision in *ACA International v. FCC*<sup>23</sup> will require the FCC to revisit its TCPA regulations in any event, and presents an excellent opportunity for a broader reconsideration. Most importantly, such a reconsideration should provide clarity on which calling systems constitute automatic dialing

---

<sup>22</sup> 15 U.S.C. § 1692c.

<sup>23</sup> No. 15-1211 (D.C. Cir.) (Mar. 16, 2018) ([link](#)).

systems for purposes of the TCPA. Further, the FCC’s revised regulations should establish clear standards for how to deal with calls to numbers that have been reassigned and should provide clear exemptions for push notifications and other messaging platforms like iMessage that do not use telephony rails.

#### *(iv) E-SIGN Act and UETA*

---

The Electronic Signatures in Global and National Commerce Act (“**E-SIGN Act**”), adopted in 2000, permits the use of electronic records to satisfy certain requirements that information be provided in writing and is broadly applicable to a wide range of financial products and services. While the E-SIGN Act was a significant step forward for its time, use of electronic records is subject to various potentially cumbersome requirements, particularly in the modern context.

The E-SIGN Act’s most significant barrier to innovation is its requirement that a consumer must consent to receive disclosures electronically in a manner that reasonably demonstrates that he or she can access information in the electronic form that it will be provided. This reasonable demonstration requirement is straightforward when consent is given in an online or mobile device environment, but is less clear when the consent is given in person, by phone or by paper. This requirement may have made sense when the statute was enacted 18 years ago, but makes much less sense today. Given the ubiquity of access to electronic delivery methods, the consumer’s consent should be sufficient without an accompanying demonstration. Alternatively, regulators should provide clarifying guidance that demonstration could also be satisfied by confirmation/statement by the consumer or requesting changes such as making the timing of when the demonstration could occur more flexible.

In addition, financial institutions seeking to comply with the E-SIGN Act must, prior to obtaining a consumer’s consent to receive documents electronically, provide the consumer with a statement of the hardware and software requirements for access to and retention of electronic records. This provision no longer makes sense because so many different platforms work for accessing and storing information and the ubiquity and rapid obsolescence of the latest hardware and software undercut the usefulness of this disclosure.

The FSOC Fintech Subcommittee should review the requirements of the E-SIGN Act to determine how its provisions can be better tailored to the modern context. In particular, the FSOC Fintech Subcommittee should determine the best way to address and better tailor the E-SIGN Act’s outdated “reasonable demonstration” requirement and should consider eliminating or modifying the E-SIGN Act’s requirement to explain the hardware and software requirements to access and store information.

Following its review, the FSOC Fintech Subcommittee should recommend regulatory clarifications through guidance where possible, but Congressional action to make the above modifications may ultimately be required.

Relatedly, the FSOC Fintech Subcommittee should review and make recommendations for how the Uniform Electronic Transactions Act (“**UETA**”), first promulgated by the Uniform Law Commission in 1999, could be modified to better account for new technologies. UETA is meant to ensure that electronic signatures are not denied legal effect or enforceability solely because of their electronic form and has been adopted by nearly every state. Given that UETA is now nearly twenty years old, however, the various state laws that adopted the provisions of UETA no longer properly reflect modern technology. For example, UETA’s definition of electronic signatures does not include blockchain-based records. UETA should be updated and modernized to reflect new technologies, and its revised form should be quickly adopted by the states. To the extent these state-level revisions to UETA would create tension with the E-SIGN Act,<sup>24</sup> the E-SIGN Act should be modified by Congress to avoid such a result.

### *(v) Digital Books and Records*

---

Broker-dealers’ digital books and records that are required to be stored by the SEC must be stored in a non-rewritable, non-erasable format such as the “write once, read many” (“**WORM**”) format.<sup>25</sup> Compliance with the WORM requirement, which was adopted in 1997, is burdensome and outdated. For example:<sup>26</sup>

- Records stored in WORM cannot effectively be used for business continuity planning or cybersecurity defenses because the nature of these records makes such use of this technology impractical and, in some cases, impossible. Data stored in WORM is essentially a static snapshot of a record that is locked and secured from any manipulation or deletion, as opposed to a complete system that could be used to stand up a production system during or following a disaster event.
- In simple terms, archiving dynamic data in WORM storage requires firms to create static documents or reports that are comprised of data generated by and from dynamic and interconnected computer systems. This process of compilation—which occurs solely information for WORM storage purposes—is costly, time-consuming, and generates information with less utility. Further, the stored document comprises a snapshot of the

<sup>24</sup> The E-SIGN Act preempts certain state laws that modify, limit or supersede its provisions, with exceptions for, as relevant here, those state laws that constitute an enactment or adoption of UETA.

<sup>25</sup> 17 C.F.R. § 240.17a-4(f).

<sup>26</sup> For more detail on these burdens *see* SIFMA, Financial Services Roundtable, Futures Industry Association, International Swaps and Derivatives Association, and Financial Services Institute, Petition for Rulemaking to Amend Exchange Act Rule 17a-4(f) (Nov. 14, 2017) ([link](#)).

actual record at a specific point in time, and it is not intrinsically useful in recreating the record or demonstrating the dynamic nature of the communications in question.

- WORM storage requirements are hindering innovation in the brokerage industry due to the inordinate amount of resources allocated to the maintenance of these systems and the implementation challenges for new systems. Firms are required to allocate substantial capital to WORM storage technologies that serve a very narrow purpose. These WORM storage expenditures could otherwise be dedicated to solving practical technology issues facing the industry.

Because neither the banking regulators nor the CFTC require that records be stored in WORM format, the disparity between recordkeeping standards put in place by the SEC and those put in place by other regulators makes implementing new technology unnecessarily challenging.

The SEC should amend Rule 17a-4(f) to remove WORM storage requirements and implement electronic recordkeeping standards that employ principles-based and technology-agnostic requirements such as those applicable to investment advisers, investment companies, transfer agents, and now swap dealers and futures commission merchants.<sup>27</sup> As an example for the SEC to look to, the CFTC recently eliminated the WORM requirement from its rules, choosing to modernize its recordkeeping requirement by introducing a principles-based approach, rather than prescriptively requiring that digital books and records be stored in WORM format.

The FSOC Fintech Subcommittee should ensure that digital recordkeeping requirements are technology neutral and harmonized in order to increase efficiency and result in significant cost savings, particularly for smaller firms. Under a principles-based, non-prescriptive approach to recordkeeping, financial institutions could adopt DLT, such as blockchain, to fulfill regulatory requirements, thereby reducing costs. Having consistent recordkeeping standards across various types of financial institutions will further enhance broker-dealers' abilities to efficiently comply with recordkeeping rules by using the available technology that best fits their business models.

#### F. The FSOC Fintech Subcommittee should create a framework for the agencies to issue appropriate and consistent no-action letters or interpretive relief.

---

No-action and interpretive letters are appropriate and valuable tools for the agencies to use to address concerns from regulated entities and to take into account developments—including developments related to technology—that may not have been anticipated at the time that a given law was enacted or at the time that a rule was promulgated. The benefit of these no-action and interpretive letters is limited, however, because many financial institutions are regulated by more

<sup>27</sup> See *id.* at 9 for proposed rule text that our membership has suggested previously.

than one agency, and therefore have no assurance that a given agency will necessarily agree with another agency's no-action or interpretive position. For example, though the CFPB's no-action letter policy covers banks, a CFPB no-action determination is of little use if the bank that has requested the no-action letter cannot be sure that the OCC, Federal Reserve, FDIC, Federal Trade Commission or other applicable regulators will take a similar position.

The FSOC Fintech Subcommittee, drawing on its statutory authority to enhance coordination between the agencies, should take on a coordinating role with respect to innovation-related no-action applications and requests for other interpretive guidance. If the FSOC Fintech Subcommittee determines that no-action relief is warranted, the FSOC Fintech Subcommittee should encourage each agency to issue appropriate no-action relief or to take other necessary steps to ensure that the relief granted by a no-action letter issued by one agency is applied consistently by each other relevant agency.

### G. The FSOC Fintech Subcommittee should encourage coordination between state regulators and facilitate the establishment of uniform, national data breach notification requirements.

---

Regulators should recognize that state-by-state data breach statutes often present inconsistent standards and obligations for financial institutions, requiring firms to devote already scarce resources to complying with these differing standards and obligations that could be better spent on innovation. With different standards for each state—for example, varying types of client notices based on a customer's residence—it remains difficult and costly for financial institutions to adapt to multiple and regularly changing standards while working to address these same issues in the face of emerging technologies and new products offered to clients. Treasury has previously recommended that states adopt a uniform regulation for insurers regarding data breach notification, and has further recommended that, if the states do not adopt a uniform standard, Congress should pass a law setting forth data breach notification requirements for insurers.<sup>28</sup>

Treasury's recommendation that states adopt a uniform data breach notification standard for insurers is sensible,<sup>29</sup> but it should be broadened and reissued to account for all institutions, not only insurers. Standardization for data incidents would allow the industry to focus resources on a single approach for communicating with clients. A single standard would also promote

<sup>28</sup> U.S. Department of the Treasury, A Financial System That Creates Economic Opportunities: Asset Management and Insurance at 117-18 (Oct. 2017) ([link](#)).

<sup>29</sup> While this White Paper strongly endorses a uniform standard, it does not explicitly support Treasury's specific recommendation for all states to adopt the NAIC cybersecurity model law. While the NAIC cybersecurity model law contains some appropriate security standards, other elements of the model law are uniquely burdensome. The model law also fails to provide an exclusive standard for any particular state.

awareness through a single set of rules with a common vocabulary. Customers would know what to expect to receive from their financial institution in the event of a data incident and how best to take self-help steps for additional protection.

#### H. The FSOC Fintech Subcommittee should facilitate international coordination on fintech issues and the adoption, with appropriate modifications, of international best practices in the fintech space.

---

President Trump’s Core Principles for Regulating the United States Financial System embrace the idea that U.S. companies should be competitive with non-U.S. firms in domestic and foreign markets and recognize that properly tailored financial regulation plays a key role in fostering an environment in which U.S. companies can effectively compete. The United States is lagging behind its international peers in its approach to fintech regulation, due in part to the fragmented nature of the U.S. financial regulatory system.

Attached as Appendix A to this White Paper is a chart highlighting some of the international approaches to fintech regulation. We recognize that the United States is fundamentally different from these other countries, not only in the breadth and depth of our economy, but in the unique regulatory structure developed here. We do not advocate for the wholesale adoption of non-U.S. regulatory policies without in-depth review.<sup>30</sup> At the same time, however, examination and understanding of best practices could be a critical step forward in assuring that the United States remains a leader in the global financial system.

The FSOC Fintech Subcommittee should review practices adopted by non-U.S. regulators, consider which practices best align with the needs of U.S. institutions, and work to create new U.S. practices that are primarily focused on market needs and competitiveness. In this way, the FSOC Fintech Subcommittee could enable the United States to become a world leader in fintech innovation.

By reviewing methods used by international regimes and, where appropriate, adapting them to the U.S. context, Treasury and the FSOC Fintech Subcommittee can ensure that U.S. agencies allow U.S. financial institutions to remain competitive while ensuring that the goals of safety and soundness are adequately addressed.<sup>31</sup>

---

<sup>30</sup> See GAO Fintech Report at 59 (“However, some [non-U.S.] initiatives may not be appropriate for the U.S. regulatory structure. For example, adopting certain initiatives could raise concerns about U.S. agencies picking winners, in which firms that participate in these programs may be better positioned to succeed than other firms. Further, particular initiatives may not align with agencies’ legal authorities or missions.”).

<sup>31</sup> For example, the FSOC Fintech Subcommittee could consider implementing a scorecard system similar to what the European Commission has done with their European Innovation Scoreboard that measures, among other things, the supervisory burden for an institution offering new financial products or engaging in new activities.



## Recommendation Two

---

Regulators should assure that all parties that have access to sensitive consumer information, including data aggregators adopt and follow appropriate minimum data access, data handling, and data security standards, and act in a safe and responsible way.<sup>32</sup>

We strongly support the concept that consumers should have the right to access and use their personal financial data as they wish.<sup>33</sup> We believe, however, that any party that obtains, holds or uses that data must be held to appropriately tailored minimum data and security standards like those followed by regulated financial institutions that undertake the same activities. Any party that obtains, holds or uses data must also take full responsibility for any data they receive and provide to others. Consumers also deserve clear and conspicuous explanations of how third parties will access and use their financial account data,<sup>34</sup> and clients should be required to consent affirmatively to this activity before it begins. These minimum standards are necessary in order to protect consumer interests, and, ultimately, these should be specific obligations limiting the use of consumer data and safeguarding the privacy and integrity of such information. Importantly, the minimum standards must include clear regulatory oversight and accountability as well as liability for the failure to abide by those standards.

First and foremost, the agencies should, through notice and comment, provide specific guidance that third parties and others in the data-access chain are “financial institutions” subject to the well-established Gramm-Leach-Bliley Act (“**GLBA**”) data security standards.<sup>35</sup> Without this guidance there is no mechanism to assure that the aggregators and other participants in the fintech ecosystem are in compliance with such requirements or, equally importantly, that they have the financial capacity to meet corresponding liabilities should they fail to do so.<sup>36</sup>

---

<sup>32</sup> With respect to several of the recommendations that follow, the FSOC Fintech Subcommittee may be able to assist, but we discuss these issues separately from the FSOC Fintech Subcommittee-specific recommendations above due to the importance of these issues to our membership and to the financial system as a whole.

<sup>33</sup> In this respect, we view the release by the CFPB of non-binding principles for consumer-authorized financial data sharing and aggregation as a positive step. See Consumer Financial Protection Bureau, Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (Oct. 18, 2017) ([link](#)).

<sup>34</sup> See GAO Fintech Report at 27 (“Some data aggregators may hold consumer data without disclosing what rights consumers have to delete the data or prevent the data from being shared with other parties. A leak of these or other data held by fintech firms may expose characteristics that people view as sensitive.”).

<sup>35</sup> There should be no doubt that companies gathering and using customer financial data are “financial institutions” for the purposes of the privacy provisions found in Title V of GLBA. A financial institution is any person, the business of which is engaging in financial activities as defined in Section 4(k) of the BHC Act. Gathering and using such financial data is the essence of being a financial institution. Such guidance would not require Congressional action.

<sup>36</sup> As the CFPB’s Consumer Protection Principles for Data Aggregation recognize, “[p]arties responsible for unauthorized access” should be “held accountable for the consequences of such access.”



Next, the agencies should differentiate between the *use* of data, on the one hand, and the *aggregation* of data, on the other hand.

### A. Use of Data

---

Because consumer and system protection is not technology dependent, it is appropriate for financial regulators, consistent with the principles set out in this White Paper, to regulate the use of data without delay. Whenever data is used to enable or provide banking services (e.g., gathering of funds, lending money, making payments, transferring money, allocating investments), this use of data should be subject to separate authorization and be regulated based on the underlying activity and should be subject to minimum requirements already in place for those underlying activities—for instance, authorization protocols, cybersecurity standards and AML and KYC rules.<sup>37</sup>

### B. Data Aggregation

---

In contrast, when it comes to data aggregation, the financial services industry should be allowed to reach solutions without the imposition of formal regulations.<sup>38</sup> This does not mean, however, that Treasury and the financial regulators have no role to play. As the GAO noted recently, “until regulators coordinate and assist the industry in clarifying and balancing the valid interests on both sides, consumers could have to choose between facing potential losses or not using what they may find to be an otherwise valuable financial service, and fintech firms providing useful services to consumers will face barriers to providing their offerings more broadly.”<sup>39</sup>

The FSOC Fintech Subcommittee should work with the industry to agree to a set of minimum standards (e.g., for access, disclosure, data handling, security and customer control) for any third party that aggregates or has access to a consumer’s personal financial data, in addition to, as discussed above, GLBA data security standards applicable to financial institutions. Once these minimum standards have been developed and agreed upon, Treasury and the individual financial regulators should encourage the industry to implement the standards as quickly as possible but, given the rapid current pace of innovation, should refrain from imposing the minimum standards through regulation at this time. Instead, the role of regulators at this stage should be to provide

---

<sup>37</sup> As we note elsewhere, the FSOC Fintech Subcommittee should play a key role in fostering agreement on the appropriate minimum standards for each activity.

<sup>38</sup> See GAO Fintech Report at 56 (noting views from the Federal Reserve and the OCC that premature regulatory action with respect to data aggregation could be detrimental).

<sup>39</sup> Id. at 57. We note that SIFMA already is coordinating a broad-based industry effort to create a set of industry-wide principles for protecting, sharing and aggregating customer financial information in order to promote, transparency, efficiency and trust in the marketplace. See SIFMA, Issues: Personal Data Aggregation ([link](#)).

clarity on the threshold requirements and support and collaborate in the development of industry standards. The minimum standards should include the following:

- Because of the extensive damage that could result from data being compromised, all participants in the fintech chain should work with the industry to develop and implement a means to access consumer financial data that does not require sharing their confidential financial account credentials (e.g., personal IDs and passwords). Instead, all participants should work to maximize the availability and use of modern, safe and hygienic methods (e.g., OAuth), which triangulate authentication with the bank and protects consumer from having to share this sensitive information with third parties.
- Because data aggregators are often retained by third parties, such as fintech service providers, these aggregators are often invisible to consumers. Clear disclosure and explanation of this relationship, including the name and contact information of the aggregator, should also be included as part of the required notice and consent. Any aggregator that has a direct consumer relationship should already be clearly subject to GLBA and required to provide a Privacy Notice in connection with establishing the consumer relationship.
- Third parties that do not have direct consumer relationships and only facilitate access to data should only access the customer financial account data necessary to provide the product or service they are offering, and should not be permitted to access or use other non-public and confidential personal information.
- Third parties that do not have direct consumer relationships and only facilitate access to data must ensure that clear and conspicuous explanations of how they will access and use consumers' financial account data, including whether they will pass that data on to other parties, are provided to consumers. Consumers must be able to control that access both before it begins and on an ongoing basis.
- Consumers should be able to withdraw their consent easily and at any time with confidence that data aggregators with whom they have relationships, or behind-the-scenes third parties, will stop collecting their personal information and delete any access credentials or tokens within a reasonable time of withdrawal of their consent.
- Consumers deserve assurances that anyone accessing their personal information will keep it safe and secure, adopt the same data and security standards followed by regulated financial institutions, and share full responsibility for any personal information that they receive and provide to others while such data is in their custody or control. In addition, consistent standards should be applied across the aggregator community regarding notifying consumers and federal banking regulators about any personal data breach.

- Third parties that fail to maintain and adhere to appropriate data and security standards should bear financial responsibility for the losses incurred due to that failure.

### Recommendation Three

---

The federal banking agencies should revisit and modify as appropriate their current interpretations of certain banking statutes, including with respect to the meaning of control under the BHC Act and the business of banking under the National Bank Act in order to ensure that such interpretations do not impede investments in fintech innovation.

Current federal banking statutes, many of which were enacted decades or even more than a century ago, have not kept pace with technological innovation. Laws and regulations designed to address what banking entailed many years ago are in some cases ill-suited to address banking as it actually exists today. These statutes and the agencies' interpretations of them have discouraged bank investments in fintech and exacerbated the fragmentation of our regulatory system due to a lack of consistency in the application of similar elements of different statutes.

The following subsections contain specific recommendations regarding bank regulatory statutes, regulations or guidance that should be updated to facilitate greater bank involvement in fintech activities without sacrificing financial stability or consumer protection.

#### A. "Control" Under the BHC Act

---

The definition of control under the BHC Act constrains the types of investments and relationships that a BHC and its subsidiaries may have in or with other companies. To the extent a BHC makes a "controlling" investment in another company, that company must be engaged only in a relatively narrow set of permissible activities. Control is defined as the ownership of 25% of a class of voting securities, the power to elect a majority of the board, or the power to exercise a controlling influence over management or policies as determined by the Federal Reserve after notice and hearing. While the first two tests are straightforward, the final test, to quote Federal Reserve Vice-Chairman for Supervision Quarles, is "now quite a bit more ornate than the basic standards set forth in the statute and in some cases cannot be discovered except through supplication to someone who has spent a long apprenticeship in the art of Fed interpretation."<sup>40</sup>

---

<sup>40</sup> Randal K. Quarles, Vice Chair for Supervision, Federal Reserve, Early Observations on Improving the Effectiveness of Post-Crisis Regulation (Jan. 19, 2018) ([link](#)).

The impact of this expansion of the concept of control has serious and important ramifications in the fintech area. If control exists, the company becomes constrained by the activities limitations of the BHC Act. It becomes subject to supervision and regulation like any other BHC subsidiary, thus subject to regulatory costs and burdens. For startup companies generally, and fintech companies in particular, the limitations on flexibility and the compliance and regulatory costs can inhibit innovation. Thus, BHCs generally try to limit their initial investments and restrain their business relationships with the company so as to avoid the amorphous control standard, meaning that business models with substantial promise but with little capital miss out on an important source of financing.

We agree with Treasury’s acknowledgment in its Asset Management Report that the BHC Act’s definition of control may not be appropriate in the Volcker Rule context.<sup>41</sup> We believe that the Federal Reserve should more broadly update its “controlling influence” guidance, however, so that at a minimum the parameters of controlling influence go back to the statutory standard of actual power to exercise a controlling influence over management or policies rather than the mere possibility that some degree of controlling influence might be present under certain circumstances as viewed by the Federal Reserve staff.

Furthermore, the Federal Reserve’s “controlling influence” guidance should be transparent, public, and subject to notice and comment. Once an investment is made in compliance with the Federal Reserve’s control parameters, BHCs should be encouraged, rather than discouraged, to exert the appropriate oversight of their investments and leverage the established business relationship. These reforms would enable BHCs to devote more capital and effort to innovation, benefitting the fintech company, the financial institution, and consumers.

## B. Permissible Incidental or Financial Activities Under the BHC Act

The BHC Act restricts the types of activities in which a BHC and its subsidiaries can engage. BHCs and their subsidiaries are generally prohibited from owning or controlling voting shares of any company that is not a bank and from engaging in activities other than banking or managing or controlling banks and other subsidiaries authorized under the BHC Act, subject to certain enumerated exemptions. These enumerated exemptions have essentially been frozen at a time well before the current explosion of technological innovations in the financial area. Because these exemptions are fixed, and because the fintech company must fit squarely within the parameters of the exemption, BHCs can be discouraged from making investments unless they are sure that the target will stay squarely within the range of permissible activities. Again, startup companies generally, and fintech companies specifically, are attempting to adapt rapidly to an ever-changing environment, and artificial parameters can discourage the innovation necessary to

<sup>41</sup> Treasury Asset Management Report at 54.

succeed. And while a BHC may always seek approval to engage in new activities, the approval process is slow and uncertain, and the Federal Reserve has been very reluctant to expand the area of permissibility.

BHCs that elect to be treated as financial holding companies (“**FHCs**”) may also engage in a broader range of activities that are financial in nature or incidental to activities that are financial in nature. It also permits FHCs to engage in activities that are complementary to activities that are financial in nature or incidental to activities that are financial in nature. While we would have hoped that this flexibility would have led to additional expansion, the Federal Reserve has determined that a new activity is financial in nature or incidental to an activity financial in nature only two times in the almost two decades since the power was granted to the Federal Reserve in 1999.

The Federal Reserve should interpret the BHC Act in light of modern markets and technology, and should proactively expand the list of activities that are expressly permissible under the BHC Act where possible by, for example, determining that certain fintech activities are financial in nature. Similarly, Congress and the Federal Reserve should not seek to restrict activities currently permissible under the BHC Act. For example, Congress should not act on the Federal Reserve’s 2016 request to limit merchant banking under the BHC Act.

### C. The Business of Banking Under the National Bank Act

---

The National Bank Act allows national banks to engage in the business of banking as defined under the Act and grants them the power to engage in “all such incidental powers as shall be necessary” to carry out that business.<sup>42</sup> The OCC has over the years demonstrated great flexibility in adapting the traditional banking powers to our modern economy and financial system, as well as in interpreting the incidental powers provision. For instance, while the National Bank Act states that banks can carry on the business “by discounting and negotiating promissory notes, drafts, bills of exchange, and other evidences of debt; by receiving deposits; by buying and selling exchange, coin, and bullion; by loaning money on personal security; and by obtaining, issuing, and circulating notes,”<sup>43</sup> the OCC has found numerous activities to be the functional equivalent of such items. As it has expanded the core business of banking, it has found many activities “necessary, useful or convenient” in offering permissible banking products and services. State-chartered banks, by virtue of state “wild-card” statutes that grant state banks the powers enjoyed by national banks, have also benefitted from the OCC’s efforts in this field.

This flexibility and adaptability to current conditions is essential and must be preserved. Even the OCC, however, has been relatively restrained in recent years and there is continued

---

<sup>42</sup> 12 U.S.C. § 24 (Seventh).

<sup>43</sup> *Id.*

ambiguity surrounding the scope of the business of banking that leaves national banks uncertain as to whether and to what extent they are allowed to innovate.

There is also an unfortunate interplay between the OCC's determinations of activities permissible for a national bank and the Federal Reserve's interpretation of the parameters of permissible investments by BHCs under Section 4(c)(5) of the BHC Act. Under Section 4(c)(5), a BHC may invest in "shares which are of the kinds and amounts eligible for investment by national banking associations under the provisions of section 24 of this title."<sup>44</sup> Logically, one would presume that if the OCC had determined an investment permissible for a national bank, it would be permissible for a BHC.<sup>45</sup> Unfortunately the Federal Reserve takes a very restrictive view of this exemption, and will not allow BHCs to invest in companies engaged in many of the activities the OCC has found permissible for national banks. Instead, the Federal Reserve should allow BHCs to make investments under Section 4(c)(5) of the BHC Act that the OCC has determined are permissible for a national bank.

The OCC should continue its long tradition of interpreting the National Bank Act in light of modern markets and technologies and should evaluate where additional expansion might be in order as it gains additional experience with fintech companies through its Office of Innovation and through its participation in the FSOC Fintech Subcommittee.

More generally, the agencies should publish decisions requested by institutions regarding permissibility matters related to specific innovations in redacted form and after sufficient delay to allow the requesting institution time to launch its new product or activity.

Whether by clarifying legislation or regulatory interpretation, allowing BHCs the same power afforded national banks would enhance investment opportunities and grant much needed flexibility.

## D. Brokered Deposits

---

Brokered deposits allow banks to gain access to a larger pool of potential investment funds and improve liquidity by enabling them to efficiently source deposits in large denominations in fewer individual transactions. Only well-capitalized banks can solicit and accept brokered deposits, however. In addition, under the liquidity coverage ratio rule, the outflow rate is generally assumed to be higher for brokered deposits than for other deposits. These restrictions are based on the belief that deposit brokers will withdraw brokered deposits in times of stress with little or no warning.

---

<sup>44</sup> 12 U.S.C. § 1843(c)(5).

<sup>45</sup> Indeed, one would think that if an activity were permissible for a national bank, given that it is funded by insured deposits, the investment would be even more appropriate for a BHC where insured deposits are not at risk.

The FDIC defines brokered deposit as “any deposit that is obtained, directly or indirectly, from or through the mediation or assistance of a deposit broker.”<sup>46</sup> Deposit broker is in turn defined as “[a]ny person engaged in the business of placing deposits, or facilitating the placement of deposits, of third parties with insured depository institutions or the business of placing deposits with insured depository institutions for the purpose of selling interests in those deposits to third parties.”<sup>47</sup> The FDIC has interpreted the definition of deposit broker broadly, including in recent guidance that stated, “a brokered deposit may be any deposit accepted by an insured depository institution from or through a third party, such as a person or company or organization other than the owner of the deposit.”<sup>48</sup>

This broad approach discourages banks from partnering with fintech companies. For example, certain fintech companies offer customers one-stop platforms for financial information and services and would like to include banks on their offering platforms. While a bank’s inclusion on such a platform should be considered a standard marketing partnership, if the platform involves steps taken to optimize the customer experience (e.g., linking systems, enabling pre-population of fields), those steps could be seen as the fintech company “facilitating” the placement of deposits, potentially making them brokered deposits. That determination, and the negative regulatory consequences, makes little sense when applied to fintech marketing partnerships. Unlike traditional deposit brokers, these marketing partners typically have no authority whatsoever to direct withdrawal of funds once placed by consumers, so these deposits are at no greater risk of light in times of stress than are standard consumer deposits.

The FDIC’s current view of brokered deposits discourages innovative and beneficial partnerships between banks and fintech companies with no apparent safety and soundness benefit. Therefore, to encourage innovative and beneficial partnerships between banks and fintech companies, the FDIC should clarify that these types of digital marketing relationships for the benefit of consumers will not be viewed as facilitating the placement of deposits.

## Recommendation Four

---

The SEC should reexamine rules that may unnecessarily inhibit the growth of both traditional and digital forms of advice and should revisit rules that govern how documents must be delivered.

---

<sup>46</sup> 12 C.F.R. § 337.6(a)(2).

<sup>47</sup> 12 U.S.C. § 1831f; 12 C.F.R. § 337.6(a)(5)(i)(A).

<sup>48</sup> FDIC, Guidance on Identifying, Accepting, and Reporting Brokered Deposits, Frequently Asked Questions (revised Jul. 14, 2016) ([link](#)).



## A. Digital Investment Advice

---

Digital advisers are simply an evolution of traditional advisers and their activities fit within the existing regulatory framework for investment advisers under the Investment Advisers Act of 1940 (the “**Advisers Act**”). Innovation in the digital advisory space could be impeded if regulators were to consider implementing requirements applicable solely to digital advisers.

SIFMA supports the SEC’s approach to digital advisers as set forth in its 2017 guidance, which stated that digital advisers are subject to the fiduciary obligations and provisions of the Advisers Act.<sup>49</sup> While acknowledging that digital advisers may face “unique considerations” in terms of satisfying their obligations under the Advisers Act (e.g., satisfying suitability obligations exclusively through questions on a digital platform), the SEC did not suggest that additional regulation was necessary.

Like traditional advisers, digital advisers provide advice to clients through a fiduciary relationship established by contract and collect information from those clients to establish a reasonable basis for such advice. The fundamental difference is that digital advisers interact with their clients primarily, and in some cases, exclusively, through electronic means. For example, a digital adviser and client may interact exclusively via a website or mobile application with no direct human interaction. A digital adviser may also use an algorithm that generates portfolio recommendations based solely on a client’s answers to questions regarding their personal circumstances and investment objectives such that there is no human involvement in an individual recommendation beyond the development and maintenance of the algorithm. These developments in part have arisen out of client demand as certain consumers prefer a purely online experience or do not feel that the costs of additional services are justified by the value they provide.

Additional regulation could make the provision of digital advisory services more burdensome and costly, thus limiting the growth of digital advisers that expand consumer choice and that also provide previously underserved markets access to investment advice in an easier and more affordable manner. More can be done to better tailor existing rules to more effectively support innovation for both traditional and digital advisory services.

SEC Rule 3a-4, promulgated under the Investment Company Act of 1940, provides a nonexclusive safe harbor from the definition of investment company for programs that provide discretionary investments advisory services to clients. As currently constructed, the Rule 3a-4 safe harbor requires that the client have the ability to impose reasonable restrictions on the management of their account, including the ability to designate particular securities or types of securities that should not be purchased for that account. The safe harbor also requires annual or

---

<sup>49</sup> SEC, Division of Investment Management, IM Guidance Update No. 2017-02 (Feb. 2017) ([link](#)).



more frequent contact with the client to determine whether there has been a change in the client's financial situation or investment objectives. Because digital advisory programs tend to offer a more limited range of investment options and rely primarily on ETFs and mutual funds, the SEC should, through notice and comment, consider revisions to Rule 3a-4 to focus the safe harbor on a client's ability to customize the investment experiences offered by the digital adviser while moving away from the safe harbor's current focus on a client's ability to impose restrictions on his or her portfolio. The SEC should also consider ways in which required client contacts under the safe harbor can be better tailored to the context of digital investment advice.

Advisers Act Rule 206(4)-3 makes it unlawful, subject to certain exceptions, for any registered investment adviser to pay a cash fee, directly or indirectly, to someone who has solicited any client for or has referred any client to, an investment adviser. While the rule does not reach advertisements for impersonal advisory services that do not purport to meet the objectives or needs of a specific client, the risk of an impermissible solicitation could arise if, through use of data, advertising becomes more tailored. The SEC should therefore proactively clarify Rule 206(4)-3 to make clear that compensation arrangements for online advertisements of this nature are not cash payments for client solicitations as prohibited under that rule. When clarifying the rule, the SEC should, through notice and comment, seek input on the scope of online advertisements to which the revised rule would not apply.

The SEC should also support a disclosure approach for all investment advisers modeled on FINRA Rule 2210 that would allow the use of testimonials in certain cases, conditioned on a requirement that the investment advisor discloses that the testimonial may not be representative of the experiences of other consumers and that there is no guarantee of future performance or success. As an intermediate step, the SEC could consider limiting testimonials to non-investment performance-related matters, such as the client's experience with a particular advisor.

## B. Required Deliveries of Fund Investment and Disclosure Documents

---

Current SEC rules, quite appropriately, seek to protect consumers by ensuring that they have access to fund documents that may contain important disclosures. These rules, however, have not necessarily kept pace with the times. For example, Advisers Act Rule 204-3<sup>50</sup> and Part 2 of Form ADV require that registered investment advisers deliver annually to their clients or prospective clients either a copy of their current brochure or a summary of material changes made to the brochure in the past year with an offer to provide a copy of the current brochure upon request. While delivery of the brochure may, in certain cases, be made electronically, all such deliveries must be made in accordance with the SEC's 1996 and 2000 guidance related to

---

<sup>50</sup> 17 C.F.R. § 275.204-3.

the use of electronic media.<sup>51</sup> These guidance documents require that, in order to deliver brochures electronically, investment advisers must either “(i) obtain the intended recipient’s informed consent to delivery through a specific electronic medium; (ii) obtain evidence that the intended recipient actually received the electronic delivery or (iii) make the delivery through “certain facsimile methods.”<sup>52</sup>

Separately, in May 2015, the SEC proposed Rule 30e-3 under the Investment Company Act of 1940.<sup>53</sup> This proposed rule would permit mutual funds and intermediaries, such as life insurers, to provide notice to shareholders of the internet availability of shareholder reports.<sup>54</sup> The SEC, however, has not yet finalized this proposed rule.

We fully agree with Treasury’s prior recommendation that regulators consider “innovative uses of new technology to enhance the delivery of information to fund investors.”<sup>55</sup> Consistent with this recommendation, the SEC should consider an updated model for electronic delivery of fund investment and disclosure documents.

As Treasury has previously recommended, the SEC should finalize its proposed Rule 30e-3. But modernization efforts can and should go further. The delivery of fund reports and other materials by electronic means, such as a website or via e-delivery, would, as Treasury noted, “enable a greater level of detail and information to reach investors through an online platform that would likely enhance the user experience and provide greater educational value for investors.”<sup>56</sup>

---

<sup>51</sup> SEC, Use of Electronic Media by Broker-Dealers, Transfer Agents, and Investment Advisers for Delivery of Information, Investment Advisers Act Release No. 1562, 61 Fed. Reg. 24644 (May 15, 1996) ([link](#)) [hereinafter 1996 Electronic Delivery Guidance]; SEC Interpretation: Use of Electronic Media, Release Nos. 33-7856, 34-42728, IC-24426 (May 4, 2000) ([link](#)).

<sup>52</sup> 1996 Electronic Delivery Guidance at 24647.

<sup>53</sup> Investment Company Reporting Modernization, 80 Fed. Reg. 33590 (June 12, 2015) ([link](#)).

<sup>54</sup> As Treasury has previously explained, “A fund relying on the proposed rule would be required to comply with certain conditions, including making the shareholder report and other information publicly accessible and free of charge on a website, providing notice to shareholders of the availability of the shareholder report online, and allowing shareholders to request paper copies by mail. The website materials must be presented in a format convenient for reading online and printing on paper and permit a person to retain an electronic version. Most notably, the proposed rule would permit the use of implied consent to delivery by website in the absence of further instruction from the shareholder.” Treasury Asset Management Report at 49.

<sup>55</sup> Treasury Asset Management Report at 50.

<sup>56</sup> *Id.*

## Recommendation Five

---

To resolve the uncertainty created by the *Madden v. Midland Funding, LLC* decision and to assure the smooth functioning of our financial markets, the Administration should promote a legislative solution to the court challenges to the valid-when-made doctrine.

The valid-when-made doctrine, established by Supreme Court precedent years ago, provides that a loan that is lawful when made will remain lawful even if transferred to a third party that could not have initially made the loan in question. The valid-when-made doctrine, although essential to the smooth functioning of our financial system, has been called into question on a number of fronts, including various court decisions, the most prominent of which is *Madden v. Midland Funding, LLC*.<sup>57</sup> In *Madden*, where a debt collector purchased a debt originally owed to a national bank, the U.S. Court of Appeals for the Second Circuit held that the debt collector was not entitled to protection from state-law usury claims under the National Bank Act and could not rely on the fact that the loans in question were valid and permissible when made by the originating bank.

Our financial markets depend on the continued validity of the valid-when-made doctrine. Banks routinely sell or securitize loans for balance sheet management purposes and will often sell written-down or charged-off loans to third parties who are in better positions to collect. More recently, banks have partnered with marketplace lenders to offer attractive and safe alternatives to abusive forms of consumer credit. By undermining basic assumptions as to the assignability of assets that banks have legally created, the *Madden* decision impairs liquidity and significantly interferes with the core powers afforded to banks under federal law.

Hand-in-hand with the valid-when-made doctrine is the true lender doctrine. In instances where multiple parties are involved in extending credit, some courts have begun to evaluate which of those parties is the true lender. Courts have taken a variety of approaches (and in many cases, it seems, a results-oriented approach, taking into account the nature of the loans in question)<sup>58</sup> to determine which of those parties is the true lender, with the concomitant responsibilities and compliance obligations under applicable law. Often a party other than the bank making the loan is deemed to be the true lender, bringing into play applicable state interest and usury laws and state lender licensing requirements, among other things.

---

<sup>57</sup> 786 F.3d 246 (2d Cir. 2015), *cert. denied* 136 S. Ct. 2505 (June 27, 2016).

<sup>58</sup> Compare *CFPB v. CashCall, Inc.*, No. CV 15-cv-7522-JFW (RAOx), 2016 WL 4820635 (C.D. Cal. Aug. 31, 2016) (true lender challenge upheld) with *Beechum v. Navient Solutions, Inc.*, C.D. Cal., No. 2:15-cv- 08239-JGB-KK (Sept. 20, 2016) (true lender challenge denied, without discussion).

Because of the fact-specific nature of these judicial inquiries, and the high variability among courts in the rules that are applied, bank partnerships with responsible marketplace lenders are subject to uncertainty and potential challenges, regardless of whether or not the loan is safe, sound, consumer-friendly and appropriate.

In addition to harming consumers, the uncertainty that has been created by the true lender doctrine has interfered with the development of sound and appropriate innovation in delivering banking services and—like the uncertainty created by the *Madden* decision and its progeny—requires and deserves a solution.

We suggest that the FDIC and OCC take steps to put an end to the confusion surrounding the true lender doctrine that is not only harming consumers but interfering with the development of sound and appropriate innovation in delivering banking services by confirming the valid-when-made doctrine. While the concerns raised by *Madden* can be addressed through a relatively straightforward legislative affirmation of the valid-when-made doctrine,<sup>59</sup> establishing clear guidelines for determining when a national or state chartered bank is the true lender (in a manner that addresses the concerns of various constituencies, and that evolves with industry changes) is a more complex exercise which, we believe, may be accomplished through a combination of enabling legislation and joint agency rulemaking. The agencies and Congress should reject any definition of true lender that is based upon the “predominant economic interest” standard adopted by certain courts, as the differences among the courts’ interpretations of such standard, as well as the unpredictability of the outcome of the application of such standard, are already contributing to the current market uncertainty. Instead, the agencies and Congress should look to standards emphasizing sound business practices and safety and soundness principles such as those included in the supplemental examination procedures recently adopted by the OCC.<sup>60</sup>

In addition to supporting current and future legislation, regulators could take a variety of steps to put an end to the confusion surrounding *Madden*. For example, the OCC, which submitted an *amicus* brief to the Supreme Court opposing the ruling in *Madden*, should follow up with an interpretive opinion on the interest rates preemption issue. Doing so would not only clear up some uncertainty surrounding this doctrine but may spark other regulators to issue their own opinions addressing *Madden*. Accumulated pressure by regulators could cause the courts to seriously reconsider the Second Circuit ruling.

---

<sup>59</sup> The House of Representatives in February 2018 passed a bipartisan “Madden Fix” bill that would reaffirm the valid-when-made doctrine and add clarifying language to the National Bank Act to preempt state-law usury limits. See H.R. 3299, Protecting Consumers Access to Credit Act of 2017 (115<sup>th</sup> Cong. 2d Sess., 2018) ([link](#)). We strongly support the bipartisan Madden Fix.

<sup>60</sup> See OCC Bulletin 2017-7, Supplemental Examination Procedures for Risk Management of Third-Party Relationships (Jan. 24, 2017) ([link](#)).

## Recommendation Six

---

The agencies should foster the responsible adoption of distributed ledger technologies by updating regulations that impede their use.

DLT, such as blockchain, offers a means to securely, accurately, and efficiently store information in a decentralized form, optimizing the means in which information is protected and distributed. DLT could have a major impact on the way financial institutions conduct business. At the same time, and as with other issues discussed in this White Paper, continued uncertainty related to the application of existing regulatory requirements has meant that DLT has not been fully utilized in areas where it could be most beneficial, improving controls and efficiency.

CFTC Commissioner Behnam recently stated, “Whether the meteoric rise of bitcoin or the equally swift development of [DLT], the general public and policy makers have taken notice across the globe. I hope that the U.S. will take a leading role in paving the way for a well-defined, fair, and balanced regulatory regime. In my view the best and most efficient manner to achieve this important and much needed goal involves [FSOC] ... FSOC is perfectly suited to address the promise and risks posed by” fintech.<sup>61</sup>

We agree with Commissioner Behnam that FSOC, and an FSOC Fintech Subcommittee in particular, would be well-placed to encourage the continued responsible adoption of DLT. Even in the absence of an FSOC Fintech Subcommittee, however, the agencies should continue to encourage DLT innovation and should not hinder its growth through prohibitive, unnecessary or antiquated regulation or through narrow interpretations of existing regulations. DLT is a new, developing technology that could be used to modify existing market activities and operations. Therefore, we believe that, at least initially, the existing regulatory framework can be adapted for DLT. To ensure that DLT continues to grow and evolve, the agencies should be willing to make regulatory accommodations when DLT projects operate in ways not covered by current regulations, including in a joint or coordinated fashion, where warranted.

For example, if securities were issued on a distributed ledger or tracked on a ledger to facilitate trading and settlement, custody, control location, or transfer agents, regulations may need to be amended to reflect this new approach. Furthermore, if trading or settlement processes were done via DLT, information would be made available to counterparties directly through the ledger and rules regarding confirmations and trade and settlement notifications may need to be modified. As the use of DLT continues to mature, this technology’s features of immutability and cryptographic security make it likely that it can be employed with strong cybersecurity to establish safe custody of virtual assets, and regulators will need to be prepared to potentially

---

<sup>61</sup> Behnam Remarks, *supra* note 7.

issue guidance regarding how to apply existing rules and, as needed, promulgate rule amendments to accommodate this.<sup>62</sup>

We believe tools we recommend earlier in this White Paper, such as the single regulatory sandbox and agency no-action or interpretive letters, would also do much to promote responsible DLT innovation in an efficient manner.

The FSOC Fintech Subcommittee should work with regulators, both on the federal and state level, to coordinate approaches to DLT across both regulated and non-regulated entities. A coordinated regulatory approach will result in a more competitive industry by facilitating adoption, acceptance and interoperability for all market participants. Finally, regulators should also consider the application of DLT to their own internal processes.

## Recommendation Seven

---

**In the field of cloud computing, the agencies should draw upon the expertise of industry groups and look wherever possible to harmonize standards across jurisdictions.**

The availability of cloud technologies also provides key benefits to financial institutions of all sizes, and is playing an important part in the modernization of infrastructures and business models. The benefits offered by the cloud include economies of scale and cost efficiencies, the ability for firms of diverse sizes and business models to scale computing power to their needs, greater security, and greater ease of innovation and analytics.

At the same time, and as with DLT, continuing uncertainty related to the application of existing regulatory structures to the use of the cloud and cloud computing vendors makes realizing these benefits difficult. For instance, while many regulators have stated that the use of the cloud constitutes outsourcing, there are challenges and questions surrounding the blanket application of the outsourcing regulatory framework to the cloud services business model that have created uncertainty and delayed broader adoption of this technology. In the case of vendor audits, for example, regulators often require on-site due diligence reviews. In the cloud context, on-site access is often difficult for financial institutions to negotiate, particularly when a cloud service provider services many hundreds or thousands of clients.

---

<sup>62</sup> Virtual assets may be treated as securities or currency, among others, for regulatory purposes. The SEC's Customer Protection Rule, Securities Exchange Act Rule 15c3-3, for example, requires a registered broker-dealer which carries customer securities to promptly obtain and maintain the physical possession or control of all fully paid and excess margin customer securities, and the rule specifies "good control locations" at which the broker-dealer may control the custody of such securities. The rule separately requires broker-dealers to calculate and deposit in a special reserve bank account for the benefit of customers the net amount of cash it owes to customers. The rule does not directly address the treatment of virtual assets and regulatory guidance or rulemaking may be required to prevent uncertainty or permit innovation.

While some institutions have successfully adopted cloud technologies, they have been forced to rely on their examination teams to navigate these issues, and that process has slowed adoption and innovation due to inconsistencies introduced by examiners at different institutions.

Further, certain European member states have imposed requirements that firms within their jurisdictions store their data only within their own country or only within Europe. These data localization requirements, which are described in greater detail in Recommendation Eight below, sometimes extend to a mandate to use only locally-based clouds and are yet another potential barrier to more widespread adoption of cloud technologies.

Consistent with the collaborative principles outlined above, regulators should draw on the expertise of industry groups and look wherever possible to harmonize standards across jurisdictions with a view toward providing greater regulatory certainty. Regulators must recognize the need for flexibility and should make use of industry-regulatory partnerships to develop guidance, rather than formal rules, where appropriate.<sup>63</sup> Dialogues in this area are ongoing. For example, the National Institute of Standards and Technology (“**NIST**”) Cloud Computing Standards Roadmap Working Group has worked with over one thousand participants from industry, academia and government (including Treasury) to foster “voluntary consensus standards development and related conformity assessment activities, which can help to accelerate the [U.S. Government] agencies’ secure adoption of cloud computing.”<sup>64</sup> An FSOC Fintech Subcommittee could further facilitate such partnerships.

In addition to taking action to clarify the application of existing regulations, financial regulators have a key role to play in addressing concerns related to the risks that use of cloud technologies could pose to the financial system. Regulators should, in accordance with the collaboration principles outlined above, create working groups or other fora for discussion in which emerging security and financial stability issues related to the cloud could be addressed if they arise.

## Recommendation Eight

---

**The Administration should work to discourage other jurisdictions from adopting unreasonable data localization requirements.**

Cross-border data transfer plays an important role in enabling digital trade and encouraging growth in the U.S. economy. The ability to transfer data and information freely across borders is essential for financial services firms that operate in a global environment and is an important aspect of data security. Data localization relates to a country’s laws and regulations which

<sup>63</sup> As recommended elsewhere in this White Paper, any such guidance should be issued through notice and comment.

<sup>64</sup> NIST Special Publication 500-291, Version 2, NIST Cloud Computing Standards Roadmap (July 2013) ([link](#)).



require firms handling the data of their citizens (including personal data) to store, process or handle that data within that country's borders. Data localization requirements have serious implications for American firms in today's economy. Such policies erect barriers to competition and innovation without enhancing data security and privacy and have discriminated particularly against financial services firms in recent years without any credible policy justification for such action. Further, the resources required for compliance with data localization laws may deter firms from entering or expanding in a market, limiting job creation and investment. These costs are passed along to consumers, reducing their access to goods and services.

Data localization policies have other negative consequences. Limitations on cross-border data access inhibit firms' cybersecurity controls (and ability to monitor and prevent cyber-attacks), and hamper sharing of cyber threats within firms and with law enforcement. In addition, requirements to store data onshore create additional points of entry for bad actors to infiltrate networks. Further, restrictions on cross-border data flow introduce compliance risk for firms, as privacy laws and blocking statutes introduce conflicts of law for multinational firms subject to multiple regulatory reporting regimes. Accordingly, data localization policies can undermine firms' efforts to comply with regulatory requirements (including KYC and AML rules). Finally, data localization also affects firms' business continuity and disaster recovery plans. Local data back-ups are less robust and may create tangible challenges for seamless continuity of service for clients.

To its credit, the United States generally has adopted sensible policies on cross-border data flows in recognition of the fact that data localization measures are counterproductive, fragment the global operations of firms, increase cybersecurity risks, and inhibit cross-border trade and investment. U.S. financial regulators should, in their interactions with their non-U.S. counterparts, encourage their fellow regulators to pursue policy approaches that help deliver efficient and secure cross-border data flow without adversely harming trade and investment flows that support economic growth in the United States.

## Recommendation Nine

---

**Treasury and the agencies should facilitate the implementation of artificial intelligence tools that could facilitate compliance and should also support wider adoption of machine learning technologies.**

There are two areas in which financial regulators can encourage the use of artificial intelligence and machine learning. First, financial regulators should themselves consider developing machine-readable regulations (i.e., regulations drafted in a structured format that are easier for machines to digest). UK's Financial Conduct Authority is currently considering the benefits and



implications of a move to machine-readable regulations in financial services.<sup>65</sup> As we note elsewhere in this White Paper, U.S. regulators should not adopt fintech regulatory practices from other jurisdictions in a wholesale manner and should in each case tailor any regulatory practice adopted from elsewhere to the unique contours of the U.S. financial system. Even so, to ensure that the U.S. does not miss out on any potential regulatory advancements that facilitate progress consistent with President Trump’s Core Principles, U.S. regulators should analyze the potential benefits—and the potential downsides—of machine-readable regulations. As stated previously, the FSOC Fintech Subcommittee could play a key role in creating and overseeing a public-private task force to carry out this analysis.

Second, financial regulators should work with the financial services industry to better understand the benefits and risks of the industry’s current and future use of artificial intelligence and machine learning. Machine learning and artificial intelligence offer significant opportunities for financial institutions to improve services and reduce costs. Processes that combine artificial intelligence and automation, such as cognitive automation, could be used to replace human labor for both simple and complex repetitive tasks in areas such as mortgage lending, improving both operational efficiency and customer service. Machine learning technologies are complex, however, so regulators should focus on developing technological expertise and establishing a dialogue with the industry, rather than issuing formal guidance.

### A. Machine Readable Solutions

U.S. regulators should explore creating a machine readable format for various regulatory regimes to allow the integration of advanced technologies into existing compliance structures. By taking the lead in this regard, U.S. regulators would encourage the fintech industry to continue to build out compliance solutions that take advantage of machine reading formatted regulations.

An early area for exploration of this concept could be in routine supervisory reporting of numerical regulatory outcomes and data sets. Other, less numbers-based types of regulation would require more work to transpose into machine-readable code and could start to be tackled once more simple reporting has successfully been automated.

### B. Industry’s Use of Artificial Intelligence and Machine Learning

Because of the complex nature of machine learning, regulators should not at this time issue formal guidance on this topic. Instead, regulators should take steps to ensure regulatory staff at all levels are adequately informed about machine learning technology and how machine learning has affected and will affect various aspects of the financial services industry, including the

<sup>65</sup> Financial Conduct Authority, Call for Input: Using technology to achieve smarter regulatory reporting (last updated Mar. 30, 2018) ([link](#)).

integration of cognitive automation into existing compliance frameworks. To do so, regulators should collect and catalogue issues as they arise and should have an open dialogue with the industry regarding these issues. An FSOC Fintech Subcommittee could facilitate such interactions, recognizing that artificial intelligence is a prime area for exploration in the sandbox context.

Regulators should work with the industry, for example, to help financial institutions better understand how they can comply with fair lending requirements when using machine learning and alternative data, including how to measure disparities, demonstrate business need for—or financial inclusion benefits from—particular alternative data inputs or approaches. Although it may be possible to make credit available to more people through these methods, even small-scale experimentation is impeded by a lack of clarity.<sup>66</sup>

The FSOC Fintech Subcommittee should also work with industry and other stakeholders to develop alternatives for meeting adverse action notification requirements in a machine learning context that provide consumers sufficient information regarding their credit applications while recognizing that inflexible interpretations of current adverse action rules are inappropriate given that the rules may not have contemplated the more sophisticated (and often more tailored and accurate) analyses possible under machine learning.

Finally, regulators should work with the industry to provide clarity on the use of artificial intelligence and machine learning specific to firms that make available virtual assistants that communicate with the public, open accounts, respond to balance inquiries, make transfers, execute transactions, and make recommendations all based on a standardized set of investment objectives. In particular, rules related to retention of communications, suitability and sales practices should be clarified.

---

<sup>66</sup> See GAO Fintech Report at 48-49 (“Fintech lenders may face challenges because agencies with authorities related to consumer protection and fair lending have not issued guidance on the use of alternative data and modeling. . . . Staff we interviewed from two consulting firms that advise on fintech told us that lack of clarity or coordination on fair lending and use of alternative data and modeling creates uncertainty for fintech lenders. This has led some fintech lenders to forgo use of alternative data for underwriting purposes since they do not know if it will produce outcomes that violate fair lending laws and regulations.”).

## IV. APPENDIX A – INTERNATIONAL APPROACHES TO FINTECH REGULATION

## APPENDIX A – INTERNATIONAL APPROACHES TO FINTECH REGULATION

The chart below gives a brief synopsis of the current state of fintech regulation in key jurisdictions.<sup>1</sup>

Jurisdiction	Regulatory Approach	Licensing Regime
<b>United States</b>	<p>Fintech is regulated at both the federal and state level, and this fragmented regulatory regime has caused the United States to fall behind.</p> <p>Current regulatory initiatives are rather limited compared to peers.</p>	<p>Currently fintech companies adhere to the same licensing requirements as more traditional businesses.</p> <p>No regulatory sandbox initiative in place.</p> <p>Unlicensed fintech companies do not have the opportunity to experiment or introduce new technologies into the market as fintech companies in other jurisdictions do.</p>
<b>United Kingdom</b>	<p>The UK has focused on creating a regulatory environment that encourages growth and competition between fintech companies and supports the development of new technologies that will innovate the financial services market.</p> <p>The UK was one of the first countries to embrace fintech and is widely seen as the gold-standard in the global fintech market. It was the first to propose and adopt the creation of a regulatory sandbox to allow fintech start-ups to experiment with new products and services subject to appropriate regulatory oversight.</p> <p>In 2014, the Financial Conduct Authority developed Project Innovate as a way to support the authorization of innovative fintech startups.</p>	<p>Fintech companies are subject to the same licensing requirements as other firms, but Project Innovate provides fintech companies with a platform to place products and services on the market and receive supervisory support during their first year of business.</p>

<sup>1</sup> For a comparison focusing on prominent non-U.S. examples of regulatory sandboxes, see GAO Fintech Report at 90-93.

Jurisdiction	Regulatory Approach	Licensing Regime
<b>Singapore</b>	<p>Singapore is an emerging fintech market and is the primary entryway into the Asian market.</p> <p>Singapore has sought to achieve balance by introducing fintech regulation at the rate that technologies improve so as to ensure that innovation is allowed to grow without the burden of a heavily regulated environment.</p> <p>The Monetary Authority of Singapore (“MAS”) supports progressive fintech regulation and collaboration with the fintech community.</p>	No fintech licensing regime, but the MAS has developed a fintech regulatory sandbox to provide fintech startups an opportunity to introduce new technologies on a smaller scale.
<b>Japan</b>	The Financial Services Agency is working to transform Japan into a fintech hub by reworking some of its existing financial regulations and introducing new regulations that include investments in fintech ventures, digital currencies, and crowdfunding.	Fintech companies are governed by the same licensing regimes as conventional financial services.
<b>Hong Kong</b>	Hong Kong subjects fintech companies to existing legal and regulatory frameworks.	Fintech companies are governed by the same licensing regimes as conventional financial services.

Tab 15



# SIFMA Data Aggregation Principles

Data aggregation applications compile customer financial information from multiple accounts and institutions onto a single platform. These applications may help investors better understand their overall financial situation and make more informed investment and financial decisions while, at the same time, create security risks for the financial institutions' data systems and individual investor information. SIFMA has adopted these principles as guidance for our members when working with data aggregation applications. While each member must determine for itself whether and how best to address these issues, these principles strive to provide customers with secure access to their financial information, while maintaining the security and integrity of our members' systems.

## 1. Access

- Customers may use third-parties to access their financial account data and SIFMA member firms believe that such access should be safe and secure.

## 2. Security and Responsibility

- Customers should not have to share their confidential financial account credentials (personal IDs and passwords) with third-parties.
- Customers deserve assurances that anyone accessing their financial account data will keep it safe and secure, adopt the same data and security standards followed by regulated financial institutions, and take full responsibility for any data that they receive and provide to others.

## 3. Transparency and Permission

- Customers should first receive a clear and conspicuous explanation of how third parties will access and use their financial account data, and then be able to consent affirmatively to this activity before it begins.
- Customers should be able to withdraw their consent easily and at any time with confidence that third parties will delete and stop collecting their financial account data and delete any access credentials or tokens.

## 4. Scope of Access and Use

- Customer information available to share with third parties typically includes financial account data such as holdings, balances, and transaction information, and does not include other non-public and confidential personal information.
- For customer protection, account activities such as third-party trading, money or asset movement, client verification, and other services that go beyond financial account data aggregation should be subject to separate agreements and require separate informed affirmative consent.

# Tab 16





## **Policy Statement on Financial Technology Companies' Eligibility to Apply for National Bank Charters**

July 31, 2018

It is the policy of the Office of the Comptroller of the Currency (OCC) to consider applications for national bank charters from companies conducting the business of banking, provided they meet the requirements and standards for obtaining a charter. This policy includes considering applications for special purpose national bank charters from financial technology (fintech) companies that are engaged in the business of banking but do not take deposits.

This policy statement is based on broad authority granted to the OCC by the National Bank Act,<sup>1</sup> as implemented in existing regulation<sup>2</sup> and established OCC procedures.<sup>3</sup>

The OCC is issuing this policy statement to clarify its intent to exercise its existing chartering authority. The OCC also recognizes the importance of supporting responsible innovation in the federal banking system to better enable the system to

- evolve to meet the needs of the consumers, businesses, and communities it serves;
- operate in a safe and sound manner;
- provide fair access to financial services;
- treat customers fairly; and
- promote economic opportunity and job creation.

The OCC recognizes that the business of banking evolves over time, as do the institutions that provide banking services. As the banking industry changes, companies that engage in the business of banking in new and innovative ways should have the same opportunity to obtain a national bank charter as companies that provide banking services through more traditional means. The OCC will require these new entrants to the national banking system to adhere to the same high standards that apply to all national banks.

The OCC adopts this policy after careful consideration of the extensive stakeholder feedback and public comment received over the past two years.

---

<sup>1</sup> See 12 USC 21, 26, and 27.

<sup>2</sup> See 12 CFR 5.20.

<sup>3</sup> See [Comptroller's Licensing Manual](#), specifically the "[Charters](#)" booklet (September 2016) and the *Comptroller's Licensing Manual* Supplement, "Considering Charter Applications From Financial Technology Companies" (July 2018).



### **OCC Chartering Authority**

The National Bank Act gives the OCC broad authority to grant charters for national banks to carry on the “business of banking.” This authority extends to special purpose national banks. As defined in the OCC’s regulations, the “business of banking” includes any of the three core banking functions of receiving deposits, paying checks, or lending money. Section 5.20 of the OCC’s regulations provides that, to be eligible for a national bank charter, a special purpose national bank must conduct at least one of these three core banking functions. Thus, the OCC has authority to grant a national bank charter to a fintech company that engages in one or more of those core banking activities.

### **OCC Support for Responsible Innovation**

The federal banking system must adapt to the rapid technological changes taking place in the financial services industry to remain relevant and vibrant and to meet the evolving needs of the consumers, businesses, and communities it serves. The OCC encourages all national banks and federal savings associations to develop strategies that incorporate responsible innovation to address the changing operating environment and evolving needs and preferences of their customers. The OCC has developed an agency-wide framework to support responsible innovation throughout the federal banking system and established the Office of Innovation to serve as a clearinghouse for innovation-related matters and a point of contact for OCC staff, banks, and nonbanks to facilitate innovation-related activities.

Considering applications from fintech companies for national bank charters is one important way that the OCC supports responsible innovation in the federal banking system. Companies engaged in the business of banking should have a path to become a national bank, provided they meet the rigorous standards necessary to become and succeed as a national bank.

Chartering a qualified fintech company as a national bank would also have important public policy benefits. The national bank charter provides a framework of uniform standards and robust supervision. Applying this framework to fintech companies that qualify can level the playing field with regulated institutions and help ensure that they operate in a safe and sound manner and fairly serve the needs of consumers, businesses, and communities. In addition, applying the OCC’s uniform supervision over national banks, including fintech companies, will help promote consistency in the application of laws and regulations across the country and ensure that consumers are treated fairly. More broadly, providing a path for fintech companies to become national banks promotes consumer choice, economic growth, modernization, and competition—all of which strengthen the federal banking system and support the nation’s economy.



## Chartering Standards and Supervisory Expectations

The decision to consider national bank charter applications from qualifying fintech companies is consistent with the OCC's longstanding chartering standards and supervisory expectations. The OCC will use its existing chartering standards and procedures for processing applications from fintech companies as outlined in the *Comptroller's Licensing Manual*. As with all national banks, the OCC will consider whether a proposed bank has a reasonable chance of success, will be operated in a safe and sound manner, will provide fair access to financial services, will treat customers fairly, and will comply with applicable laws and regulations. The OCC will also consider whether the proposed bank can reasonably be expected to achieve and maintain profitability and whether approving the charter will foster healthy competition.

A fintech company that receives a national bank charter will be subject to the same high standards of safety and soundness and fairness that all federally chartered banks must meet. As it does for all banks under its supervision, the OCC would tailor these standards based on the bank's size, complexity, and risk profile, consistent with applicable law. In addition, a fintech company with a national bank charter will be supervised like similarly situated national banks, including with respect to capital, liquidity, and risk management.

The OCC also expects a fintech company that receives a national bank charter to demonstrate a commitment to financial inclusion. The nature of that commitment will depend on the company's business model and the types of products, services, and activities it plans to provide. By providing a high standard similar to the Community Reinvestment Act's expectations for national banks that take insured deposits, the financial inclusion commitment will help ensure that all national banks provide fair access to financial services and treat customers fairly.

In addition, a fintech company approved for a national bank charter will be required to develop a contingency plan to address significant financial stress that could threaten the viability of the bank. The plan would outline strategies for restoring the bank's financial strength and options for selling, merging, or liquidating the bank in the event the recovery strategies are not effective. The specific considerations related to supervision, capital, liquidity, financial inclusion, and contingency planning are described in the agency's supplement to the *Comptroller's Licensing Manual*, "Considering Charter Applications From Financial Technology Companies."

While the OCC is open and receptive to charter applications from qualified fintech companies, the OCC will not approve proposals that are contrary to applicable law, regulation, policy, or safety and soundness. Exercising the OCC's existing authority to grant special purpose charters does not alter existing barriers separating banking and commerce. Further, proposals that include financial products and services that have



predatory, unfair, or deceptive features or that pose undue risk to consumer protection, would be inconsistent with law and policy and would not be approved.

//signed//

---

Joseph M. Otting  
Comptroller of the Currency

July 31, 2018

---

Date

Tab 17

A Financial System  
That Creates Economic Opportunities  
**Nonbank Financials, Fintech,  
and Innovation**



JULY 2018

# A Financial System That Creates Economic Opportunities **Nonbank Financials, Fintech, and Innovation**

## **Report to President Donald J. Trump**

Executive Order 13772 on Core Principles  
for Regulating the United States Financial System

**Steven T. Mnuchin**

*Secretary*

**Craig S. Phillips**

*Counselor to the Secretary*





## Staff Acknowledgments

Secretary Mnuchin and Counselor Phillips would like to thank Treasury staff members for their contributions to this report. The staff's work on the report was led by Jessica Renier and W. Moses Kim, and included contributions from Chloe Cabot, Dan Dorman, Alexandra Friedman, Eric Froman, Dan Greenland, Gerry Hughes, Alexander Jackson, Danielle Johnson-Kutch, Ben Lachmann, Natalia Li, Daniel McCarty, John McGrail, Aryn Moolji, Brian Morgenstern, Daren Small-Moyers, Mark Nelson, Peter Nickoloff, Bimal Patel, Brian Peretti, Scott Rembrandt, Ed Roback, Ranya Rotolo, Jared Sawyer, Steven Seitz, Brian Smith, Mark Uyeda, Anne Wallwork, and Christopher Weaver.



# Table of Contents

<b>Executive Summary .....</b>	<b>1</b>
Nonbank Financials, Fintech, and Innovation	4
Emerging Trends in Financial Intermediation	6
Summary of Issues and Recommendations	9
<b>Embracing Digitization, Data, and Technology .....</b>	<b>15</b>
Digitization	17
Consumer Financial Data	22
The Potential of Scale	44
<b>Aligning the Regulatory Framework to Promote Innovation .....</b>	<b>61</b>
Challenges with State and Federal Regulatory Frameworks	63
Modernizing Regulatory Frameworks for National Activities	66
<b>Updating Activity-Specific Regulations .....</b>	<b>81</b>
Lending and Servicing	83
Payments	144
Wealth Management and Digital Financial Planning	159
<b>Enabling the Policy Environment .....</b>	<b>165</b>
Agile and Effective Regulation for a 21st Century Economy	167
International Approaches and Considerations	177
<b>Appendices</b>	
Appendix A: Participants in the Executive Order Engagement Process	187
Appendix B: Table of Recommendations	195
Appendix C: Additional Background	213

# Acronyms and Abbreviations

## Acronym/Abbreviation Term

ABA	American Bankers Association
ACH	Automated Clearing House
AI	Artificial Intelligence
AMC	Appraisal Management Company
AML	Anti-Money Laundering
API	Application Programming Interface
APR	Annual Percentage Rate
AQB	Appraiser Qualifications Board
ASB	Appraisal Standards Board
ATM	Automated Teller Machine
AVM	Automated Valuation Model
BHC	Bank Holding Company
BHC Act	Bank Holding Company Act
BSA	Bank Secrecy Act
Bureau	Bureau of Consumer Financial Protection
CEG	Cybersecurity Expert Group
C.F.R.	Code of Federal Regulations
CFT	Countering the Financing of Terrorism
CFTC	U.S. Commodity Futures Trading Commission
CHAPS	Clearing House Automated Payment System
CHIPS	Clearing House Interbank Payments System
CMA	Competition and Markets Authority (U.K.)
CRA	Community Reinvestment Act
CROA	Credit Repair Organizations Act
CSBS	Conference of State Bank Supervisors
Cyber Apex	Next Generation Cyber Infrastructure Apex Program
DARPA	Defense Advanced Research Projects Agency
DHS	U.S. Department of Homeland Security
DIUx	Defense Innovation Unit Experimental

DLT	Distributed Ledger Technology
DOD	U.S. Department of Defense
Dodd-Frank	Dodd-Frank Wall Street Reform and Consumer Protection Act
DOJ	U.S. Department of Justice
DOL	U.S. Department of Labor
Education	U.S. Department of Education
EMV	Europay, Mastercard, and Visa
ESIGN	Electronic Signatures in Global and National Commerce Act
E.U.	European Union
FATF	Financial Action Task Force
FBIIC	Financial and Banking Information Infrastructure Committee
FCA	False Claims Act
FCA	U.K. Financial Conduct Authority
FCC	Federal Communications Commission
FCRA	Fair Credit Reporting Act
FDCPA	Fair Debt Collection Practices Act
FDIC	Federal Deposit Insurance Corporation
FedACH	Federal Reserve Banks' Automated Clearing House
FFIEC	Federal Financial Institutions Examination Council
FHA	Federal Housing Administration
FHA-HAMP	FHA Home Affordable Modification Program
FHFA	Federal Housing Finance Agency
FHLB	Federal Home Loan Bank
FICO	Fair Isaac Corporation
FIL	Financial Institutions Letter
FinCEN	Financial Crimes Enforcement Network
FINRA	Financial Industry Regulatory Authority
Fintech	Financial Technology
FIRREA	Financial Institutions Reform, Recovery, and Enforcement Act
FlexMod	GSE Flex Modification
FPS	Faster Payments Service (U.K.)

FRB	Board of Governors of the Federal Reserve System
FRBNY	Federal Reserve Bank of New York
FSB	Financial Stability Board
FS-ISAC	Financial Services Information Sharing and Analysis Center
FTC	Federal Trade Commission
G-7	Group of 7
G20	Group of 20
GAO	U.S. Government Accountability Office
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation (E.U.)
GLBA	Gramm-Leach-Bliley Act
GRC	Governance, Risk and Compliance
GSE	Government-Sponsored Enterprise
HUD	U.S. Department of Housing and Urban Development
IaaS	Infrastructure as a Service
IRS	Internal Revenue Service
ISO	International Organization for Standardization
IT	Information Technology
LOA	Levels of Assurance
MAS	Monetary Authority of Singapore
MBA	Mortgage Bankers Association
MBS	Mortgage-Backed Securities
MCSBA	Maryland Credit Services Business Act
MERS	Mortgage Electronic Registration System
MMIF	Mutual Mortgage Insurance Fund
MPL	Marketplace Lender
MSB	Money Services Business
MTRA	Money Transmitter Regulators Association
NACHA	National Automated Clearinghouse Association
NAIC	National Association of Insurance Commissioners
NBA	National Bank Act

NCUA	National Credit Union Administration
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NMLS	Nationwide Mortgage Licensing System or Nationwide Multistate Licensing System
NSF	National Science Foundation
NSS	National Settlement Service
OBIE	Open Banking Implementation Entity (U.K.)
OCC	Office of the Comptroller of the Currency
OFX	Open Financial Exchange
P2P	Person-to-Person or Peer-to-Peer
PaaS	Platform as a Service
PCI-DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
PIN	Personal Identification Number
PLS	Private-Label Securities
PSD2	Revised Payment Services Directive (E.U.)
PSP	Payment Service Provider
RTP	Real Time Payments
SaaS	Software as a Service
SAFE Act	Secure and Fair Enforcement for Mortgage Licensing Act
SEC	U.S. Securities and Exchange Commission
SIFMA	Securities Industry and Financial Markets Association
SRO	Self-Regulatory Organization
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SWIFT GPI	Society for Worldwide Interbank Financial Telecommunication Global Payments Innovation
TCH	The Clearing House
TCPA	Telephone Consumer Protection Act
TFFT	Basel Committee on Banking Supervision's Task Force on Financial Technology
Treasury	U.S. Department of the Treasury

U.K.	United Kingdom
U.S.	United States
UDAAP	Unfair, Deceptive, or Abusive Acts or Practices
UDAP	Unfair or Deceptive Acts or Practices
UETA	Uniform Electronic Transactions Act
URPERA	Uniform Real Property Electronic Recording Act
U.S.C.	United States Code
USDA	U.S. Department of Agriculture
USPAP	Uniform Standards of Professional Appraisal Practice
VA	U.S. Department of Veterans Affairs
ZB	Zettabyte

# Executive Summary



## Introduction

President Donald J. Trump established the policy of his Administration to regulate the U.S. financial system in a manner consistent with a set of Core Principles. These principles were set forth in Executive Order 13772 on February 3, 2017. The U.S. Department of the Treasury (Treasury), under the direction of Secretary Steven T. Mnuchin, prepared this report in response to that Executive Order. The reports issued pursuant to the Executive Order identify laws, treaties, regulations, guidance, reporting, and record keeping requirements, and other Government policies that promote or inhibit federal regulation of the U.S. financial system in a manner consistent with the Core Principles.

The Core Principles are:

- A. Empower Americans to make independent financial decisions and informed choices in the marketplace, save for retirement, and build individual wealth;
- B. Prevent taxpayer-funded bailouts;
- C. Foster economic growth and vibrant financial markets through more rigorous regulatory impact analysis that addresses systemic risk and market failures, such as moral hazard and information asymmetry;
- D. Enable American companies to be competitive with foreign firms in domestic and foreign markets;
- E. Advance American interests in international financial regulatory negotiations and meetings;
- F. Make regulation efficient, effective, and appropriately tailored; and
- G. Restore public accountability within federal financial regulatory agencies and rationalize the federal financial regulatory framework.

## Scope of This Report

The financial system encompasses a wide variety of institutions and services, and accordingly, Treasury has delivered a series of four reports related to the Executive Order covering:

- The depository system, covering banks, savings associations, and credit unions of all sizes, types, and regulatory charters (the Banking Report,<sup>1</sup> which was publicly released on June 12, 2017);
- Capital markets: debt, equity, commodities and derivatives markets, central clearing, and other operational functions (the Capital Markets Report,<sup>2</sup> which was publicly released on October 6, 2017);

---

1. U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities: Banks and Credit Unions* (June 2017).

2. U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities: Capital Markets* (Oct. 2017).



- The asset management and insurance industries, and retail and institutional investment products and vehicles (the Asset Management and Insurance Report,<sup>3</sup> which was publicly released on October 26, 2017); and
- Nonbank financial institutions, financial technology, and financial innovation (**this report**).

## Review of the Process for This Report

For this report, Treasury incorporated insights from the engagement process for the previous three reports issued under the Executive Order and also engaged with additional stakeholders focused on data aggregation, nonbank credit lending and servicing, payments networks, financial technology, and innovation. Over the course of this outreach, Treasury consulted extensively with a wide range of stakeholders, including trade groups, financial services firms, federal and state regulators, consumer and other advocacy groups, academics, experts, investors, investment strategists, and others with relevant knowledge. Treasury also reviewed a wide range of data, research, and published material from both public and private sector sources.

Treasury incorporated the widest possible range of perspectives in evaluating approaches to regulation of the U.S. financial system according to the Core Principles. A list of organizations and individuals who provided input to Treasury in connection with the preparation of this report is set forth as *Appendix A*.

## Nonbank Financials, Fintech, and Innovation

Nonbank financial firms play important roles in providing financial services to U.S. consumers and businesses by providing credit to the economy across a wide range of retail and commercial asset classes. Nonbanks are well integrated into the U.S. payments system and play key roles such as facilitating back-end check processing; enabling card issuance, processing, and network activities; and providing customer-facing digital payments software. Nonbank financial firms also play important roles in capital markets and in providing financial advice and execution services to retail investors, among a range of other services.

The financial crisis altered the environment in which banks and nonbanks compete to provide financial services. Specifically, many traditional financial companies such as banks, credit unions, and insurance companies experienced significant distress during the crisis. This distress caused the insolvency or restructuring of many existing financial companies, particularly those with volatile funding sources and concentrated balance sheets. The government responded to this distress, and the unprecedented magnitude of taxpayer support it triggered, by writing far-reaching laws that mandated the adoption of hundreds of new regulations. In some cases, these policy changes made certain product segments unprofitable for banks, thereby driving activity

---

3. U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities: Asset Management and Insurance* (Oct. 2017).

outside of the banking sector and creating opportunities for emerging nonbank financial firms to address unmet market demands.

At the same time, and as part of a longer-term trend, the rapid development of financial technologies has enabled financial services firms to improve operational efficiencies and lower regulatory compliance costs that increased as a result of the expansion of regulations following the financial crisis. Since the financial crisis, there has been a proliferation in technological capabilities and processes at increasing levels of cost effectiveness and speed. The use of data, the speed of communication, the proliferation of mobile devices and applications, and the expansion of information flow all have broken down barriers to entry for a wide range of startups and other technology-based firms that are now competing or partnering with traditional providers in nearly every aspect of the financial services industry.

The landscape for financial services has changed substantially. From 2010 to the third quarter of 2017, more than 3,330 new technology-based firms serving the financial services industry have been founded, 40% of which are focused on banking and capital markets.<sup>4</sup> In the aggregate, the financing of such firms has been growing rapidly, reaching \$22 billion globally in 2017, a thirteen-fold increase since 2010.<sup>5</sup> Significantly, lending by such firms now makes up more than 36% of all U.S. personal loans, up from less than 1% in 2010.<sup>6</sup> Additionally, some digital financial services reach up to some 80 million members,<sup>7</sup> while consumer data aggregators can serve more than 21 million customers.<sup>8</sup>

Important trends have arisen as a consequence of these factors, including:

- The nonbank sector has responded opportunistically to the pullback in services and increased regulatory challenges placed on traditional financial institutions, including the launch of numerous startup platforms;
- Many of these platforms have rapidly grown beyond the startup phase, employing technology-enabled approaches to customer acquisition and process support for their services;
- Innovative new platforms in the nonbank financial sector are, in some cases, standalone providers, while others have focused on providing support for or interconnectivity with traditional financial institutions through partnerships, joint ventures, or other means;

4. Deloitte, *Fintech by the Numbers: Incumbents, Startups, Investors Adapt to Maturing Ecosystem* (2017), at 3 and 7, available at: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-dcfs-fintech-by-the-numbers-web.pdf>.

5. Id.

6. Hannah Levitt, *Personal Loans Surge to a Record High*, Bloomberg (July 3, 2018), available at: <https://www.bloomberg.com/news/articles/2018-07-03/personal-loans-surge-to-a-record-as-fintech-firms-lead-the-way> (analyzing data from TransUnion).

7. Credit Karma, *Press Release – Credit Karma and Silver Lake Announce \$500 Million Strategic Secondary Investment* (Mar. 28, 2018), available at: <https://www.creditkarma.com/pressreleases>.

8. Envestnet, *2017 Annual Report*, at 8, available at: <http://www.envestnet.com/report/2017/download/EN-2017-AnnualReport-Final.pdf>.

- Large technology companies with access to vast stores of consumer data have simultaneously entered the financial services industry, primarily in payments and credit provision; and
- The increasing scale of technology-enabled competitors and the corresponding threat of disruption has raised the stakes for existing firms to innovate more rapidly and pursue dynamic and adaptive strategies. As a result, mature firms have launched platforms aimed at reclaiming market share through alternative delivery systems and at lower costs than they were previously able to provide.

Consumers increasingly prefer fast, convenient, and efficient delivery of services. New technologies allow firms with limited scale to access computing power on levels comparable to much larger organizations. The relative ubiquity of online access in the United States, combined with these new technologies, allows newer firms to more easily expand their business operations.

In this report, we explore the characteristics of, and regulatory landscape for, nonbank financial firms with traditional “brick and mortar” footprints not covered in the previous Core Principles reports, as well as newer business models employed by technology-based firms. We also address the ability of banks to innovate internally, as well as partner with such technology-based firms. Foundational to the report’s findings, we explore the implications of digitization and its impact on access to clients and their data, focusing on several thematic areas, including:

- The collection, storage, and use of financial data;
- Cloud services and “big data” analytics;
- Artificial intelligence and machine learning; and
- Digital legal identity and data security.

This report includes a limited treatment of blockchain and distributed ledger technologies. These technologies, as well as digital assets, are being explored separately in an interagency effort led by a working group of the Financial Stability Oversight Council. The working group is a convening mechanism to promote coordination among regulators as these technologies evolve.

## Emerging Trends in Financial Intermediation

Financial services are being significantly reshaped by several important trends, including (1) rapid advances in technology; (2) increased efficiencies from the rapid digitization of the economy; and (3) the abundance of capital available to propel innovation.

### Technological Advances in Financial Services

In addition to other benefits, innovations in financial technology expand access to services for underserved individuals or small businesses and improve the ease of use, speed, and cost of such services. Businesses providing financial services benefit from opportunities to improve their product offerings to win market share and reduce per-customer operational costs.

**Expanded access to credit and financial services.** Digital advice platforms are making financial planning tools and wealth management capabilities previously limited to higher net worth households available to a much broader segment of households. New platforms for lending are developing business models that take advantage of new types of data and credit analysis, potentially serving consumer and small business borrower segments that may not otherwise have access to credit through traditional underwriting approaches. Unbanked or underbanked populations can gain improved access to banking services through new mobile device-based banking applications.

**Expanded speed, convenience, and security.** Consumer and business demand for increased convenience and speed have driven the digitization of financial services. For example, increased digitization of the mortgage process has improved the online experience of financing a home, but additional innovations could dramatically help to further shorten the time it takes to close a mortgage, which still took an average of 52 days in 2016.<sup>9</sup> Borrowers seeking to refinance or consolidate higher-rate student loans or other consumer debts can obtain accelerated credit decisions from some lenders, as can small business entrepreneurs looking to expand their business or manage their seasonality.

Payment systems also benefit from innovations that are delivering greater speed and security. The proliferation of mobile and person-to-person payments allows end-users a way to quickly transfer money using identifiers such as an e-mail address or phone number. Contactless payment methods that store and tokenize payment information are also increasingly being used and could provide a more convenient and secure way to pay. These innovations are helping small businesses to lower the barriers to receive payments.

**Reduced cost of services and operational efficiencies.** Online marketplace lenders generally offer unsecured consumer loans that are designed to refinance existing higher-rate debts into lower-rate debt, reducing borrowing costs for consumers. Digital financial advice providers are able to leverage technology to scale their services to larger numbers of investors and to provide such services at more affordable prices than traditional providers. The increasing digitization of payments is expected to reduce significant costs in the current payment processes for businesses and firms by, for example, replacing physical paper checks with electronic payments and reducing inefficiencies in cross-border payments.

## Digitization of Finance and the Economy

Changes in the hardware industry, as reflected in advances in core computing and data storage capacity, represent a sea change in capabilities and expand the potential for financial services to be provided on a more cost-effective basis. When considered alongside the ubiquity of mobile devices and the growth in the volume and facility of applications and flexibility of mobile communication, the implications for financial services are significant. The collection and storage of data and the application of advanced computational techniques allow for a new generation of approaches in the

9. Andreas Fuster et al., *The Role of Technology in Mortgage Lending*, Federal Reserve Bank of New York Staff Report No. 836 (Feb. 2018), at 12, available at: [https://www.newyorkfed.org/medialibrary/media/research/staff\\_reports/sr836.pdf](https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr836.pdf).

design, marketing, and delivery of financial services. At the same time, these new approaches may raise new concerns about data privacy and theft or misuse.

Consider the recent proliferation of digital data available for analysis. By 2020, digitized data is forecasted to be generated at a level that is more than 40 times the level produced in 2009.<sup>10</sup> In 2012, it was estimated that 90% of the digitized data in the world had been generated in just the prior two years.<sup>11</sup> Since 2012, more than one billion more people have gained access to the internet, with 2.5 billion people connected to the internet in 2012 and 3.7 billion people in 2017.<sup>12</sup> Globally, there are an estimated 27 billion devices connected to the internet, including smartphones, tablets, and computers, with expectations for 125 billion connected devices by the year 2030.<sup>13</sup>

Parallel to these growing improvements in data and connectivity are expanding complementary technologies, such as cloud computing and machine learning. These technologies enable firms to store vast amounts of data and efficiently increase computing resources. Unsurprisingly, for financial services firms, data analytics and machine learning (or artificial intelligence) are two of the top three areas of tech investment.<sup>14</sup> Other technology developments that are poised to impact innovation in financial services include advances in cryptography and distributed ledger technologies, giving rise to blockchain-based networks.

## Investment Capital

The flow of capital into investments in financial technology is very large. U.S. firms accounted for nearly half of the \$117 billion in cumulative global investments from 2010 to 2017.<sup>15</sup> Unfolding alongside these investments, many large, well-established firms involved in data, software, cloud computing, internet search, mobile devices, retail e-commerce, payments, and telecommunications have begun to engage in activities directly or indirectly related to financial services. Many of these firms are based in the United States, including firms having some of the largest market capitalizations in the world.

The availability of capital, the large size of the financial services market, and continued advancements in technology make accelerating innovation nearly inevitable. This includes investments in innovation by traditional financial institutions, such as banks, asset managers and insurers, to

---

10. A.T. Kearney, *Big Data and the Creative Destruction of Today's Business Models* (2013), at 2, available at: <https://www.atkearney.com/documents/10192/698536/Big+Data+and+the+Creative+Destruction+of+Today+s+Business+Models.pdf/f05aed38-6c26-431d-8500-d75a2c384919> (discussing Oracle forecast).

11. *Id.*

12. *Id.*

13. IHS Markit, *The Internet of Things: A Movement, Not a Market* (Oct. 2017), at 2, available at: [https://cdn.ihs.com/www/pdf/IoT\\_ebook.pdf](https://cdn.ihs.com/www/pdf/IoT_ebook.pdf). For projections that do not consider computers and phones, see Gartner, Inc., *Press Release – Gartner Says 8.4 Billion Connected “Things” Will be in Use in 2017, up 31 Percent from 2016* (Feb. 7, 2017), available at: <https://www.gartner.com/newsroom/id/3598917>.

14. PricewaterhouseCoopers, *Redrawing the Lines: FinTech's Growing Influence on Financial Services* (2017), at 9, available at: <https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-global-fintech-report-2017.pdf>.

15. Treasury analysis of FT Partners data.

provide higher quality, more secure, and more efficient services while meeting consumer demand for speed and convenience.

## Summary of Issues and Recommendations

Treasury’s review of the regulatory framework for nonbank financial institutions and innovation more broadly has identified significant opportunities to accelerate innovation in the United States consistent with the Core Principles. This review has identified a wide range of measures that could promote economic growth, while maintaining strong consumer and investor protections and safeguarding the financial system.

Treasury believes that innovation is critical to the success of the U.S. economy, particularly in the financial sector. Throughout Treasury’s findings, opportunities have been identified to modernize regulation to embrace the use of data, encourage the adoption of advanced data processing and other techniques to improve business processes, and support the launch of alternative product and service delivery systems. Support of innovation is critical across the regulatory system — both at the federal and state levels. Treasury supports encouraging the launch of new business models as well as enabling traditional financial institutions, such as banks, asset managers, and insurance companies, to pursue innovative technologies to lower costs, improve customer outcomes, and improve access to credit and other services.

Treasury’s recommendations in this report can be summarized in the following four categories:

- Adapting regulatory approaches to changes in the aggregation, sharing, and use of consumer financial data, and to support the development of key competitive technologies;
- Aligning the regulatory framework to combat unnecessary regulatory fragmentation, and account for new business models enabled by financial technologies;
- Updating activity-specific regulations across a range of products and services offered by nonbank financial institutions, many of which have become outdated in light of technological advances; and
- Advocating an approach to regulation that enables responsible experimentation in the financial sector, improves regulatory agility, and advances American interests abroad.

A list of all of Treasury’s recommendations in this report is set forth as **Appendix B**, including the recommended action, method of implementation (Congressional and/or regulatory action), and which Core Principles are addressed.

Key themes of Treasury’s recommendations are as follows.

### Embracing Digitization, Data, and Competitive Technologies

This report catalogues key elements in the evolution of digitization, data, and scalable technologies and highlights areas of relevance to many aspects of financial services, including lending, financial advice, and payments. Treasury recommends that key provisions of the Telephone Consumer



Protection Act be updated, and believes closing the digital divide to enable the entire U.S. population to benefit from modern information and communication flow is a priority.

Treasury makes numerous recommendations that would improve consumers' access to data and its use by third parties that would support better delivery of services in a responsible manner. Treasury has identified the need to remove legal and regulatory uncertainties currently holding back financial services companies and data aggregators from establishing data-sharing agreements that would effectively move firms away from screen-scraping to more secure and efficient methods of data access. The U.S. market would be well served by a solution developed in concert with the private sector that addresses data sharing, standardization, security, and liability issues. It is important to explore efforts to mitigate implementation costs for community banks and smaller financial services companies with more limited resources to invest in technology. Additionally, Treasury recommends that Congress enact a federal data security and breach notification law to protect consumer financial data and ensure that consumers are notified of breaches in a timely and consistent manner.

Removing regulatory barriers to foundational technologies, including the development of digital legal identity, is important to improving financial inclusion and enabling the use of scalable, competitive technologies. Similarly, facilitating the further development and incorporation of cloud technologies, machine learning, and artificial intelligence into financial services is important to realizing the potential these technologies can provide for financial services and the broader economy.

### **Aligning the Regulatory Framework to Promote Innovation**

Many statutes and regulations addressing the financial sector date back decades. As a result, the financial regulatory framework is not always optimally suited to address new business models and products that continue to evolve in financial services. This has the potential negative consequence of limiting innovation that might benefit consumers and small businesses. Financial regulation should be modernized to more appropriately address the evolving characteristics of financial services of today and in the future.

It is important that state regulators strive to achieve greater harmonization, including considering drafting of model laws that could be uniformly adopted for financial services companies currently challenged by varying licensing requirements of each state. Treasury encourages efforts to streamline and coordinate examinations and to encourage, where possible, regulators to conduct joint examinations of individual firms. Treasury supports Vision 2020, an effort by the Conference of State Bank Supervisors that includes establishing a Fintech Industry Advisory Panel to help improve state regulation, harmonizing multi-state supervisory processes, and redesigning the successful Nationwide Multistate Licensing System.

At the federal level, Treasury encourages the Office of the Comptroller of the Currency to further develop its special purpose national bank charter, previously announced in December 2016. A forward-looking approach to federal charters could be effective in reducing regulatory fragmentation and growing markets by supporting beneficial business models.

Finally, Treasury encourages banking regulators to better tailor and clarify guidance regarding bank partnerships with nonbank financial firms, particularly smaller, less-mature companies with innovative technologies that do not present a material risk to the bank. Treasury believes it is important to encourage the partnership model to promote innovation. Further, Treasury makes recommendations regarding changes to permissible activities, including bank activities related to acquiring or investing in nonbank platforms.

### **Updating Activity-Specific Regulations**

This report surveys a wide range of activities where specific recommendations for regulatory reform are suggested. The range of financial services includes:

#### **Marketplace Lending**

Marketplace lenders are expanding access to credit for consumers and businesses in the United States. Treasury recognizes that partnerships between banks and marketplace lenders have been valuable to enhance the capabilities of mature financial firms. Treasury recommends eliminating constraints brought about by recent court cases that would unnecessarily limit the functioning of U.S. credit markets. Congress should codify the “valid when made” doctrine and the role of the bank as the “true lender” of loans it makes. Federal banking regulators should also use their available authorities to address both of these challenges.

#### **Mortgage Lending and Servicing**

Treasury recognizes that the primary residential mortgage market has experienced a fundamental shift in composition since the financial crisis, as traditional deposit-based lender-servicers have ceded sizable market share to nonbank financial firms, with the latter now accounting for approximately half of new originations. Some of this shift has been driven by the post-crisis regulatory environment, including enforcement actions brought under the False Claims Act for violations related to government loan insurance programs. Additionally, many nonbank lenders have benefitted from early adoption of financial technology innovations that speed up and simplify loan application and approval at the front-end of the mortgage origination process. Policymakers should address regulatory challenges that discourage broad primary market participation and inhibit the adoption of technological developments with the potential to improve the customer experience, shorten origination timelines, facilitate efficient loss mitigation, and generally deliver a more reliable, lower cost mortgage product.

#### **Student Lending and Servicing**

The federal student loan program represents more than 90% of outstanding student loan volume and is managed by an extensive network of nonbanks for servicing and debt collection. The program is complex due to a variety of loan types, repayment plans, and product features that make the program difficult for borrowers to navigate and increase the difficulty and cost of servicing. Treasury recommends that the U.S. Department of Education establish and publish minimum effective servicing standards to provide servicers clear guidelines for servicing and help set expectations about how the servicing of federal loans is regulated. Treasury provides recommendations related to the greater use of technology in communications with borrowers, enhanced portfolio



performance monitoring and management by Education, and greater institutional accountability for schools participating in the federal financial aid programs.

### **Short-Term, Small-Dollar Lending**

While the demand for short-term, small-dollar loans is high, lenders have been constrained by unnecessary regulatory guidance at the federal level. Treasury recommends that the Bureau of Consumer Financial Protection (Bureau) rescind its Payday Rule, which applies to nonbank short-term, small-dollar lenders, as the states already maintain the necessary regulatory authorities and the rule would further restrict consumer access to credit. Treasury also recommends that both federal and state banking regulators take steps to encourage prudent and sustainable short-term, small-dollar installment lending by banks.

### **Debt Collection**

Debt collectors and debt buyers play an important role in minimizing losses in consumer credit markets, thereby allowing for increased availability of and lower priced credit to consumers. A variety of stakeholders have expressed concerns about the adequacy of loan information provided when a loan is sold or transferred for collection. When debt collectors and buyers do not receive adequate information, they are unable to demonstrate to the consumer that the debt is valid and owed. Treasury recommends the Bureau establish minimum effective federal standards for third-party debt collectors, including standards for the information that must be transferred with the debt for purposes of third-party collection or sale.

### **New Credit Models and Data**

A growing number of firms have begun to use or explore a wide range of newer data sets or advanced algorithms, including machine learning-based methods, to support credit underwriting decisions. Treasury recognizes that these new credit models and data sources have the potential to meaningfully expand access to credit and the quality of financial services, and therefore recommends that financial regulators further enable their testing. In particular, regulators should provide regulatory clarity for the use of new data and modeling approaches that are generally recognized as providing predictive value consistent with applicable law for use in credit decisions.

### **Credit Bureaus**

The consumer credit bureaus collect sensitive information on millions of Americans, and thus are required to protect the information they collect. While the credit bureaus are subject to state and federal regulation for consumer protection purposes, and have been subject to state and federal enforcement actions related to data security, they are not routinely supervised for compliance with the federal data security requirements of the Gramm-Leach-Bliley Act. Treasury recommends that the relevant agencies use appropriate authorities to coordinate regulatory actions to protect consumer data held by credit reporting agencies and that Congress continue to assess whether further authority is needed in this area. Treasury also recommends that Congress amend the Credit Repair Organizations Act to exclude national credit bureaus and national credit scorers in order to allow these entities to provide credit education and counseling services to consumers to prospectively improve their credit scores.

### **IRS Income Verification**

The Internal Revenue Service (IRS) system that lenders and vendors use to obtain borrower tax transcripts is outdated and should be modernized in order to minimize delays in accessing tax information, which would facilitate the consumer and small business credit origination process. In other data aggregation situations, such as gathering borrower bank balances, lenders generally are able to obtain the needed borrower financial information through an application programming interface (API) to instantaneously and safely transfer data. The IRS's current technology should be updated to accommodate lender access of borrower information to instantaneously and safely transfer data, comparable to similar private sector solutions. While the IRS is working to update its technology more broadly, these efforts would benefit from additional funding, which would facilitate upgrades to support more efficient income verification, bringing a critical component of the credit process up to speed with broader innovations in financial technology.

### **Payments**

Treasury recommends that the states work to harmonize money transmitter requirements for licensing and supervisory examinations, and urges the Bureau to provide more flexibility regarding the issuance of remittance disclosures. Treasury encourages the Federal Reserve to move quickly in facilitating a faster retail payments system, such as through the development of a real-time settlement service that would allow for more efficient and widespread access to innovative payment capabilities. Such a system should take into account the ability of smaller financial institutions, such as community banks and credit unions, to access innovative technologies and payment services.

### **Wealth Management and Digital Financial Planning**

Digital financial planning tools can expand access to advice for Americans to accumulate sufficient wealth, particularly as individuals have become more responsible for their own retirement planning. Under the current regulatory structure, financial planners may be regulated at both the federal and state levels. Although many financial planners are regulated by the Securities and Exchange Commission or state securities regulators, they may also be subject to regulation by the Department of Labor, the Bureau, federal or state banking regulators, state insurance commissioners, state boards of accountancy, and state bars. This patchwork of regulatory authority increases costs and potentially presents unnecessary barriers to the development of digital financial planning services. Treasury recommends that an appropriate existing regulator of a financial planner be tasked with primary oversight of that financial planner and other regulators defer to that regulator.

### **Regulating a 21st Century Economy**

Treasury advocates an agile approach to regulation that can evolve with innovation. It is critical not to allow fragmentation in the financial regulatory system, at both the federal and state level, to interfere with innovation. Financial regulators must consider new approaches to effectively promote innovation, including permitting meaningful experimentation by financial services firms to create innovative products, services, and processes.

Internationally, many countries have established “innovation facilitators” and various regulatory “sandboxes” — testing grounds for innovation. These sandboxes have each generally supported common principles, such as promoting the adoption and growth of innovation in financial services,

providing access to companies in various stages of the business lifecycle, providing varying degrees of regulatory relief while maintaining consumer protections, and improving the timeliness of regulator feedback offered throughout the development lifecycle. While replicating this approach in the United States is complicated by the fragmentation of our financial regulatory system, Treasury is committed to working with federal and state financial regulators to establish a unified solution that accomplishes these objectives — in essence, a regulatory sandbox.

The ability of regulators to engage with the private sector to test and understand new technologies and innovations as they arise is equally important. Treasury recommends that Congress pass legislation authorizing financial regulators to use other transaction authority for research and development and proof of concept technology projects. Treasury encourages financial regulators to pursue robust engagement efforts with industry and establish clear points of contact for outreach to enable the symbiotic relationship necessary to maintaining U.S. global competitiveness.

Treasury will work to ensure actions taken by international organizations align with U.S. national interests and the domestic priorities of U.S. regulatory authorities. This should include a focus on the needs of U.S. companies that operate on a global basis. Participation by the relevant experts in international forums and standard-setting bodies is important to share experiences regarding respective regulatory approaches and to benefit from lessons learned.

### **A Bright Future for Innovation**

The United States is the global leader in technological innovation. The pace of technological development in financial services has increased exponentially, offering potential benefits to the U.S. economy. Treasury encourages all financial regulators to stay abreast of developments in technology and to properly tailor regulations in a manner that does not constrain innovation. Regulators must be more agile than in the past in order to fulfill their statutory responsibilities without creating unnecessary barriers to innovation. Ensuring a bright future for financial innovation, regulators should take meaningful steps to facilitate and enhance the nation's strength in technology and work toward the common goals of fostering vibrant financial markets and promoting growth through responsible innovation.

# **Embracing Digitization, Data, and Technology**



## Overview

The cost of collecting, transmitting, and storing vast amounts of data has sharply declined over the last 20 years, which has driven a technological revolution in many industries. Related technologies built on top of this increased ability to collect and manage data, like machine learning and artificial intelligence, have enabled a wide range of practical applications, many of which are relevant to the financial services industry. The combination of digitization, data, and technology can promote economic growth, increase consumer satisfaction, and improve choice, opportunity, and economic inclusion for all Americans. These factors also stimulate innovation, increase competition, and enhance the global competitiveness of the United States.

Key upgrades to the regulatory system are needed to enable the financial system to realize the benefits of economy-wide advances in these new technologies, including updating rules for financial services in the digital economy, assuring the existence of secure and open access to financial data, and aligning requirements for core infrastructure and competitive technologies. In each instance, there is a significant role for both the public and private sector — in fact, collaboration between the two is essential. Likewise, many regulations were adopted in and for a very different era, requiring a focus on modernization and appropriate tailoring that is consistent with the Core Principles.

## Digitization

The transformation of business into the digital era has had a profound impact on innovation and economic growth. Converting information into digital form made it possible for data to be electronically stored, transmitted, and analyzed. As the costs of storing and processing data have decreased, the amounts of data collected and retained have correspondingly increased. When combined with developments in communication and networking, the modern economy exists in a digital environment that allows near-instantaneous access to significant volumes of information. Ensuring this data is used in a manner that safely creates new products and services with positive effects on the economy and society is an important national objective.

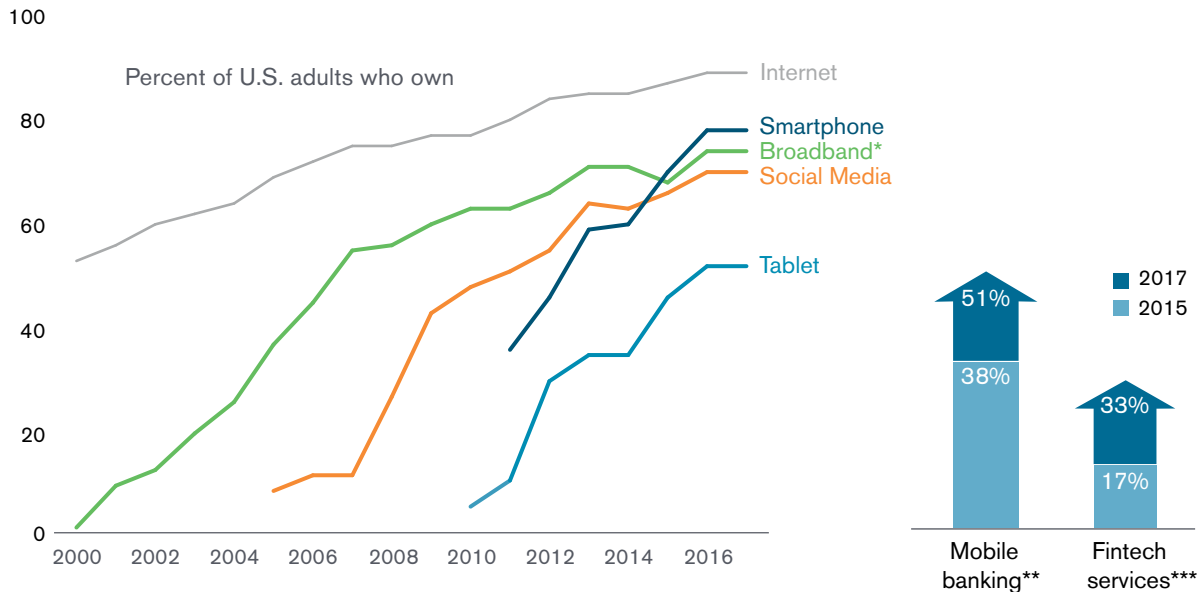
The key driver of this digital business environment is the increasingly widespread use of digital devices by Americans. Consider that nearly 90% of U.S. adults are online.<sup>16</sup> Moreover, 77% own a mobile phone with advanced digital capabilities, 53% own a tablet, and 46% have used digital voice assistants.<sup>17</sup> Most Americans use a combination of phone calls, text messages, and e-mails to manage their business and personal relationships. As a result, Americans' digital addresses (e.g., e-mail, device, chat ID) have increasingly become the equivalent of what a physical mailing address or telephone landline was in the past — the most effective way to reach a person for a business purpose.

---

16. Pew Research Center, *Internet/Broadband Fact Sheet* (Feb. 5, 2018), available at: <http://www.pewinternet.org/fact-sheet/internet-broadband/>.

17. Kenneth Olmstead, Pew Research Center, *Nearly Half of Americans Use Digital Voice Assistants, Mostly on their Smartphones* (Dec. 12, 2017), available at: <http://www.pewresearch.org/fact-tank/2017/12/12/nearly-half-of-americans-use-digital-voice-assistants-mostly-on-their-smartphones/>; Pew Research Center, *Mobile Fact Sheet* (Feb. 5, 2018), available at: <http://www.pewinternet.org/fact-sheet/mobile/>.

Figure 1: Technology Adoption and Usage



\* used at home.

\*\* as a percentage of survey respondents that have a bank account.

\*\*\* as a percentage of survey respondents that are active online.

Source (left): Chart and data recreated from Pew Research Center analysis.

Sources (right): For mobile banking data, Federal Reserve analysis of Survey of Household Economics and Decisionmaking and Survey of Consumers' Use of Mobile Financial Services.

For fintech services growth, see Ernst and Young, *EY FinTech Adoption Index 2017*, at 13.

Financial institutions and technology-focused firms have recognized this shift in where consumers “reside” and have consequently been transforming their business activities to meet customers’ demand for digital interaction where possible. Consumers are rapidly adopting services provided by new fintech companies. Survey data indicate that up to one-third of online U.S. consumers use at least two fintech services — including financial planning, savings and investment, online borrowing, or some form of money transfer and payment.<sup>18</sup>

Banking is also increasingly digital. Today, 50% of people with bank accounts use mobile devices to access their information, up from 20% in 2011,<sup>19</sup> while the number of physical bank branches

18. Ernst & Young Global Limited, *EY FinTech Adoption Index 2017: The Rapid Emergence of FinTech* (2017), available at: <https://www.ey.com/Publication/vwLUAssets/ey-fintech-adoption-index-2017/%24FILE/ey-fintech-adoption-index-2017.pdf>.

19. Ellen A. Merry, Board of Governors of the Federal Reserve System, *Mobile Banking: A Closer Look at Survey Measures*, FEDS Notes (Mar. 27, 2018), available at: <https://doi.org/10.17016/2380-7172.2163>.

has been declining since 2009.<sup>20</sup> U.S. banks of all sizes are enabling digital engagement with their customers and are increasingly offering mobile phone applications that provide for a full suite of banking services, among other efforts.

This digital transformation of the economy and financial services requires wide-ranging changes to the U.S. regulatory system. For example, there is a need to modernize regulations for digitally communicating with consumers. Other regulations that should be implemented are discussed throughout this report and include: updating regulations to better facilitate secure access to digitized data, authentication of digital identity, and support for core financial service activities such as lending, payments, and investment advice.

## Digital Communications

### **Telephone Consumer Protection Act**

In 1991, Congress passed the Telephone Consumer Protection Act (TCPA) to restrict telemarketing calls and the use of automatic telephone dialing systems (autodialers) and prerecorded voice messages.<sup>21</sup> The Federal Communications Commission (FCC) is responsible for rules implementing the TCPA. Among the restrictions, the TCPA forbids telemarketers from calling a cell phone using an autodialer without first obtaining prior express consent of the called party.<sup>22</sup> However, current implementation of the TCPA constrains the ability of financial services firms to use digital communication channels to communicate with their customers despite consumers' increasing reliance on text messaging and e-mail communications through their mobile devices.

In 2015, the FCC issued an order responding to 21 requests for clarification or amendment to the FCC's TCPA rules and orders.<sup>23</sup> Financial services firms raised three primary concerns with the FCC's 2015 order. First, the definition of autodialer was overly broad because it included the capacity to make an autodialed call, as opposed to the actual use of the equipment as an autodialer. Second, by only providing a one-call safe harbor, which permitted a caller only a single call to determine whether a phone number was reassigned, the FCC order exposed firms to significant liability — up to a \$500-per-call penalty — for dialing reassigned numbers, even when one call was insufficient to permit the firm to learn that the number was reassigned. Third, the order permitted consumers to revoke consent “using any reasonable method,” and prohibited callers from “infring[ing] on that ability by designating an exclusive means to revoke.”<sup>24</sup> Regarding revocation, firms asked for clear guidance detailing reasonable methods of revocation given the TCPA's penalties for noncompliance.

20. Julie Stackhouse, Federal Reserve Bank of St. Louis, *Why Are Banks Shuttering Branches?*, On the Economy Blog (Feb. 26, 2018), available at: <https://www.stlouisfed.org/on-the-economy/2018/february/why-banks-shuttering-branches>.

21. Public Law No. 102-243 [codified at 47 U.S.C. § 227].

22. 47 U.S.C. § 227(b)(1)(A).

23. See Federal Communications Commission, In the Matter Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 et al., *Declaratory Rule and Order*, CG Docket No. 02-278 (June 18, 2015), available at: [https://apps.fcc.gov/edocs\\_public/attachmatch/FCC-15-72A1\\_Rcd.pdf](https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-72A1_Rcd.pdf) (“FCC 2015 Order”).

24. *Id.* at 7996.



On March 16, 2018, the U.S. Court of Appeals for the D.C. Circuit ruled on these three issues in a case brought against the FCC by ACA International, a trade group representing debt collectors.<sup>25</sup> First, the D.C. Circuit held that the FCC’s definition of autodialer was arbitrary and capricious because, under the FCC’s definition, “all smartphones qualify as autodialers because they have the inherent ‘capacity’ to gain [autodialer] functionality by downloading an app.”<sup>26</sup> Second, the Court held that the one-call safe harbor was arbitrary and capricious because the FCC failed to explain why a “caller’s reasonable reliance on a previous subscriber’s consent necessarily cease[s] to be reasonable once there has been a single, post-reassignment call.”<sup>27</sup> Third, the Court upheld the FCC’s use of a “reasonable means” standard for revocation of consent but left open the possibility of different “revocation rules mutually adopted by contracting parties.”<sup>28</sup>

After the D.C. Circuit’s decision, the FCC reconsidered how the TCPA applies to reassigned numbers, issuing a proposed rule on preventing unwanted calls to reassigned numbers and seeking comment on methods to establish a reassigned numbers database.<sup>29</sup> A reassigned numbers database — long supported by market participants and consumer advocates — could reduce unwanted calls to consumers and reduce caller liability by permitting callers to conduct due diligence to learn whether a number has been recently reassigned and, if it has, remove that number from their autodialed calls.<sup>30</sup>

### **Fair Debt Collection Practices Act**

Congress enacted the Fair Debt Collection Practices Act (FDCPA), in part, to “eliminate abusive debt collection practices by debt collectors.”<sup>31</sup> The responsibility of enforcement is shared by the Bureau of Consumer Financial Protection (the Bureau) and the Federal Trade Commission (FTC).<sup>32</sup> However, current implementation of the FDCPA may inadvertently make interactions between debt collectors and consumers needlessly cumbersome. The FDCPA prohibits debt collectors from disclosing information about a consumer’s debt to unauthorized third parties and allows consumers to terminate communication about the debt.<sup>33</sup> While using e-mail or voicemail to communicate with a consumer about his or her debt is permissible under FDCPA, potential litigation risk can arise if the debt collector inadvertently discloses information regarding the debt to an unauthorized third party while using contact information provided by the borrower. As a result, even if consumers increasingly prefer to communicate digitally, such as via text messages and e-mail, litigation risk can discourage debt collectors from doing so.

25. *ACA International v. FCC*, 885 F.3d 687 (D.C. Cir. 2018).

26. *Id.* at 700.

27. *Id.* at 707.

28. *Id.* at 709-10.

29. Advanced Methods to Target and Eliminate Unlawful Robocalls (Apr. 20, 2018) [83 Fed. Reg. 17631 (Apr. 23, 2018)].

30. *Id.*

31. 15 U.S.C. § 1692(e).

32. *Id.* § 1692i; see also Bureau of Consumer Financial Protection, *Fair Debt Collection Practices Act: Annual Report 2018* (Mar. 2018), at 7, available at: [https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb\\_fdcpa\\_annual-report-congress\\_03-2018.pdf](https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_fdcpa_annual-report-congress_03-2018.pdf).

33. 15 U.S.C. § 1692c(b).



*Recommendations*

Treasury recognizes that the increasingly digitized nature of the economy and financial system requires revisiting of customer communication and disclosure rules that were designed primarily for an era of physical mail and telephone calls. Treasury has identified some opportunities for reform of the TCPA and FDCPA regulatory regimes but recommends that regulators proactively identify other rules in need of revision.

Treasury recommends that the FCC continue its efforts to address the issue of unwanted calls through the creation of a reassigned numbers database. Treasury recommends that the FCC create a safe harbor for calls to reassigned numbers that provides callers a sufficient opportunity to learn that the number has been reassigned.

In addition, Treasury recommends that the FCC provide clear guidance on reasonable methods for consumers to revoke consent under the TCPA.

Additionally, Congress should consider statutory changes to the TCPA to mitigate unwanted calls to consumers and provide for a revocation standard similar to that provided under the FDCPA.

Treasury also recommends that the Bureau promulgate regulations under the FDCPA to codify that reasonable digital communications, especially when they reflect a consumer's preferred method, are appropriate for use in debt collection.

### Closing the Digital Divide

“Digital divide” describes the gap between populations that have access to modern information and communication technology and those that have no or limited access. The FCC estimates 30% of people living in rural America lack access to broadband compared to 2.1% of people in urban areas, which means that nearly 24 million rural Americans cannot fully access the benefits of the digital economy.<sup>34</sup> Access to the digital economy allows Americans to benefit from the rapid growth of technology and innovation.

Broadband access has become increasingly important for economic opportunity, job creation, education, and civic engagement. Rural communities have made large gains in adopting technology, but substantial segments of rural America still lack the infrastructure needed for high-speed internet, and any access that rural areas have is often slower than that of non-rural areas.<sup>35</sup> In February 2017, the FCC took action designed to expand and preserve mobile coverage across rural America and in tribal lands.<sup>36</sup> The FCC stated that the next stages of the

34. Federal Communications Commission, *2018 Broadband Deployment Report* (Feb. 2, 2018), available at: [https://apps.fcc.gov/edocs\\_public/attachmatch/FCC-18-10A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/FCC-18-10A1.pdf).
35. Andrew Perrin, Pew Research Center, *Digital Gap Between Rural and Nonrural America Persists*, blog post (May 19, 2017), available at: <http://www.pewresearch.org/fact-tank/2017/05/19/digital-gap-between-rural-and-nonrural-america-persists/>.
36. Federal Communications Commission, *In the Matter of Connect America Fund Universal Service Reform – Mobility Fund, Report and Order and Further Notice of Proposed Rulemaking* (Feb. 23, 2017), available at: [https://apps.fcc.gov/edocs\\_public/attachmatch/FCC-17-11A1\\_Rcd.pdf](https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-11A1_Rcd.pdf).

Connect America Fund<sup>37</sup> will be implemented and will provide additional funding for rural fixed broadband over the next decade.<sup>38</sup>

Additional support for these efforts is reflected in Executive Order 13821, which states that “it shall therefore be the policy of the executive branch to use all viable tools to accelerate the deployment and adoption of affordable, reliable, modern, high-speed broadband connectivity in rural America.”<sup>39</sup> Concurrently, the President instructed the Secretary of the Interior to develop a plan to increase access to tower facilities and other infrastructure managed by the Department of the Interior in rural America for broadband deployment.<sup>40</sup>

Deployment of more infrastructure to support broadband in rural areas will help to close the digital divide and assist more Americans in underserved communities to participate in the digital economy and overcome geographic isolation.

## Consumer Financial Data

As a result of digitization, vast amounts of data now exist in forms that can be readily aggregated and analyzed with computing power. Online and mobile applications that draw on these data make it possible for consumers to view banking and other financial account information, often held at different financial institutions, on a single platform, monitor the performance of their investments in real-time, compare financial and investment products, and even make payments or execute transactions. Applications can also assist with automatic savings, budget advice, credit decisions, and fraud and identity theft detection in real-time.<sup>41</sup>

In short, digitized record-keeping and these applications have exponentially improved a consumer’s ability to make financial decisions. It has given rise to a new sector of nonbank financial institutions focused on products and services utilizing data aggregation, based on data obtained with the consumer’s consent. The rise of such financial institutions presents questions regarding the way in which they operate and are currently regulated.

37. The Connect America Fund, also known as the Universal Service High-Cost Fund, is the FCC’s program to expand voice and broadband services for areas where they are unavailable.

38. Federal Communications Commission, *Connect America Fund Phase II Auction Scheduled for July 24, 2018 - Notice and Filing Requirements and Other Procedures for Auction 903* (Feb. 1, 2018), available at: [https://apps.fcc.gov/edocs\\_public/attachmatch/FCC-18-6A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/FCC-18-6A1.pdf).

39. Executive Order 13821, *Streamlining and Expediting Requests to Locate Broadband Facilities in Rural America* (Jan. 8, 2018) [83 Fed. Reg. 1507 (Jan. 11, 2018)].

40. Executive Office of the President, *Supporting Broadband Tower Facilities in Rural America on Federal Properties Managed by the Department of the Interior* (Jan. 8, 2018) [83 Fed. Reg. 1511 (Jan. 12, 2018)].

41. See Letter from the Center for Financial Services Innovation to the Bureau of Consumer Financial Protection, *CFPB-2016-0048 Request for Information Regarding Consumer Access to Financial Records* (Feb. 21, 2017), available at: <https://www.regulations.gov/document?D=CFPB-2016-0048-0047>.

## Data Aggregation

Data aggregation generally refers to any process in which information from one or more sources is compiled and standardized into a summary form.<sup>42</sup> Often data are aggregated for specific business or research purposes such as statistical analysis, performance tracking, or recordkeeping. As of the end of June 2018, five of the largest publicly-traded U.S. companies by market capitalization are integral drivers of the digital economy and use data aggregation for telecommunications, logistics, marketing, social media, and other purposes.<sup>43</sup>

### How Data Aggregation Works

At the most basic level, data aggregation in the financial services sector necessarily involves consumers, financial services firms, data aggregators, and consumer financial technology (fintech) application providers. “Consumers” are the individuals who are users of financial services and the principal providers of the information collected by financial service companies. In the consumer financial services data aggregation framework, consumers decide which applications to use in order to access their data, give consent for that access, and provide necessary authentication (i.e., login) information.

“Financial services companies” or “financial services firms” include banks, mutual funds, insurance companies, broker-dealers, wealth management firms, and other financial institutions that provide traditional retail banking, depository, credit, brokerage, investment, and other account management services to consumers. These companies are the sources of consumer financial account and transaction data.

“Data aggregators” are the firms that access, aggregate, share, and store consumer financial account and transaction data they acquire through connections to financial services companies. Aggregators are intermediaries between the fintech applications that consumers use to access their data, on the one hand, and the sources of data at financial services companies on the other. An aggregator may be a generic provider of data to consumer fintech application providers and other third parties, or it may be part of a company providing branded and direct services to consumers.

Finally, “consumer fintech application providers” are the firms that access consumer financial account and transaction data, either from data aggregators or financial services companies, in order to provide value-added products and services to consumers. Consumers access these services through “fintech applications” — i.e., the websites or mobile apps — created by these firms. Consumer fintech application providers may also have direct links to financial services companies in order to, for example, provide direct services to a bank’s customers, access payments systems, or facilitate credit origination.

Operationally, the key data aggregation processes involve acquiring, compiling, standardizing, and disseminating consumer financial data. Data aggregators may differ in the breadth and sophistication of the aggregation services they offer, and may specialize in different types of data or target a

42. See also Request for Information Regarding Consumer Access to Financial Records (Nov. 14, 2016) [81 Fed. Reg. 83806, 83808-09 (Nov. 22, 2016)] (“Data Aggregation RFI”).

43. These companies are Apple, Amazon, Alphabet [Google], Microsoft, and Facebook, based on Treasury analysis of Bloomberg data.

Figure 2: Participants in the Consumer Financial Services Data Aggregation Framework

Participant	Description	Role
<b>Consumers</b>	<ul style="list-style-type: none"> <li>Individuals</li> </ul>	<ul style="list-style-type: none"> <li>Choose which fintech applications serve needs</li> <li>Accept terms and conditions</li> <li>Give consent for data sharing</li> <li>Provide login credentials or other information for authentication</li> </ul>
<b>Data aggregators</b>	<ul style="list-style-type: none"> <li>Firms that aggregate consumer financial data to share with other third-parties, e.g. consumer fintech application providers</li> <li>Firms that aggregate consumer financial data to provide branded and direct services to consumers</li> </ul>	<ul style="list-style-type: none"> <li>Compile consumer financial account and transaction data obtained (1) through consumer-provided credentials (e.g., screen-scraping) and/or (2) through authorized connections with financial services companies (e.g., APIs)</li> <li>Provide data to consumer fintech application providers and other third-parties</li> <li>May develop own fintech applications</li> <li>Often invisible to consumers</li> </ul>
<b>Consumer fintech application providers</b>	<ul style="list-style-type: none"> <li>Third-party firms offering value-added financial products and services to consumers</li> </ul>	<ul style="list-style-type: none"> <li>Create and market fintech applications for consumers</li> <li>Frequently rely on data from aggregators to run applications</li> <li>Applications enable consumers to monitor accounts, track budget and financial goals, pay bills, make peer-to-peer payments, take out loans, receive investment advice, etc.</li> </ul>
<b>Financial services companies</b>	<ul style="list-style-type: none"> <li>Retail banks and other depository institutions</li> <li>Retail broker-dealers</li> <li>Mutual fund companies</li> <li>Wealth management firms</li> <li>Insurance companies</li> <li>Other traditional financial institutions</li> </ul>	<ul style="list-style-type: none"> <li>Provide traditional banking, investment, insurance and other financial services to consumers</li> <li>Sources of consumer financial account and transaction data</li> <li>Data may be accessed directly (e.g., APIs) or indirectly (e.g., screen-scraping)</li> </ul>

Source: Treasury staff analysis.

specific developer base.<sup>44</sup> Some data aggregators may focus on aggregating financial account balances, transactions data, or credit card activity, for example, or they may primarily support consumer fintech application providers geared toward offering specific products (such as auto loans or mortgages) or services (such as peer-to-peer payments or budget tracking).

44. For an account of the evolution of data aggregation services, see Michael Kitces, *The Six Levels of Account Aggregation #FinTech and PFM Portals for Financial Advisors*, blog post (Oct. 9, 2017), available at: <https://www.kitces.com/blog/six-levels-account-aggregation-pfm-fintech-solutions-accounts-advice-automation/>.

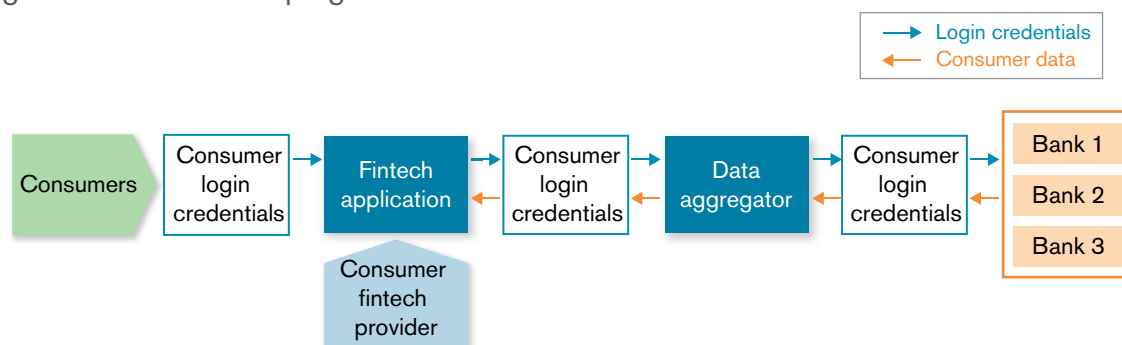
In general, data aggregators make data available by providing a platform on or through which consumer fintech application providers can build and run their applications and provide an interface with consumers. Because data aggregators are few in number compared to financial services companies — a relative handful versus thousands — and because they have generally sunk the costs of connecting to financial services companies, consumer fintech application providers only have to “build” to the data aggregators’ specifications and not to hundreds or thousands of platforms run by individual financial institutions.<sup>45</sup>

Before these processes and interfaces can commence, however, a data aggregator requires access to consumers’ data housed at financial services companies. At present, there are two primary methods through which data aggregators gain access to consumer financial data: “screen-scraping” and application programming interfaces (APIs).

### Screen-Scraping

When data aggregators and consumer fintech application providers lack a direct connection to run fintech applications using data housed at financial services companies, they often rely on screen-scraping. In screen-scraping, consumers provide their account login credentials — usernames and passwords — in order to use the fintech application.<sup>46</sup> Consumers may or may not appreciate that they are providing their credentials to a third-party, and not logging in directly to their financial services company. Using these login credentials, data aggregators access consumers’ financial

Figure 3: Screen-Scraping



Source: Treasury staff analysis.

45. By one data aggregator’s account, there are eight major aggregators of consumer-authorized data in the United States. See MX Technologies Inc., *A List of Financial Data Aggregators in the United States*, blog post (Mar. 5, 2018), available at: <https://www.mx.com/moneysummit/a-list-of-financial-data-aggregators-in-the-united-states>. The listed data aggregators were Intuit, Quovo, Plaid, Envestnet/Yodlee, Morningstar/ByAllAccounts, Fiserv/CashEdge, Finicity, and MX.
46. Screen-scraping is not a recent development. As far back as 2001, regulators identified the practice of sharing consumer login credentials for data aggregation services as raising additional risks. See Office of the Comptroller of the Currency, *Bank-Provided Account Aggregation Services*, OCC Bulletin 2001-12 (Feb. 28, 2001), available at: <https://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-12.html>; Federal Financial Institutions Examination Council, *E-Banking*, IT Examination Handbook (Aug. 2003), at App. D, available at: [https://ithandbook.ffiec.gov/media/274777/ffiec\\_itbooklet\\_e-banking.pdf](https://ithandbook.ffiec.gov/media/274777/ffiec_itbooklet_e-banking.pdf).

accounts, and then, either manually or through specialized software, acquire the financial account and transaction data and even process data requests or execute transactions. Equally concerning, financial services companies are not always aware when screen-scraping methods are being used to access their customers' data.

Although screen-scraping can be an effective method of obtaining data, it is generally considered to have certain vulnerabilities and drawbacks. Many of the risks and concerns associated with data aggregation described in this report — whether for consumers, financial services companies, consumer fintech application providers, or data aggregators themselves — stem from the practice of screen-scraping.

### Application Programming Interfaces

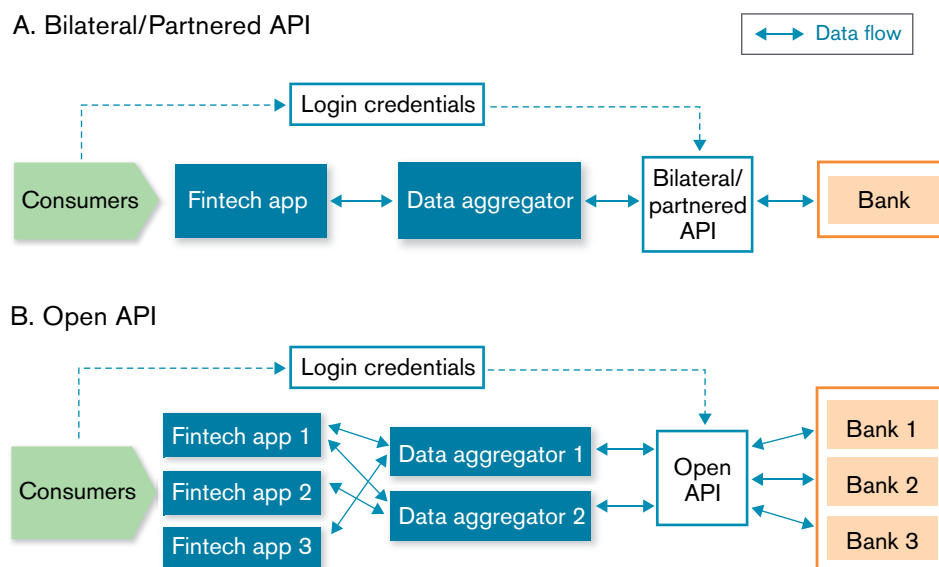
The second method of accessing consumer financial account and transaction data is through an API or similar form of direct feed. For purposes of this report, an API can be loosely described as a clearly specified program that links two or more systems and that enables a well-defined communication and data exchange between them in order to run applications and other software. An API is not a specific technology, but rather a technology-enabled agreement or protocol that enables a computer system or source of data to interact with or be used by other software.<sup>47</sup> Unlike in the case of screen-scraping, data aggregation through an API generally means that financial services companies are knowingly participating in the sharing of data. As such, financial services companies can potentially deploy APIs that allow for the inclusion of robust security features, greater transparency and access controls for consumers, improved data accuracy, and more predictable and manageable information technology costs. APIs, however, cost money to develop, which could raise particular hurdles for smaller financial institutions with fewer information technology resources.

APIs may be designed to be open or they may be restricted to selected partners. In an open API, any third-party data aggregator or consumer fintech application provider that meets certain predetermined and published standards (e.g., security, licensing, etc.) can gain access to consumer data and build consumer-facing applications. In contrast, partnered APIs entail bilateral and exclusive agreements between financial services companies and data aggregators or consumer fintech application providers. In either case, the API method of access is generally enabled through consumer consent provided to the financial services company or at the API access point rather than through giving consumer login credentials to third-parties.

---

47. To illustrate how this works, think for example of nearly any app or website — for example, for ride-sharing services, retail stores, special events, etc. — that includes a map or the ability to provide point-to-point (or turn-by-turn) directions. These apps and websites generally do not create their own maps and navigation software. Instead, they would incorporate the maps and navigation software of an internet-based provider that specializes in aggregating mapping and navigation data. This provider makes its mapping and navigation products available for use by third-parties by establishing an API that includes instructions, tools, and other resources that enable software developers to incorporate such products into their own apps and websites.

Figure 4: Application Programming Interfaces (API)



Source: Treasury staff analysis.

### Efforts to Improve Data Aggregation

Data aggregators, consumer fintech application providers, and financial services companies generally agree that consumers should have secure and reliable access to their financial account and transaction data, and that, in principle, consumers, if they opt-in, should be able to utilize fintech applications and other innovations that make use of their data. However, there is a lack of consensus on what secure and reliable access entails. As described by one observer, “the U.S. debate seems stuck at the yet-to-be resolved issue of migrating account aggregators from screen scraping-based to more secure and efficient API-based data-sharing methodologies.”<sup>48</sup> As long as this impasse remains unresolved, consumers will be caught in the middle.

Consequently, data aggregators, consumer fintech application providers, and financial services companies in the United States are looking for better approaches to data aggregation. Despite the recognized advantages of using APIs as opposed to screen-scraping methods for data aggregation, current APIs have their limitations. Some data aggregators have entered into bilateral agreements to obtain data through an API, but this approach can be difficult to scale given the large number of U.S. financial services companies. In addition, data aggregators told Treasury that access through APIs was frequently and

48. Bob Hedges, The Clearing House, *Banking Perspectives: Consumer Data in an API-Enabled World* (4th Qtr. 2017), available at: <https://www.theclearinghouse.org/banking-perspectives/2017/2017-q4-banking-perspectives/articles/open-banking>.



unilaterally restricted, interrupted, or terminated by financial services companies.<sup>49</sup> Hence, Treasury's understanding is that a significant amount of data is still obtained through screen-scraping.

Much of the focus is on improving API methods to resolve issues such as standardizing data elements and fair and proportional allocation of liability and accountability in the event of a data breach. In some cases, participants from across the data aggregation framework are collaborating to develop robust open APIs that serve the needs of all stakeholders.<sup>50</sup> Further, trade groups are also starting to solidify views and have developed principles with respect to data aggregation.<sup>51</sup>

### Open Banking in the United Kingdom

In considering regulatory approaches for data aggregation, the efforts in other countries that have created their own regulatory regimes for consumer access to financial account and transaction data can provide a useful comparison point. In August 2016, the United Kingdom's Competition and Markets Authority (CMA) issued a report, which concluded that the market for retail banking was not sufficiently competitive and was dominated by large banks. The CMA outlined a package of remedies called Open Banking, which required the nine largest U.K. banks to adopt "open API banking standards... [and] to make data available using these standards."<sup>52</sup> Other banks can opt-in on a voluntary basis.

49. See also Robin Sidel, *Big Banks Lock Horns with Personal-Finance Web Portals*, The Wall Street Journal (Nov. 4, 2015).
50. One such effort is being carried out through the OFX Consortium, the origins of which date back to 1997. The OFX specification is one of original standards for the exchange of financial information between consumers and financial services providers. In April 2016, the OFX Consortium released OFX 2.2, which introduced new standards including data tags and tokenized authentication solutions for sharing consumer financial data. See OFX Consortium, *OFX 2.2 Released with OAuth-Token based Authentication*, Business Wire (Apr. 7, 2016), available at: <https://www.businesswire.com/news/home/20160407006078/en/OFX-2.2-Released-OAuth-Token-based-Authentication>. A more recent effort is that of the Aggregation Services Working Group of the FS-ISAC. The Working Group, which consists of representatives from financial services companies, data aggregators, and fintech developers, recently issued the second version of its API for secure, tokenized data transfer. See Financial Services Information Sharing and Analysis Center, *Press Release – FS-ISAC Enables Safer Financial Data Sharing with API* (Feb. 13, 2018), available at: <https://www.fsisac.com/article/fs-isac-enables-safer-financial-data-sharing-api>.
51. See, e.g., Securities Industry and Financial Markets Association, *SIFMA Data Aggregation Principles* (Apr. 2018), available at: <https://www.sifma.org/wp-content/uploads/2018/04/sifma-Data-Aggregation-Principles.pdf>. The SIFMA principles affirm that consumers "may use third-parties to access their financial account data" and "such access should be safe and secure." See also Renee Hobbs, Envestnet|Yodlee, *Envestnet|Yodlee, Quovo and Morningstar ByAllAccounts: Statement of Joint Principles for Ensuring Consumer Access to Financial Data*, blog post (May 11, 2018), available at: <https://www.yodlee.com/blog/envestnet-yodlee-quovo-and-morningstar-byallaccounts-statement-of-joint-principles-for-ensuring-consumer-access-to-financial-data/>. These three data aggregators proposed a "Secure Open Data Access" framework, which includes the following four components: (1) consumers must be able to access their financial account data for purposes of using any legitimate application; (2) consumers must provide affirmative consent on the basis of clear and conspicuous disclosure regarding the use of their data; (3) all entities who handle consumer account information must adhere to best practices for security standards and implement traceability/transparency; and (4) the entity responsible for a consumer's financial loss must make the consumer whole.
52. See Competition and Markets Authority, *Retail Banking Market Investigation: Final Report* (Aug. 9, 2016), at 441-461, available at: <https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf>.



These remedies are aimed at increasing competition, including lowering costs for consumers switching between financial institutions.

The first stage of Open Banking went live in March 2017, when the covered banks were required to make certain “open data” — i.e., public information such as the location of branches and automated teller machines as well as the terms of certain banking products — widely available online. The full Open Banking standard came into effect in January 2018. The CMA established the nonprofit Open Banking Implementation Entity (OBIE) to work with banks and third-party fintech developers to help integrate with Open Banking and to test their products and services based on the data. Fintech developers enrolled in Open Banking must be regulated by the U.K. Financial Conduct Authority.<sup>53</sup>

Open Banking uses “read/write” APIs with standards and specifications defined by OBIE. To securely access and share data, the participating banks develop API “endpoints” on which fintech developers can build applications. The use of APIs permits consumers to retain full control over their account information. Consumers must give explicit consent before using any fintech applications and are redirected to their bank’s login screen to enter their login credentials. Consumers determine which information can be accessed, for how long and for what purpose, and can revoke their consent at any time. Shared data is encrypted and its usage is tracked, and only regulated persons can access it.

There are significant differences between the United States and the United Kingdom with respect to the size, nature, and diversity of the financial services sector and regulatory mandates. Given those differences, an equivalent Open Banking regime for the U.S. market is not readily applicable. Nonetheless, as Open Banking matures in the United Kingdom, U.S. financial regulators should observe developments and learn from the British experience.

### **Issues and Recommendations**

Consumers’ ability to realize the benefits of data aggregation is limited, in part due to the lack of agreement between data aggregators and financial services companies over access to consumer financial account and transaction data. However, Treasury recognizes that significant strides have been made in recent years to bridge these disagreements. As information and data technology advances, and with sustained commitment to the principle that consumers should be able to freely access and use their financial account and transaction data, Treasury believes that improved approaches to data aggregation that will benefit consumers and financial institutions alike are surely attainable.

### **Consumer Access to Financial Account and Transaction Data**

The only express statutory provision regarding access to a consumer’s own financial account and transaction data is Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank).<sup>54</sup> It states that, subject to rules prescribed by the Bureau, financial services

53. As of July 2018, there were 33 regulated third-party providers enrolled in Open Banking. See <https://www.openbanking.org.uk/regulated-providers/>.

54. Codified at 12 U.S.C. § 5533.

companies subject to the Bureau's jurisdiction as covered persons<sup>55</sup> are required to make available to a consumer, upon request, certain financial account and transaction data concerning any product or service obtained by the consumer from that financial services company.<sup>56</sup> This data must be made available in an electronic form usable by the consumer.<sup>57</sup>

In November 2016, the Bureau issued a request for information to better understand the benefits and risks associated with market developments that rely upon data aggregation.<sup>58</sup> Subsequently, the Bureau published nonbinding principles in October 2017 expressing a vision for a “robust, safe, and workable data aggregation market,”<sup>59</sup> although it noted that “few, if any, individual stakeholders” enumerated all of the consumer protection concerns presented in the principles.<sup>60</sup>

As described by the Bureau, financial data subject to consumer and consumer-authorized access may include any transaction, series of transactions, or other aspect of consumer usage, the terms of any account, such as a fee schedule, realized consumer costs, such as fees or interest paid, and realized consumer benefits, such as interest earned or rewards.<sup>61</sup> The principles underscore the role of companies that access consumers' financial data, with their permission, in order to provide services that hold the promise of “improved and innovative consumer financial products and services.”<sup>62</sup>

In addition to the Bureau, other groups have developed their own principles for data aggregation, including the Securities Industry and Financial Markets Association, the Consumer Financial Data Rights Coalition, and the Center for Financial Services Innovation.<sup>63</sup> While Treasury is not endorsing any particular set of principles, they contain common themes on topics such as security, access, and consumer consent, which can form the basis for consensus on consumer-authorized data aggregation.

55. Under Section 1002(6) of Dodd-Frank [12 U.S.C. § 5481(6)], a “covered person” is defined as “any person that engages in offering or providing a consumer financial product or service,” and any affiliate of such a person, if the affiliate acts as a service provider to that person. Notwithstanding the broad definition of “covered person,” other provisions place limits on the Bureau's jurisdiction for certain entities. See, e.g., 12 U.S.C. § 5517.

56. 12 U.S.C. § 5533(a). Section 1033, however, applies only to information that the covered person can retrieve in the ordinary course of its business with respect to that information. 12 U.S.C. § 5533(b)(4).

57. 12 U.S.C. § 5533(a).

58. Data Aggregation RFI.

59. Bureau of Consumer Financial Protection, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (Oct. 18, 2017), available at: [https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb\\_consumer-protection-principles\\_data-aggregation.pdf](https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf) (“Bureau Data Principles”).

60. Bureau of Consumer Financial Protection, *Consumer-Authorized Financial Data Sharing and Aggregation: Stakeholder Insights that Inform the Consumer Protection Principles* (Oct. 18, 2017), at 2, available at: [https://files.consumerfinance.gov/f/documents/cfpb\\_consumer-protection-principles\\_data-aggregation\\_stakeholder-insights.pdf](https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf) (“Bureau Stakeholder Insights”).

61. Bureau Data Principles, at 3.

62. *Id.* at 1.

63. See footnote 51. See also Center for Financial Services Innovation, *CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration* (Oct. 2016), available at: <https://s3.amazonaws.com/cfsi-innovation-files-2018/wp-content/uploads/2016/10/27001530/2016-Consumer-Data-Sharing-CDAWG-One-pager-Final-1.pdf>.

### Direct Consumer Access Versus Consumer-Authorized Access

In response to the Bureau’s request for information, conflicting views were expressed on whether data aggregators are covered by Section 1033.<sup>64</sup> Some financial services companies argued that access rights apply only to direct consumer access to their data but not to consumer-authorized access through a data aggregator or a fintech application. In contrast, consumer groups, data aggregators, and consumer fintech application providers asserted that consumers are entitled to access their financial account and transaction data via fintech applications.

The definition of “consumer” in Title X of Dodd-Frank includes not only an individual, but “an agent, trustee, or representative acting on behalf of an individual.”<sup>65</sup> This definition is best interpreted to cover circumstances in which consumers affirmatively authorize, with adequate disclosure, third parties such as data aggregators and consumer fintech application providers to access their financial account and transaction data from financial services companies. Otherwise, narrowly interpreting Section 1033 as applying only to direct consumer access would do little to advance consumer interests by eliminating many of the benefits they derive from data aggregation and the innovations that flow through from fintech applications.

#### *Recommendation*

Treasury recommends that the Bureau affirm that for purposes of Section 1033, third parties properly authorized by consumers, including data aggregators and consumer fintech application providers, fall within the definition of “consumer” under Section 1002(4) of Dodd-Frank for the purpose of obtaining access to financial account and transaction data.

### Entities Covered by Data Access Requirements

Section 1033 applies only to “covered persons” under Dodd-Frank, which includes a subset of financial services companies. Furthermore, the Bureau’s jurisdiction is subject to limitations for some financial services companies subject to regulation by other federal or state regulators, including: persons regulated by a state securities commission, to the extent that such persons act in a regulated capacity, or by the Securities and Exchange Commission (SEC);<sup>66</sup> persons regulated by the Department of Labor (DOL) that are offering 401(k) plans or employee benefit plans;<sup>67</sup> and persons regulated by state insurance regulators that are offering insurance products.<sup>68</sup>

Financial services companies primarily regulated by regulators other than the Bureau play important roles in the retirement savings plans of many Americans. While one approach is to expand the scope of Section 1033 to expressly include these companies, Treasury does not believe that step is necessary. Treasury has not identified evidence of market failure with respect to electronic access to data held by financial services companies not subject to Section 1033. In outreach meetings, financial planners and investment advisers advised Treasury that many broker-dealers and their

64. See Bureau Stakeholder Insights, at 4-5.

65. 12 U.S.C. § 5481(4).

66. See 12 U.S.C. § 5517(h)-(i).

67. See 12 U.S.C. § 5517(g).

68. See 12 U.S.C. § 5517(f).

custodians have been providing financial account and transaction data in a usable electronic format for a long time.<sup>69</sup> Such data, for instance, is needed to produce performance reports and monitor asset allocations. However, in outreach meetings with Treasury, financial planners and investment advisers indicated that the current data feeds from broker-dealers were generally reliable.

### *Recommendations*

Treasury recommends that regulators such as the SEC, Financial Industry Regulatory Authority, DOL, and state insurance regulators recognize the benefits of consumer access to financial account and transaction data in electronic form and consider what measures, if any, may be needed to facilitate such access for entities under their jurisdiction.<sup>70</sup> However, Treasury recommends against further legislative action to expand the scope of Section 1033 at this time.

### Consumer Disclosure, Consent, and Termination

The products and services discussed in this section require consumer authorization as the legal basis for accessing the financial account and transaction data. But consumers cannot make informed choices without transparent, comprehensible, and readily accessible disclosure. Without adequate disclosure, consumers will be unable to clearly understand and weigh the risks and benefits of using fintech applications and letting third-parties access and use their personal and financial data.

Some fintech applications and data aggregators make hard-to-follow disclosures as to which financial account and transaction data will be obtained and how that data will be utilized and stored. In other cases, the disclosures, terms, and conditions may be hard to find or they may be written in dense legalistic language that induces the consumer to head straight to the “accept” button, or else forgo usage of the service.

Disclosures may not be fully effective to the extent that consumers remain unaware of the data relationships underlying the services they are using. For example, for fintech applications that rely on a data aggregator to obtain or process the consumer’s financial account and transaction data, the role of the data aggregator may be opaque to the consumer. As consumers increasingly access fintech applications through their mobile devices, the likelihood that they will read and understand long and meticulous disclosures diminishes.

While complex disclosures designed to protect service providers rather than inform consumers are a problem, consumers should make every effort to read disclosures so that they understand their rights and obligations. It is not enough to assert that measures are needed to ensure that consumers understand what they are agreeing to when they use third-party applications. As one observer wrote, “[d]isclosures written in plain language might increase consumer awareness, but

69. A number of the financial planners and investment advisers indicated that it was more difficult to obtain data from 401(k) plans, particularly the smaller ones, than from traditional broker-dealers.

70. See, e.g., General Instruction C.(3).g of Form N-1A under the Securities Act and Investment Company Act (requiring electronic machine-readable information about mutual funds).

that only works if consumers actually read the ‘Terms and Conditions’ before downloading the latest financial app.”<sup>71</sup>

While consumers have to some extent become conditioned to opt for convenience over security, they nevertheless continue to look to their primary financial institutions for protection of their personal and financial data.<sup>72</sup> This raises issues of importance for these financial institutions, including how to verify that their customers have in fact authorized a third party to access their account or initiate a transaction. Further, data aggregators may obtain significantly more consumer financial data than necessary to provide the service that the customer requested, often unknown to the customer. The implications of these features give rise to a potentially wide cascade of issues regarding downstream use of the data, including broader issues related to data privacy that are beyond the scope of this report.

Finally, consumers should have an easy way to revoke their consent to data aggregator access to their financial account and transaction data. Otherwise, data aggregators may retain and continue to use the data and, in some circumstances, may even be able to acquire additional data. It is important that requirements regarding customer authorization be improved to allow customers to exercise control over the scope and duration of data being obtained, how the data is used, and to whom it may be provided.

### *Recommendations*

Treasury recommends that the Bureau work with the private sector to develop best practices on disclosures and terms and conditions regarding consumers’ use of products and services powered by consumer financial account and transaction data provided by data aggregators and financial services companies. The goal should be to provide disclosures and terms and conditions that are written in plain language, readily accessible, readable through the preferred device used by consumers to access services, and presented in a reasonably simple and intuitive format so that consumers can give informed and affirmative consent regarding to whom they are granting access, what data is being accessed and shared, and for what purposes. If necessary, the Bureau should consider issuing principles-based disclosure rules pursuant to its authority under Section 1032 of Dodd-Frank.<sup>73</sup>

Treasury also believes that consumers should have the ability to revoke their prior authorization that permits data aggregators and fintech applications to access their financial account and transaction data. Data aggregators and fintech applications should provide adequate means for consumers

71. Amber Goodrich, Computer Services, Inc., *5 Challenges of Sharing Consumer Data*, blog post (Nov. 8, 2017), available at: <https://www.csiweb.com/resources/blog/post/2017/11/08/5-challenges-of-sharing-consumer-data>.

72. According to one survey, 91% of U.S. consumers willingly accept the terms and conditions of various mobile applications and services without reading them; for ages 18 to 34 the acceptance rate of terms and conditions, without reading them, is 97%. See Deloitte, *2017 Global Mobile Consumer Survey: US Edition* (2017), at 12, available at: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf>. See also A.T. Kearney, *Key Findings from the Consumer Digital Behavior Study* (Apr. 2018), available at: <https://www.atkearney.com/financial-services/the-consumer-data-privacy-marketplace/the-consumer-digital-behavior-study> (“Consumers view banks as their best agent in protecting consumer data privacy and security”).

73. See 12 U.S.C. § 5532.

to readily revoke the prior authorization. If necessary, banking regulators and the SEC should consider issuing rules that require financial services companies to comply with a consumer request to limit, suspend, or terminate access to the consumer's financial account and transaction data by data aggregators and fintech applications.

### Moving Away from Screen-Scraping to More Secure Access Methods

The practice of using login credentials for screen-scraping poses significant security risks, which have been recognized for nearly two decades.<sup>74</sup> Screen-scraping increases cybersecurity and fraud risks as consumers provide their login credentials to access fintech applications. During outreach meetings with Treasury, there was universal agreement among financial services companies, data aggregators, consumer fintech application providers, consumer advocates, and regulators that the sharing of login credentials constitutes a highly risky practice.

APIs are a potentially more secure method of accessing financial account and transaction data than screen-scraping. A number of foreign jurisdictions have opted to promote access through APIs, in part due to security concerns. The United Kingdom, through its open banking initiative, has specified regulatory standards for data sharing through APIs.<sup>75</sup> The European Union has adopted the Revised Payment Service Directive (PSD2), which requires banks to grant licensed third-party payment service providers access to bank infrastructure and account data. PSD2 also contemplates the standardization of APIs.<sup>76</sup> Singapore has encouraged the use of bank APIs but has not made it a regulatory mandate.<sup>77</sup>

Data aggregators and consumer fintech application providers have expressed reservations with an API approach. They claim, for example, that their efforts to work with financial services companies to do away with screen-scraping have for the most part been met with resistance, and that financial services companies have largely refused to enable direct access to their data or to set up open APIs.<sup>78</sup> There are concerns that without some sort of industry standard or regulatory guidance, API access could be restricted to certain types of data dictated by the financial services company, as opposed to the consumer, susceptible to unexpected interruptions and terminations, and subject to unreasonable and disproportionate liability.

### Recommendations

Treasury sees a need to remove legal and regulatory uncertainties currently holding back financial services companies and data aggregators from establishing data sharing agreements that effectively

74. See footnote 46.

75. Open Banking Ltd., *Guidelines for Read/Write Participants* (ver. 3.2, May 2018), available at: <https://www.openbanking.org.uk/wpcore/wp-content/uploads/Guidelines-for-Read-Write-Participants.pdf>.

76. Directive (EU) 2015/2366 of the European Parliament and of the Council (Nov. 25, 2015), available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN>.

77. Ong Chong Tee, Monetary Authority of Singapore, *The Future of Banking – Evolution, Revolution or a Big Bang?* (Apr. 16, 2018), available at: <http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2018/The-Future-of-Banking.aspx>.

78. See, e.g., Daniel Castro and Michael Steinberg, Center for Data Innovation, *Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help* (Nov. 6, 2017), available at: <http://www2.datainnovation.org/2017-open-apis.pdf>.



move firms away from screen-scraping to more secure and efficient methods of data access. Treasury believes that the U.S. market would be best served by a solution developed by the private sector, with appropriate involvement of federal and state financial regulators.

A potential solution should address data sharing, security, and liability. Any solution should explore efforts to mitigate implementation costs for community banks and smaller financial services companies with more limited resources to invest in technology.

### Liability for Unauthorized Access

Screen-scraping also appears tied to the issue of liability. Financial services companies have expressed concerns that they may bear the burden of any losses arising from a breach at the data aggregator or a downstream fintech application. Even if the consumer's losses are not limited by Regulation E,<sup>79</sup> such as when a consumer authorized a person other than the consumer to initiate an electronic funds transfer by providing login credentials to such third party, the consumer may nonetheless expect the bank or other financial institution to make him or her whole for any losses.

Providing login credentials to a data aggregator creates opportunities for bad actors to illicitly obtain such highly sensitive credentials and allow assets to be transferred out of the account. Screen-scraping also can allow a data aggregator to obtain significantly more data than needed by the underlying fintech application, including sensitive personally identifiable information, which could be subsequently stolen.<sup>80</sup> Moving away from screen-scraping can facilitate resolution of the liability issue by eliminating the need for login credentials, reducing the amount and sensitivity of unnecessary data being acquired by data aggregators and decreasing the possibility of an unauthorized transaction.

Some data aggregators have entered into agreements with financial services companies to access the financial account and transaction data through an API but conditioned on contractual liability and indemnification of the financial services company. Other data aggregators have been unable or unwilling to reach agreement on such terms. In such circumstances, data aggregators usually continue to obtain data through screen-scraping.

As the U.S. Government Accountability Office (GAO) has observed, the issue of financial responsibility for consumer losses and access to consumer financial transaction data has been discussed at meetings of federal banking regulators and the Bureau under the auspices of the Federal Financial Institutions Examination Council (FFIEC). However, these discussions have not resulted in any specific policy outcomes to guide market participants.<sup>81</sup> Without resolution of liability and other

79. 12 C.F.R. Part 205. Regulation E implements the Electronic Fund Transfer Act, which establishes a framework of the rights, liabilities, and responsibilities of participants in the electronic fund and remittance transfer systems.

80. The sensitivity of consumer financial transaction data can vary. For example, data indicating that a bank account is a checking account may be less sensitive than the associated ABA routing and account numbers. If a fintech application only needs to know the account type, then it would be unnecessary to obtain the more sensitive ABA routing and account numbers.

81. U.S. Government Accountability Office, *Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight* (Mar. 2018) at 54-57, available at: <https://www.gao.gov/assets/700/690803.pdf> ("GAO Fintech Report"). GAO reported that some regulators indicated that they had not taken more steps to resolve the disagreements surrounding financial account aggregation because they are concerned over acting too quickly. Id. at 56.

issues, “consumers could have to choose between facing potential losses or not using what they may find to be an otherwise valuable financial service, and fintech firms providing useful services to consumers will face barriers to providing their offerings more broadly.”<sup>82</sup>

#### *Recommendations*

Treasury recommends that any potential solution discussed in the prior recommendation also address resolution of liability for data access. If necessary, Congress and financial regulators should evaluate whether federal standards are appropriate to address these issues.

#### Standardization of Data Elements

There are other areas in which collaboration among market participants could improve consumers’ ability to use their data. Collaborative attempts have been made among financial services companies, data aggregators, and consumer fintech application providers to create standardized data elements, including efforts by Open Financial Exchange (OFX) and Financial Services Information Sharing and Analysis Center (FS-ISAC).<sup>83</sup> However, these efforts have not achieved full consensus to date. A standardized set of data elements and formats would help to foster innovation in services and products that use financial account and transaction data, because it may be more efficient to develop a single agreed-upon taxonomy. Data elements would need to be developed for a broad range of products and services related to banking, investments, retirement, loans, insurance, and taxes. Standardization could improve the market efficiency for financial products and services by making it easier to engage in comparative analysis.

Data currently obtained by aggregators from separate financial services companies can be incompatible and must be cleaned and standardized before it can be used. Financial services companies often use “disparate and customized formats to send and share information, employing different nomenclature for [otherwise] common terms.”<sup>84</sup>

#### *Recommendations*

Treasury recommends that any potential solution discussed in the prior recommendation address the standardization of data elements as part of improving consumers’ access to their data. Any solution should draw upon existing efforts that have made progress on this issue to date. If necessary, Congress and financial regulators should evaluate whether federal standards are appropriate to address these issues.

#### Clarifying When Data Aggregators Are Subject to Third-Party Guidance

Some banks have raised concerns over whether third-party guidance may apply if a bank enters into an API agreement with a data aggregator that establishes terms of access, because the bank has

---

82. Id. at 57.

83. See footnote 50.

84. Conrad Sheehan, Accenture, *To Capitalize on Open Banking, the Industry Needs Standards*, American Banker (Apr. 10, 2018), available at: <https://www.americanbanker.com/opinion/to-capitalize-on-open-banking-the-industry-needs-standards>.



entered into a contract.<sup>85</sup> Third party guidance clearly applies when a bank itself is providing data aggregation as a service to its customers and has hired a data aggregator to collect the data with its customer's authorization because the data aggregator becomes a service provider to the bank. But when the data aggregator has entered into an API agreement with the bank where it is not providing a service to the bank, it is unclear whether third party guidance may still apply.

Data aggregators would not consider themselves service providers to banks when, for example, they rely on screen-scraping to access financial account and transaction data that has been authorized by a consumer.<sup>86</sup> However, if data aggregators were to instead enter into an API agreement with a bank, it may become subject to third-party guidance because of the contractual relationship, which can increase compliance costs.

This regulatory uncertainty over the application of third-party guidance may, therefore, be inadvertently discouraging more API agreements between banks and data aggregators.

### *Recommendation*

Treasury recommends that the banking regulators remove ambiguity stemming from the third-party guidance that discourages banks from moving to more secure methods of data access such as APIs. Further discussion of bank regulatory oversight of third-party relationships is addressed in the following chapter on Aligning the Regulatory Framework to Promote Innovation.

### Current Regulation of Data Aggregators

The greater the amount of consumer financial account and transaction data that is retained by data aggregators, the greater is the possible harm to consumers that could result from a data breach.<sup>87</sup> Although data aggregators do not have a specific regulatory scheme similar to banks or other depository institutions, they are currently subject to regulation under the federal consumer protection laws administered by the FTC as well as state consumer protection laws.<sup>88</sup> Some financial services companies have suggested that the absence of the same level of regulatory oversight of data aggregators and downstream consumer fintech application providers raises significant risks for consumers.<sup>89</sup> In particular, they have argued that the security practices of data aggregators are not comparable to the standards applied at banks and the security practices of consumer fintech application providers are even weaker.

- 
- 85. Banking regulators have issued guidance for assessing and managing risks in third-party relationships. The guidance views a third-party relationship as "any business arrangement between a bank and another entity, by contract or otherwise."
  - 86. Treasury is aware that some data aggregators have entered into agreements with banks, sometimes on an informal basis, while engaging in screen-scraping. For example, a data aggregator may agree to pull the data during the night in order to minimize disruption to the bank's computer systems.
  - 87. In outreach meetings with Treasury, data aggregators have asserted that they mitigate data breach risk by only retaining aggregated and anonymized data that is not associated with any personally identifiable information of the consumer.
  - 88. To the extent that a data aggregator or consumer fintech application provider is providing services to a bank, the services provided are subject to the third-party oversight framework imposed by banking regulators under the Bank Services Company Act.
  - 89. American Bankers Association, *Fintech – Promoting Responsible Innovation* (May 2018), at 3-4, available at: <https://www.aba.com/Advocacy/Documents/fintech-treasury-report.pdf>.

Data aggregators and consumer fintech application providers are subject to the Gramm-Leach-Bliley Act (GLBA),<sup>90</sup> which is a federal law specifying the ways that financial institutions, including some nonbank financial institutions, protect the security and confidentiality of nonpublic personal information of individuals.<sup>91</sup> The provisions in GLBA govern how financial institutions, as defined under the statute,<sup>92</sup> implement administrative, technical, and physical safeguards to insure the security and confidentiality of customer records, protect against any anticipated threats or hazards, and protect against unauthorized access.<sup>93</sup> Financial institutions must explain their policies to their customers that are designed to safeguard sensitive data.<sup>94</sup> These provisions of GLBA are enforced by the FTC, the federal banking agencies, the SEC, and the Commodity Futures Trading Commission (CFTC). To be compliant with GLBA, financial institutions must apply specific protections to customers' private data in accordance with the institution's data security plan.

To implement GLBA, the FTC set forth the primary information security provisions in its Safeguards Rule.<sup>95</sup> The FTC's Safeguards Rule requires financial institutions to assess and develop a documented security plan that describes the company's program to protect customer information, including the following areas particularly important to information security: employee management and training, information systems, and detecting and managing system failures.<sup>96</sup> The intent of the GLBA information security requirements in the Safeguards Rule is to protect consumers and reduce reputational damage caused by unauthorized sharing or loss of private customer data. The FTC has indicated that data aggregators and consumer fintech application providers significantly engaged in financial services and products are financial institutions under GLBA and therefore subject to the Safeguards Rule.<sup>97</sup>

In addition, there are efforts underway to regulate consumer-authorized data aggregation, including potential legislation, at the state level. However, Treasury believes that state-by-state regulation, which would be more cumbersome and costly to comply with as compared with regulation by a single federal regulator, would not be workable given the complexity of data issues at hand.

### *Recommendation*

Moving away from screen-scraping and eliminating the sharing of login credentials will address the most significant concerns raised about the need to increase regulation of data aggregators and

90. Public Law No. 106-102 [codified at 15 U.S.C. Ch. 94]. Also known as the Financial Services Modernization Act of 1999.

91. 15 U.S.C. § 6801(a).

92. Financial institutions include companies that offer consumer financial products or services like loans, financial or investment advice, or insurance.

93. 15 U.S.C. § 6801(b).

94. *Id.* § 6803(c)(3).

95. 15 U.S.C. §§ 6801, 6805(b); 16 C.F.R. Part 314.

96. 16 C.F.R. §§ 314.3 and 314.4.

97. Federal Trade Commission, *Financial Institutions and Customer Information: Complying with the Safeguards Rule* (Apr. 2006), available at: <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying> (stating that the Safeguards Rule applies to companies that receive information about the customers of other financial institutions).

consumer fintech application providers. While data security concerns will remain an important issue, the Safeguards Rule appropriately addresses such concerns.<sup>98</sup>

To the extent that any additional regulation of data aggregation is necessary, Treasury recommends that it occur at the federal level by regulators that have significant experience in data security and privacy, and that will have, through legislation if necessary, broad jurisdiction to ensure equivalent treatment in the nonfinancial sector.

## Data Security and Breach Notification

### Data Security Standards

The data security provisions of GLBA are enforced by the federal banking agencies for depository institutions,<sup>99</sup> the SEC and the CFTC for entities under their jurisdiction, and the FTC for all other financial institutions.<sup>100</sup> With the exception of the FTC, these federal agencies are authorized to routinely supervise and examine for compliance with these provisions of GLBA and their implementing regulations. These agencies all maintain authority to implement regulations for GLBA.

Data security standards are significantly different between nonfinancial companies, such as retailers and manufacturers, and financial institutions. Vast amounts of consumer payment credentials and financial data are routinely stored on a nonfinancial company's internal or third-party systems, used for marketing purposes, or simply used to complete transactions instantly. Yet, nonfinancial companies are not subject to comprehensive federal data security standards under GLBA and are not subject to routine examination for compliance with data security standards. The only heightened obligation to protect data comes from the exercise of the FTC's authority under Section 5 of the Federal Trade Commission Act<sup>101</sup> to bring enforcement actions against nonfinancial companies for unfair or deceptive practices. The FTC has exercised this authority more than 60 times since 2002; however, this authority is limited to enforcement action and does not give the FTC supervision and examination rights over these nonfinancial companies.<sup>102</sup>

In addition to federal standards, nonfinancial companies and financial institutions subject to the FTC's jurisdiction under GLBA must comply with applicable state laws that impose heightened or specific data security standards. To date, only 13 states have imposed data security standards for protection of consumer financial data, which have different requirements. For instance, Florida requires a business to take "reasonable measures" to protect and secure personal information data

98. In addition to the information security requirements, GLBA also contains privacy requirements as to how financial institutions collect, use, and maintain nonpublic personal information and under what circumstances that information can be shared. These provisions are applicable to financial institutions under the Bureau's Regulation P [12 C.F.R. Part 1016].

99. See Interagency Guidelines Establishing Information Security Standards, as codified at 12 C.F.R. Part 30, App. B (OCC); 12 C.F.R. Part 208, App. D-2 and Part 225, App. F (Federal Reserve); and 12 C.F.R. Part 364, App. B (FDIC).

100. Insurance data security was examined in the Asset Management and Insurance Report.

101. 15 U.S.C. § 45(a)(1).

102. Federal Trade Commission, *Privacy & Data Security Update: 2017*, available at: [https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy\\_and\\_data\\_security\\_update\\_2017.pdf](https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf).

that is stored in “electronic form,” but Utah does not differentiate between personal information stored electronically or on paper.<sup>103</sup>

Over the last several years, many nonfinancial companies have been subject to significant data breaches of consumer financial data. For example, in 2013, Target announced that payment card information of 41 million consumers was compromised.<sup>104</sup> In 2014, Home Depot announced that the payment card information of more than 50 million customers was stolen in a data breach.<sup>105</sup> More recently, the retailer Hudson’s Bay Co. advised roughly 5 million customers of its subsidiary stores Lord & Taylor and Saks Fifth Avenue that their payment credentials had been compromised.<sup>106</sup> Data breaches are not unique to nonfinancial companies and have affected financial institutions as well.<sup>107</sup>

### Data Breach Notification

The United States does not have a national law establishing uniform national standards for notifying consumers of data breaches, or for providing them a clear and straightforward mechanism for resolving disputes.<sup>108</sup> In the absence of uniform national standards, states have been aggressive in developing their own data breach notification laws. Each state law may apply to any company located in that state or that does business with residents of that state. In practice, this means that in the event of a data breach companies could be subject to the data breach notification laws of 50 states as well as of the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands.<sup>109</sup> State laws for data breach notification often include specific provisions regarding the number of affected individuals that will trigger notification requirements, the timing of notification, and form of notification, among other requirements. Unsurprisingly, state data breach notification laws are far from uniform. Indeed, they vary in a number of significant ways, including with respect to the most fundamental aspect, namely the scope of data covered under the definition of personal

103. Compare Fla. Stat. § 501.171(2) with Utah Code § 13-44-201.

104. Target Brands, Inc., *Press Release – Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores* (Dec. 19, 2013), available at: <https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car>.

105. The Home Depot, *News Release – The Home Depot Reports Finding in Payment Data Breach Investigation* (Nov. 6, 2014), available at: <http://ir.homedepot.com/news-releases/2014/11-06-2014-014517315>.

106. Mike Murphy, *Saks, Lord & Taylor Data Breach May Affect 5 Million Customers*, MarketWatch (Apr. 1, 2018), available at: <https://www.marketwatch.com/story/saks-lord-taylor-data-breach-may-affect-5-million-customers-2018-04-01>.

107. For example, JPMorgan Chase was subject to a data breach in 2014 and Equifax suffered a data breach in 2017.

108. Federal banking regulators have adopted guidance for depository institutions in the event of unauthorized access to customer information. See Interagency Guidance on Response Programs for Unauthorized Access to Customer information and Customer Notice [70 Fed. Reg. 15736 (Mar. 29, 2005)].

109. National Conference of State Legislatures, *Security Breach Notification Laws* (Mar. 29, 2018), available at: <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

information.<sup>110</sup> Other inconsistencies among states' breach notification laws can make compliance difficult for firms and entail disparate treatment for consumers. The lack of uniformity and efficiency affects both nonfinancial companies and financial institutions.

### *Recommendation*

Congress has considered establishing a federal data security standard and breach notification standard on several occasions. For example, during the 114<sup>th</sup> Congress, two separate bills, sharing many common principles, successfully passed their respective committees.<sup>111</sup> During this Congress, legislation has again been considered to establish these federal standards.

Treasury recommends that Congress enact a federal data security and breach notification law to protect consumer financial data and notify consumers of a breach in a timely manner. Such a law should be based on the following principles:

- Protect consumer financial data
- Ensure technology-neutral and scalable standards based on the size of an entity and type of activity in which the entity engages
- Recognize existing federal data security requirements for financial institutions
- Employ uniform national standards that preempt state laws

## **Digital Legal Identity**

Digital identity products and services hold promise for improving the trustworthiness, security, privacy, and convenience of identifying individuals and entities, thereby strengthening the processes critical to the movement of funds, goods, and data as the global economy races deeper into the digital age. Digital identity systems also have the potential to generate cost savings and efficiencies for financial services firms. For instance, trustworthy digital identity systems could improve customer identification and verification for onboarding and authorizing account access, general risk management, and antifraud measures.

### **Legal Identity**

Legal identity is distinct from broader concepts of personal and social identity. Legal identity is the specification of a unique natural or legal person that (1) is based on certain pre-specified characteristics or attributes of the person that are intended to establish the person's uniqueness, (2) is recognized by the state under national law, and (3) ascribes legal rights and duties to that person. Proof of legal identity is required to open a bank, brokerage, or other account at a regulated financial institution. Digital legal identity uses electronic means to unambiguously assert and authenticate a real person's unique legal identity.

- 
110. For example, Maryland specifically includes biometric data of an individual such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristics, while other states do not. Compare Md. Code Com. Law § 14-3501(d) [as amended by House Bill 974 (May 4, 2017)] with Nevada Rev. Stat. § 603A.040.
111. Data Security Act of 2015, H.R. 2205, 114th Cong.; Data Security and Breach Notification Act of 2015, H.R. 1770, 114th Cong.

## Portability

Digital identity systems potentially allow legal identity to be portable. Portable legal identity means the individual's verified identity credentials can be used to establish legal identity for new customer relationships at unrelated financial institutions or government entities, without each financial institution's having to obtain and verify personally identifiable information (PII) to meet regulatory requirements. Portability requires developing interoperable digital identification products, systems, and processes. While not permitted in the private sector under current regulations, trustworthy portable third-party digital identity services could potentially save relying parties time and resources in identifying, verifying, and managing customer identities, including for account opening and access. Portability could also potentially save customers the inconvenience of having to prove and authenticate identity for each unrelated financial institution or government service, and reduce the risk of identity-theft stemming from the repeated exposure of PII.

## Components of a Digital Identity System

Digital identity systems may rely on various types of technology and use digital technology in several ways,<sup>112</sup> but generally involve two essential components: (1) identity proofing, enrollment, and credentialing; and (2) authentication. They may also involve a third component, federation, which is optional, but allows identity to be portable. Identity proofing and enrollment may be digital or documentary, remote, or in-person. Credentialing, authentication, and federation are always digital. Different identity service providers can provide some or all of the components of a digital identity system.

Identity proofing establishes that a subject is who they claim to be. It involves obtaining and verifying that attribute evidence is genuine and accurate, and issuing a digital credential to bind the verified identity to a real-life person. Identity proofing depends on official government registration and documentation/certification, or at least on governmentally recognized registration and certification, for verification.<sup>113</sup>

Authentication establishes that the person asserting identity is who he or she claims to be. It involves confirming, through a secure digital authentication protocol, that the individual asserting identity is in control of the technologies and credentials that bind the validated identity to a real person. Successful authentication provides reasonable, risk-based assurances to the relying party that the subject asserting identity today is the same person who previously

112. For example, digital identity systems may use electronic databases to obtain and confirm attribute information and/or store and manage records; digital credentials to authenticate identity for accessing mobile, online, and offline financial activities; and digital biometrics to provide attributes to identify and/or a credential to authenticate individuals.

113. National Institute of Standards and Technology, *Digital Identity Guidelines – Enrollment and Identity Proofing Requirements*, NIST Special Publication 800-63A (June 2017), available at: <https://pages.nist.gov/800-63-3/sp800-63a.html> ("NIST 800-63A").



asserted identity and accessed a financial service, and is in fact a given identified customer. Trustworthy authentication is key for combating account-access identity fraud.<sup>114</sup>

Federation involves the use of federated identity architecture and assertions to convey the results of an authentication process and, if requested or required, attribute information to relying parties across a set of networked systems.<sup>115</sup>

The National Institutes of Standards and Technology (NIST) of the U.S. Department of Commerce has recently established risk-based technical standards for each of the component processes of a digital identity system (enrollment and identity proofing; authentication and lifecycle management; and federation),<sup>116</sup> which are mandatory for the federal government, but only voluntary for the private sector.

### Public-Private Roles

Both the government and the private sector have important roles in establishing a trustworthy U.S. digital identity ecosystem. In the United States, the private sector is generally relied upon to develop innovative identity products, services, and business models, while the federal government is ultimately responsible for establishing the minimum substantive requirements for proving legal identity, including core attributes and acceptable attribute evidence. Federal and state government authorities also provide the official government registration and the related official root identity evidence (e.g., birth certificates, passports) on which legal identity currently depends.

Public and private sector stakeholders need to work together to develop trustworthy digital legal identity products and services for use in the financial sector and elsewhere. To facilitate this objective, stakeholders should address a number of issues, including:

- How to leverage the NIST guidelines to establish flexible, risk-based standards for digital customer identification and verification, keyed to the risk levels associated with specific customers and/or types of financial products and services
- How to ensure the trustworthiness, privacy, and cybersecurity of identity service providers, such as government or industry certification and supervision
- Business models and liability allocation appropriate for establishing portable legal identity
- Ways the public and private sectors can effectively work together to reduce regulatory burden and catalyze the market for trustworthy digital identity products and services

114. National Institute of Standards and Technology, *Digital Identity Guidelines – Authentication and Lifecycle Management*, NIST Special Publication 800-63B (June 2017), available at: <https://pages.nist.gov/800-63-3/sp800-63b.html> ("NIST 800-63B").

115. National Institute of Standards and Technology, *Digital Identity Guidelines*, NIST Special Publication 800-63-3 (June 2017), at 14-15, available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf> ("NIST 800-63-3").

116. See NIST 800-63A, 800-63B, and NIST 800-63-3. The NIST digital identity guidelines set requirements for three different levels of trustworthiness, called levels of assurance (LOAs), for each of these component processes, based on the LOA's degree of trustworthiness.

Treasury recommends that financial regulators work with Treasury to enhance public-private partnerships to identify ways government can eliminate unintended or unnecessary regulatory and other barriers and facilitate the adoption of trustworthy digital legal identity products and services in the financial services sector. This would include engaging the private sector to help the financial regulators adopt regulation in the legal identity space that is flexible, risk-, principles-, and performance-based, future-proofed, and technology-neutral. Treasury also recognizes that the development of digital legal identity products and services in the financial services sector should be implemented in a manner that is compatible with solutions developed across other sectors of the U.S. economy and government.

Treasury also supports the efforts of the Office of Management and Budget to fully implement the long-delayed U.S. government federated digital identity system. Treasury recommends policies that would restore a public-private partnership model to create an interoperable digital identity infrastructure and identity solutions that comply with NIST guidelines and would reinvigorate the role of U.S. government-certified private sector identity providers, promoting consumer choice and supporting a competitive digital identity marketplace. Treasury also seeks to leverage the U.S. government federated identity system — in particular, its certification and auditing regime for digital identity providers — to permit financial institutions to use digital identity services provided by certified providers to conduct customer identification and verification for onboarding.

Finally, Treasury encourages public and private stakeholders to explore ways to leverage the REAL ID Act<sup>117</sup> driver's license regime — particularly, robust state REAL ID license identity-proofing processes — to provide trustworthy digital identity products and services for the financial sector.

## The Potential of Scale

The ongoing digital transformation of the financial services system is being driven not only by developments in computing power, the expanding ubiquity and interconnection of computers and mobile devices, and the exponential growth in digitized financial data, but also by technologies that can benefit from advances in data and computing capacity at greater scale and with greater efficiency. Scalable technologies such as cloud computing enable financial services companies to store and process vast amounts of data and to quickly add new computing capacity to meet changing needs. At the same time, advances in big data analytics, machine learning, and artificial intelligence are expanding the frontiers of financial services firms' abilities to glean new and valuable business insights from vast datasets.

### Cloud Technology and Financial Services

Cloud technology is enabling organizations across the economy to more rapidly innovate by reducing barriers to entry to acquire high quality computing resources. Cloud computing, more specifically, enables more convenient, on-demand access to computing resources (e.g., networks, servers,

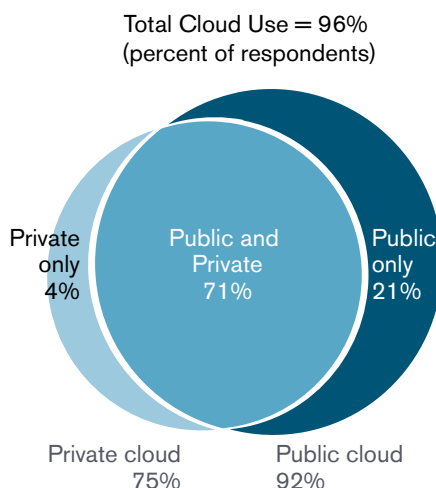
---

117. Public Law No. 109-13.



storage, applications, and services).<sup>118</sup> Cloud computing can be deployed through several models: a public cloud, which refers to when these computing resources are available in a shared environment, accessible by multiple customers of the cloud service provider; a private cloud, which refers to when these computing resources are dedicated for use by a single firm, but provided generally in the same type of convenient, rapid, on-demand manner; or a hybrid cloud, which refers to an arrangement consisting of a mix of cloud deployment models.

Figure 5: Cloud Adoption (percent of respondents)



Source: RightScale 2018 State of the Cloud Report.

Before the broad availability of a public cloud, only large organizations with ample budgets were able to cover the costs involved with building out large-scale internal information technology (IT) infrastructures. Firms would have to make large capital expenditures on computing and networking hardware as well as maintain ongoing operating expenses for multiple layers of software and large IT staffs. With public cloud services, however, firms of all sizes can essentially lease a range of computing resources and expertise from cloud service providers, potentially at lower cost.

Several large technology-focused firms have been central to the development of cloud computing, and the growth of the public cloud market in particular. To achieve the scale necessary to maximize the potential of this technology requires substantial resources. For this reason, these firms continue to dominate the market though competition has increased. The adoption of public cloud is occurring throughout the economy with, for example, survey data suggesting that some 92% of

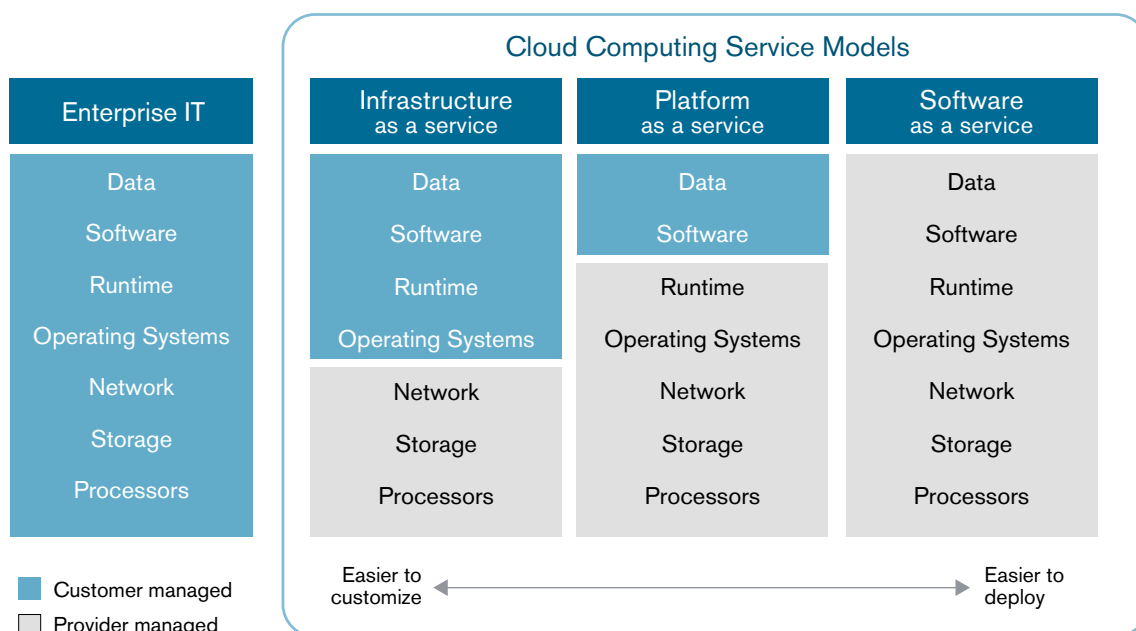
118. National Institute of Standards and Technology, *The NIST Definition of Cloud Computing*, Special Publication 800-145 (Sept. 2011), at 2-3, available at: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

businesses adopting at least some form of public cloud services.<sup>119</sup> Other sources forecast robust growth in public cloud revenues<sup>120</sup> and data usage.<sup>121</sup>

## Types of Cloud Services

While traditional IT often requires firms to manage computing resources internally, cloud computing is generally provided under three service models that provide varying degrees of outsourcing and customization. Infrastructure-as-a-service (IaaS) gives clients the greatest overall control of function and scale by allowing them to expand processing, storage, networks, and other essential

Figure 6: Traditional IT Compared to Cloud Computing



Source: Adapted from U.S. Department of Transportation, *Uses of Cloud Technology for Geospatial Applications*

119. RightScale, Inc., *RightScale 2018 State of the Cloud Report* (2018).

120. One market observer forecasts global public cloud revenue growing from \$153.5 billion in 2017 to \$186.4 billion in 2018, a 21.4% increase. See Gartner, Inc., *Press Release – Gartner Forecast Worldwide Public Cloud Revenue to Grow 21.4 Percent in 2018* (Apr. 12, 2018), available at: <https://www.gartner.com/newsroom/id/3871416>.

121. Cisco estimates, by 2021, 95% of global data center traffic will come from cloud services and applications. Annual global cloud traffic will reach 19.5 zettabytes (ZB) by the end of 2021, up from 6.0 ZB in 2016. One ZB is equal to sextillion bytes, or one trillion gigabytes. See Cisco, *Cisco Global Cloud Index: Forecast and Methodology 2016-2021* (2018), available at: <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf>.

Figure 7: NIST Definition of Cloud Computing

<b>Essential characteristics</b>	On-Demand Self-Service	User can unilaterally provision server time, network storage, etc. as needed without involving service provider.
	Broad Network Access	Capabilities are available over the network and accessed through common mechanisms (e.g. a Web browser) and devices.
	Resource Pooling	Physical and virtual resources are shared across a large pool of users, allowing for dynamic assignment according to users' demands.
	Rapid Elasticity	Computing capabilities can be scaled rapidly up or down according to users' demands, such that any given user's demand is met without interruption.
	Measured Service	Users access capabilities as a service and pay only for resources used.
<b>Service models</b>	Software-as-a-Service (SaaS)	End-user applications provided as a service only. User cannot manage or control any underlying cloud infrastructure.*
	Platform-as-a-Service (PaaS)	Application platforms or middleware provided as a service on which users can build and deploy custom applications using programming languages, libraries and other tools supported by service provider.
	Infrastructure-as-a-Service (IaaS)	Broad and scalable computing capabilities provided as a service, including processing, storage, networks, and operating systems, enabling more control over deployed applications.
<b>Deployment models</b>	Public Cloud	The cloud infrastructure is available for open use by the general public. It generally is owned by and exists on the premises of the cloud service provider.
	Private Cloud	The cloud infrastructure is available for exclusive use by a single organization. It may exist on or off premises and may be owned by the organization, a third party, or both.
	Community Cloud	The cloud infrastructure is available for use only by a specific community of users that have shared needs or concerns. It may be owned by one or more of the community users, by a third party, or some combination.
	Hybrid Cloud	The cloud exists as a configuration of two or more distinct cloud infrastructures (public, private, or community) that enables data and application portability among the separate infrastructures.

\* Cloud infrastructure includes network, servers, data, middleware, operating systems, storage, etc.

Source: National Institute of Standards and Technology.

computing resources on-demand as needed.<sup>122</sup> In contrast, software-as-a-service (SaaS) allows clients to easily use a cloud provider's software that runs on the cloud infrastructure,<sup>123</sup> but tends to provide users the least flexibility or customization. Platform-as-a-service (PaaS) models, which

122. Other service models are sometimes described by industry participants – for example, business-process-as-a-service and data-as-a-service – but generally these can be seen as variants of SaaS, PaaS, or IaaS models.

123. NIST further describes “cloud infrastructure” as consisting of the physical systems (for example, server, storage and network components) and software applications that enable the essential cloud characteristics.

includes elements of IaaS, provides clients control over the deployment and configuration of software applications, but without any control over the underlying cloud hardware/infrastructure.

### Adoption in Financial Services

Financial institutions have been adopting cloud computing in part because of the benefits it provides in effectively managing a firm's IT and computing resources.<sup>124</sup> Many firms have chosen to deploy private cloud or hybrid cloud structures to gain the benefits of cloud while also retaining greater control of their IT in order to satisfy regulatory or other requirements.<sup>125</sup> For certain uses, however, financial institutions are also adopting public cloud, including for tasks and processes that are susceptible to surges in required computing power. This can include volatile workloads associated with periodic stress testing, risk modelling and simulations, or other requirements where computing resources may need to rapidly scale (e.g., payments).

All three types of cloud service models are also being deployed within financial services. SaaS, because it tends to be the easiest to deploy, has the most widespread uptake across financial institutions.<sup>126</sup> SaaS platforms can easily handle, for example, customer relationship management and commercial lending software, as well as noncore services such as e-mail, payroll, billing, and human resources that are amenable to outsourcing. Financial institutions are generally more likely to utilize IaaS and PaaS service models to run more complex or enterprise-specific core services and applications — including treasury, payments, retail banking, and regulatory functions.

Overall, the financial services sector has reportedly been slower to adopt cloud computing than other industries, though this appears to be changing. Industry research suggests that a significant proportion of financial organizations still support much of their IT infrastructure in-house rather than through a cloud service provider.<sup>127</sup> Banks, for example, have been slow to migrate core activities for a number of reasons, including the criticality of such functions and the difficulty of transitioning away from legacy IT systems. However, expectations are for cloud adoption to increase for the financial services sector, just as with other sectors of the economy. Some analysts

124. In a May 2017 whitepaper, the Depository Trust & Clearing Corporation noted that the many relative benefits of cloud contributed to its decision to "strategically expand" the range of services and applications it runs using cloud technology, asserting that cloud computing "has reached the tipping point as the capabilities, resiliency and security of services provided by cloud vendors now exceed those of many on-premises data centers." See Depository Trust & Clearing Corporation, *Moving Financial Market Infrastructure to the Cloud* (May 2017), available at: <http://perspectives.dtcc.com/media/pdfs/13161-Cloud-WhitePaper-05-11-17.pdf>.

125. Filip Blazheski, BBVA Research, *Cloud Banking or Banking in the Clouds?* (Apr. 29, 2016), available at: [https://www.bbva-research.com/wp-content/uploads/2016/04/Cloud\\_Banking\\_or\\_Banking\\_in\\_the\\_Clouds1.pdf](https://www.bbva-research.com/wp-content/uploads/2016/04/Cloud_Banking_or_Banking_in_the_Clouds1.pdf).

126. *Id.*

127. In a 2016 study, Peak 10, an IT consultancy (reorganized as Flexential in January 2018), found that 75% of financial services firms still support technology infrastructure in-house. See Peak 10, *Financial Services and IT Study: Tackling the Digital Transformation* (2016), available at: <http://www.peak10.com/2016-financial-services-and-it-study/>; Flexential, *Financial Services Cloud Adoption: Top Concerns for Making the Move*, blog post (May 2018), available at: <https://www.flexential.com/knowledge-center/blog/financial-services-cloud-adoption-top-concerns-making-move>.

expect large U.S. banks to process the vast majority of their computing needs on cloud platforms within the next 5-10 years.<sup>128</sup>

## **Issues and Recommendations**

### **Overall Benefits and Potential Risks**

Cloud computing has helped increase the speed of innovation by allowing firms to more efficiently and rapidly deploy computing resources to meet business demands and extract usable insights from large datasets.

### **Scalability, Speed, and Cost**

Cloud computing, by enabling financial institutions to rapidly scale up or down their use of cloud applications and infrastructure, provides an efficient way to meet changing demands for computing power and enhances firms' abilities to bring new products and capabilities to market. In a traditional enterprise IT environment, procuring a single new server, for example, could take months to obtain necessary approvals and cost thousands of dollars. In contrast, cloud computing can enable firms to acquire the same computing resources in minutes and potentially at a fraction of the cost.

For new and smaller firms, the economies of scale and affordable cost structure of cloud are key factors in allowing firms to provide products at a scale, quality, and speed that they might otherwise be unable to achieve. Large firms, too, benefit from using cloud because of the sheer volume of resources and magnitude of the economies of scale available through large cloud service providers.

### **Security and Resilience**

Large cloud service providers typically have the resources and expertise to invest in and maintain state-of-the-art and comprehensive IT security and deploy it on a global basis across their platforms. Financial institutions, especially small and mid-sized firms, could find it economically infeasible to achieve similar levels of security on their own. Moreover, because cloud service providers can rapidly re-distribute data across geographically diverse storage and processing centers, cloud environments can potentially enhance firms' strategies for business continuity and operational resilience. Nevertheless, to maintain these advantages in terms of security and resilience, cloud service providers must constantly guard against the risks of being targeted by bad actors.

### **Enabling Large-Scale Data Storage and Management**

Critically, cloud enables the computing resources that are increasingly required by firms that must manage or utilize vast volumes of data, whether for regulatory purposes or in order to build and maintain competitive advantages. Firms in the financial services industry can leverage powerful machine learning and other data analytics tools to analyze large data sets with greater agility and effectiveness in line with firms' business models and strategies. These tools can potentially be used to comb through mountains of text-based documents, generate know-your-customer identity

---

128. Keith Horowitz et al., Citi Research, *U.S. Banks: Transformational Changes Unfolding in Journey to the Cloud* (Jan. 10, 2018).

maps by conducting pattern of life analytics, and convert voice-based input into text and insights about sentiment and intent.

The growth of cloud services also presents certain challenges, including potentially high transitioning costs, security and data privacy considerations, regulatory compliance standards, unrealized or over-sold cost savings compared to in-house IT management, and connectivity speed. Further, firms may face high switching costs if they seek to change cloud service providers and may find themselves with little pricing power relative to the large providers. However, many of these challenges can be addressed through appropriate adaptation of cloud computing services, such as deployment of a private or hybrid cloud, choice of service model, provision of data availability and resilience measures, and other appropriate risk management of outsourcing contracts.

### Regulatory Challenges in Adoption

Regulatory compliance issues continue to present challenges to the broader adoption of and migration to cloud technology by financial services firms. Cloud Security Alliance, an industry group, reported in March 2015, for example, that 71% of respondents to a survey on cloud adoption by financial services firms cited “regulatory restrictions” as a key reason, second only to “data security concerns” that was cited by 100% of respondents, for why they had not yet adopted cloud technology.<sup>129</sup>

Financial services firms face several regulatory challenges related to the adoption of cloud, driven in large part by a regulatory regime that has yet to be sufficiently modernized to accommodate cloud and other innovative technologies. The large number of regulators involved with allowing the use of cloud in financial services can present administrative burdens, as well as challenges with inconsistent requirements. Inconsistencies in regulators’ experience with cloud computing and in the knowledge base at the examiner level may also be a contributing factor.<sup>130</sup>

### Regulatory Outsourcing Guidelines

Financial institutions continue to seek certainty from regulators with regard to permissible uses of public cloud services, and some have indicated that they are hesitant to adopt or migrate to cloud services due in part to regulatory guidance that is either inconsistent or unclear or not well adapted for cloud services. For example, firms have expressed uncertainty over whether regulators’ third-party service provider guidance applies to all or only some cloud deployment models (IaaS, PaaS, and SaaS). Firms are also uncertain as to whether regulators would accept a broader migration to

129. Cloud Security Alliance, *How Cloud is Being Used in the Financial Sector: Survey Report* (Mar. 2015), at 10, available at: [https://downloads.cloudsecurityalliance.org/initiatives/surveys/financial-services/Cloud\\_Adoption\\_In\\_The\\_Financial\\_Services\\_Sector\\_Survey\\_March2015\\_FINAL.pdf](https://downloads.cloudsecurityalliance.org/initiatives/surveys/financial-services/Cloud_Adoption_In_The_Financial_Services_Sector_Survey_March2015_FINAL.pdf).

130. See Securities Industry and Financial Markets Association, *Promoting Innovation in Financial Services* (Apr. 6, 2018), at 37-38 (submission to Treasury).

the cloud for core activities, because financial services firms manage highly sensitive and important customer data and perform critical functions for the economy.<sup>131</sup>

Some of the regulatory guidance may also not be well adapted to cloud. Compliance with regulatory guidance that requires financial institutions to maintain physical access audit rights, for example, can present challenges, including the ability of financial institutions to negotiate on-site access, given a cloud service provider potentially has hundreds or thousands of clients. In the case of vendor audit requirements, industry and market participants have suggested that U.S. financial regulators seek to incorporate independent U.S. audit and certification standards for cloud service providers, which may provide more efficient, consistent and useful means of assessing such services.

Further, these regulatory issues may have implications for a bank's relationship with a third party that itself uses a cloud service provider (i.e., a fourth party). These "chain outsourcing" issues can present challenges to banks looking to partner with third parties that use cloud services.

### Data Localization

Data stored on the cloud can easily be moved and stored anywhere. Cloud computing is not naturally geo-centric; rather, data can be compartmentalized, moved, and processed wherever there is available storage and processing capacity. These capabilities, however, do not necessarily impede the ability of U.S. financial regulators to maintain access to regulated entities' electronic books and records for monitoring, surveillance, and other regulatory purposes, including during a financial crisis. Nevertheless, some jurisdictions have imposed requirements that mandate that data be stored or processed within national borders — so-called localization requirements — or considered such requirements.<sup>132</sup> Data localization can have unintended and harmful effects on competition, innovation, and economic growth. Concerns about data security and access can be better addressed through technology, enhanced security controls, contractual arrangements, and bilateral or multi-jurisdictional agreements.

### Outdated Record Keeping Rules

Certain rules prescribe technology requirements that may be out of date or that unnecessarily hinder adoption of new technologies such as cloud computing. Rule 17a-4 under the Securities Exchange Act of 1934,<sup>133</sup> for example, requires any electronic media used by broker-dealers to be

131. Ongoing work by industry groups and other public-private sector partnerships can perhaps be instructive in helping regulators achieve harmonization, within and across jurisdictions, of standards and requirements to provide greater regulatory certainty. The work of the NIST Cloud Computing Standards Roadmap Working Group, an industry-academia-regulatory collaboration, is one such effort. See National Institute of Standards and Technology, *NIST Cloud Computing Standards Roadmap*, Special Publication 500-291, Version 2 (July 2013), available at: [https://www.nist.gov/sites/default/files/documents/it/cloud/NIST\\_SP-500-291\\_Version-2\\_2013\\_June18\\_FINAL.pdf](https://www.nist.gov/sites/default/files/documents/it/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf).

132. There are limited examples of such restrictions today in the United States. Section 9.3.15.7 of Internal Revenue Service Publication 1075 requires that any agency using external information system services to process, store, or transmit federal tax information "restrict the location of [such systems] to areas within the United States territories, embassies, or military installations." See Internal Revenue Service, *Publication 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information* (Sept. 2016), at 95, available at: <https://www.irs.gov/pub/irs-pdf/p1075.pdf>.

133. 17 C.F.R. § 240.17a-4



stored under the “Write Once, Read Many” or “WORM” format. In effect, the rule compels firms to record and store static snapshots of data, which can be more costly and potentially less secure than employing more dynamic data storage capabilities.

### *Recommendations*

Treasury recognizes that cloud computing is a key technology with the potential to allow financial institutions to significantly enhance their ability to innovate, better serve businesses and consumers, and compete both domestically and abroad.

Treasury recommends that federal financial regulators modernize their requirements and guidance (e.g., vendor oversight) to better provide for appropriate adoption of new technologies such as cloud computing, with the aim of reducing unnecessary barriers to the prudent and informed migration of activities to the cloud. Specific actions U.S. regulators should take include: formally recognizing independent U.S. audit and security standards that sufficiently meet regulatory expectations; addressing outdated record keeping rules like SEC Rule 17a-4; clarifying how audit requirements may be met; setting clear and appropriately tailored expectations for chain outsourcing; and providing staff examiners appropriate training to implement agency policy on cloud services.

Treasury further recommends that a cloud and financial services working group be established among financial regulators so that cloud policies can benefit from deep and sustained understanding by regulatory authorities. Financial regulators should support potential policies by engaging key industry stakeholders, including providers, users, and others impacted by cloud services. Separately, Treasury encourages private industry cloud services providers to proactively formulate standards appropriate for the United States that might address the potential risks presented by the growing use of cloud technology.

Financial regulators in the United States should seek to promote the use of cloud technology within the existing U.S. regulatory framework to help financial services companies reduce the risks of noncompliance as well as the costs associated with meeting multiple and sometimes conflicting regulations.<sup>134</sup> Regulators should be wary of imposing data localization requirements and should instead seek other supervisory or appropriate technological solutions to potential data security, privacy, availability, and access issues.

---

134. This should also include development of information and communications technology standards to improve the interoperability and portability of the cloud. In cloud computing, interoperability refers to the ability of different systems or components, such as those of a financial services company and a cloud services provider, to exchange and use information or to otherwise work together successfully, while portability refers to the ability to move and adapt applications and data between systems, including the different cloud deployment models or the systems of other cloud services providers. Recent E.U. action has sought to make progress in this area. See European Commission, *FinTech Action Plan: For a More Competitive and Innovative European Financial Sector* (Mar. 8, 2018), available at: [http://eur-lex.europa.eu/resource.html?uri=cellar:6793c578-22e6-11e8-ac73-01aa75ed71a1.0001.02/DOC\\_1&format=PDF](http://eur-lex.europa.eu/resource.html?uri=cellar:6793c578-22e6-11e8-ac73-01aa75ed71a1.0001.02/DOC_1&format=PDF).



## Big Data, Machine Learning, and Artificial Intelligence in Financial Services

The application of artificial intelligence (AI) to a wide array of uses across the economy,<sup>135</sup> including financial services, has greatly increased over the past few years. The concept of AI can vary meaningfully, but generally is associated with efforts to enable machines or computers to imitate aspects of human cognitive intelligence, such as vision, hearing, thinking, and decision making. AI and machine learning algorithms have powered many innovations across the broader economy, spanning the power of internet search engines, facial-recognition software, and the potential for autonomous cars.

One of the primary sub-branches of AI development is known as machine learning. Machine learning generally refers to the ability of software to learn from applicable data sets to “self-improve” without being explicitly programmed by human programmers. The nature of “improvement” in the software would depend on the specific machine learning use-case, but could include the quality of image-recognition, the ability to more accurately and efficiently identify money laundering, or the ability to accurately predict fraud, borrower default, or the most useful web links in response to a set of search terms. In general, the more data available for the machine learning models, the better such models will perform because of their ability to learn from the examples in an iterative process referred to as “training the model.”

Machine learning has been around in some form since at least the 1940s and advanced rapidly in recent years.<sup>136</sup> It can span several categories: classical machine learning, which would include supervised learning (focusing on advanced regressions and categorization of data that can be used to improve predictions) and unsupervised learning (processing input data to understand the distribution of data to develop, for example, automated customer segments); and deep and reinforcement learning (which is based on neural networks, and may be applied to unstructured data like images or voice).<sup>137</sup>

Several interrelated developments in technology have enabled this environment:

- Dramatic improvements in the availability and affordability of computing capacity through, for example, cloud computing and the general improvements in computer hardware.
- An explosion in the abundance of digitized data and its analysis, sometimes referred to as “big data.” Consider that by 2020, digitized data is forecasted to be generated at a level that is more than 40 times the level produced in 2009.<sup>138</sup> In 2012, it was estimated that 90% of the digitized data in the world had been generated in just the prior two years.<sup>139</sup>

135. Ananad Rao, *A Strategist's Guide to Artificial Intelligence*, Strategy + Business (Summer 2017), available at: <https://www.strategy-business.com/article/A-Strategists-Guide-to-Artificial-Intelligence>.

136. See id.

137. Marko Kolanovic and Krishnamachari Rajesh, J.P. Morgan Securities LLC, *Big Data and AI Strategies: Machine Learning and Alternative Data Approach to Investing* (May 2017).

138. A.T. Kearney, *Big Data and the Creative Destruction of Today's Business Models* (2013), at 2, available at: <https://www.atkearney.com/documents/10192/698536/Big+Data+and+the+Creative+Destruction+of+Today+s+Business+Models.pdf/f05aed38-6c26-431d-8500-d75a2c384919> (discussing Oracle forecast).

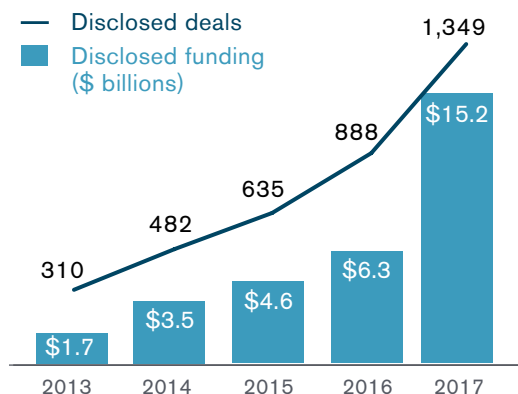
139. Id.

Since 2012, more than a billion more people have been added to the internet (2.5 billion people connected to the internet in 2012 compared to 3.7 billion people in 2017).<sup>140</sup>

- The proliferation of mobile devices and other internet connected devices (e.g., wearable devices, household appliances, components in industrial production), sometimes referred to as the “internet of things.” Globally, there are an estimated 27 billion devices (including smartphones, tablets, and computers) currently connected to the internet, with expectations for 125 billion connected devices by the year 2030.<sup>141</sup> These devices are enabling new streams of data that are being used by businesses to effectively digitize many dimensions of interaction in our physical world. Information from cars, phones, cameras, watches, manufacturing plants, are all being collected and available for analysis.

These factors are highly interwoven. The sheer magnitude of data that is now available demands analytical tools, like AI, to capably process and make use of the vast amounts of information, which is only expected to accelerate in volume, velocity, and variety. In some use-cases, for example, manual processes are simply unusable given the amount of data that exists. Cloud service providers, recognizing that many cloud-service users are also in need of adequate analytical tools, are providing various services designed to enable users to deploy an array of AI capabilities.<sup>142</sup>

Figure 8: Global Investment Trends in Artificial Intelligence



Source: CBInsights, *Top AI Trends to Watch in 2018*, at 25.

## Deployment in Financial Services

Investment in AI and machine learning has been accelerating over the past several years with a large share of such investment focused on firms looking to deploy AI and machine learning in financial services. Adoption of AI within financial services is driven by a number of factors such as the large and growing availability of data within financial services, including through third-party consumer financial data aggregators discussed elsewhere in this report, and the expectation that the use of machine learning and AI will increasingly be a driver of competitive advantage for firms through both improving firm's efficiency by reducing costs and enhancing the quality of financial services products demanded by

140. Id.

141. IHS Markit, *The Internet of Things: A Movement, Not a Market* (Oct. 2017), at 2, available at: [https://cdn.ihs.com/www/pdf/IoT\\_ebook.pdf](https://cdn.ihs.com/www/pdf/IoT_ebook.pdf). For projections that do not consider computers and phones at: Gartner, Inc., *Press Release – Gartner Says 8.4 Billion Connected “Things” Will be in Use in 2017, up 31 Percent from 2016* (Feb. 7, 2017), available at: <https://www.gartner.com/newsroom/id/3598917>.

142. See, e.g., Amazon Web Services, *Amazon Machine Learning Documentation*, available at: <https://aws.amazon.com/documentation/machine-learning/>; Microsoft Azure, *Azure AI: Artificial Intelligence Productivity for Virtually Every Developer and Scenario*, available at: <https://azure.microsoft.com/en-us/overview/ai-platform/>; Google Cloud, *Cloud Machine Learning Engine*, available at: <https://cloud.google.com/ml-engine/>; and IBM, *AI, Machine Learning and Cognitive Computing Services*, available at: <https://www.ibm.com/services/artificial-intelligence>.

customers.<sup>143</sup> Global banks, for example, report they expect application of these tools to deliver long-term cost efficiencies, risk management benefits, and revenue expansion opportunities.<sup>144</sup>

An extensive array of AI and machine learning use-cases are being considered and deployed within financial services, spanning the front-end (customer-facing) to back-office operations of a broad-set of financial services activities. These use-cases include:<sup>145</sup>

**Risk mitigation and surveillance:** Financial institutions and regulators, for example, are using machine learning-enabled software to help conduct surveillance of trader behavior by combining transaction data and unstructured text (e.g., e-mail, messaging) and voice data to help identify suspicious trading activities.<sup>146</sup> Machine learning may additionally be used to help reduce fraud and conduct surveillance for money-laundering and other illicit financing risks. Financial regulators are also beginning to employ machine learning to enhance their own analysis and understanding of economic and financial markets.<sup>147</sup>

**Enhancing investment analysis, trading strategies, and operations:** Machine learning-based software can also be used to augment human investment analysis in a variety of ways. One firm's product allows users to ask simple text questions (like an internet search engine) to generate instant correlation analyses between a broad span of potential market-moving data and financial asset prices, which could be used to greatly accelerate investment analyses.<sup>148</sup> Other use-cases include optimizing trade execution<sup>149</sup> and portfolio management and trading strategies at quantitative-oriented asset managers and hedge funds.<sup>150</sup>

143. PricewaterhouseCoopers, *Top Financial Services Issues of 2018* (Dec. 2017), available at: <https://www.pwc.se/sv/pdf-reports/finanssiell-sektor/top-financial-services-issues-of-2018.pdf> (discussion of artificial intelligence and digital labor).

144. Laura Noonan, *AI in Banking: The Reality Behind the Hype*, Financial Times (April 12, 2018) ("Noonan AI in Banking").

145. For further examples, see Lex Sokolin, *Autonomous NEXT, #Machine Intelligence & Augmented Finance: How Artificial Intelligence Creates \$1 Trillion of Change in the Front, Middle and Back Office of the Financial Services Industry* (Apr. 2018); Michael Chui et al., McKinsey Global Institute, *Notes from the AI Frontier: Applications and Value of Deep Learning* (Apr. 2018), available at: <https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-applications-and-value-of-deep-learning>; Darrell West and John R. Allen, Brookings Institution, *How Artificial Intelligence is Transforming the World* (Apr. 2018), available at: <https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/>.

146. Tony Sio, Nasdaq, *Changing the Game: Artificial Intelligence in Market Surveillance*, blog post (Apr. 2017), available at: <http://business.nasdaq.com/marketinsite/2017/Changing-The-Game-Artificial-Intelligence-In-Market-Surveillance.html>.

147. See, e.g., Andrew Haldane, Bank of England, *Will Big Data Keep Its Promise?* (Apr. 2018), available at: <https://www.bankofengland.co.uk/-/media/boefiles/speech/2018/will-big-data-keep-its-promise-speech-by-andy-haldane.pdf>.

148. See Antoin Gara, *Wall Street Tech Spree: With Kensho Acquisition S&P Global Makes Largest A.I. Deal In History*, Forbes (Mar. 6, 2018), available at: <https://www.forbes.com/sites/antoinegara/2018/03/06/wall-street-tech-spree-with-kensho-acquisition-sp-global-makes-largest-a-i-deal-in-history/>.

149. See Laura Noonan, *JPMorgan Develops Robot to Execute Trades*, Financial Times (July 31, 2017).

150. See Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications* (Nov. 1, 2017), at 18, available at: <http://www.fsb.org/wp-content/uploads/P011117.pdf>.

**Customer-interface:** Many financial services firms are employing chat-bots, which are digital customer-facing assistants that are powered by machine learning software that takes advantage of advancements in natural-language processing. For example, customers can text message with a bank through a messaging platform (and voice as well) in a conversational style to engage in certain account services. While current services are fairly limited in U.S. applications, expectations are that these systems will evolve to enable a much richer set of customer-facing services.<sup>151</sup>

**Underwriting decisions:** Firms have begun to employ machine learning based models to assist in underwriting decisions for purposes of extending credit to consumers and small businesses. Insurance firms are also using these techniques to price and market insurance products.

While many of these efforts remain in the early stages of testing and deployment, several use-cases appear poised for more wide-spread adoption. Within the banking industry, for example, large percentages of U.S. banks report either current or planned AI deployment within the next 18 months across the following use-cases: more than 60% in biometrics, about 60% in fraud & security detection, about 55% in chatbots or robo-advisers; and about 35% in voice assistants.<sup>152</sup>

### **Issues and Recommendations**

The expected rapid adoption of AI and machine learning within the financial services industry, and the economy more broadly, raises a number of important policy considerations.

#### **Benefits and Risks from Competition in AI and Big Data**

Firms expect that the effective use of AI, machine learning and big data analysis will be a key source of competitive advantage, which is spurring investment and competition.<sup>153</sup> Smaller firms may now be able to compete providing new algorithms, in part because barriers to develop such software have declined with the availability of affordable data processing capacity. Traditional financial services players may be able to leverage their product expertise while technology firms may be able to leverage their experience and deployment in AI in other contexts. Investment managers may look to employ new data sources or tools to deliver improved relative investment performance.<sup>154</sup> This multi-faceted competition can provide benefits to end-users and consumers of financial services through more affordable and higher-quality products that are more personalized and provided with greater overall convenience. The development of AI is expected to yield substantial benefits

151. Brian Patrick Eha, *This is How Financial Services Chatbots are Going to Evolve*, American Banker (May 26, 2017), available at: <https://www.americanbanker.com/news/this-is-how-financial-services-chatbots-are-going-to-evolve>.

152. See Citigroup Global Markets Inc., *Bank of the Future: The ABCs of Digital Disruption in Finance* (Mar. 2018) (citing Business Insider Intelligence, *AI in Banking and Payments* (Feb. 2018)).

153. PricewaterhouseCoopers, *Artificial Intelligence and Digital Labor in Financial Services*, available at: <https://www.pwc.com/us/en/industries/financial-services/research-institute/top-issues/artificial-intelligence.html> (last accessed June 1, 2018) (noting that about half (52%) of those in the financial services industry said they are currently making “substantial investments” in AI and that almost three out of four (72%) business decision makers expect that AI will be the business advantage of the future).

154. Tammer Kamel, Quandl, *Alternative Data – The Trend in Financial Data*, blog post (Apr. 12, 2016), available at: <https://blog.quandl.com/alternative-data> (discussing why alternative data can provide a source of potential ‘alpha’ for investment professionals).

to the broader economy and financial services.<sup>155</sup> PricewaterhouseCoopers estimated that by 2030, AI technologies could increase North American gross domestic product (GDP) by \$3.7 trillion and global GDP in \$15.7 trillion.<sup>156</sup> Within the financial services sector, large banks report that AI could help cut costs and boost returns.<sup>157</sup>

The strength and nature of the competitive advantages created by advances in AI could also harm the operations of efficient and competitive markets if consumers' ability to make informed decisions is constrained by high concentrations amongst market providers. Some analysts caution that the path of AI-based financial services technology may be similar to the path of other technology-based platforms that have trended toward high-levels of market concentration (e.g., in internet search and messaging).<sup>158</sup> An AI/machine learning model's performance improves through an abundance of data. Models that have a large market presence, therefore, have a built-in self-reinforcing advantage as their gains in market share improve the model's performance, which could in turn further their gain in market share.

### Legal and Employment Challenges

As the implications of the wide-spread adoption of AI become clearer, responsible parties are sounding alarms on potential complex downside risks.

**Detecting versus promoting fraud:** Even as AI and machine learning tools are being used to help detect fraud through risk models and image-recognition software, other applications of this technology could be used to circumvent fraud detection capabilities. For example, the digital rendering of fraudulent videos and audios may become indistinguishable from actual video and audio, which would raise significant challenges to authentication and verification functions within financial services.<sup>159</sup>

**Compatibility of legal and algorithmic decision-making:** One advantage of machine learning and AI methods is that they can potentially help avoid discrimination based on human interactions by ceding aspects of such decision making to an algorithm. However, these methods may also risk discrimination through the potential to compound existing biases, through training models with biased data and the identification of spurious correlations.<sup>160</sup> One consideration will be to ensure that decisions based upon an algorithm do not rely on incorrect, or perhaps even fraudulent, data,

155. McKinsey Global Institute, *Artificial Intelligence: The Next Digital Frontier* (June 2017), available at: <https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/how-artificial-intelligence-can-deliver-real-value-to-companies> (discussing the potential value of AI in other sectors of the economy).

156. PricewaterhouseCoopers, *Sizing the Prize: What's the Real Value of AI for Your Business and How Can You Capitalise?* (2017), available at: <https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf>.

157. See Noonan AI in Banking.

158. See, e.g., Sokolin.

159. Penny Crosman, *Bank of America, Harvard Form Group to Promote Responsible AI*, *American Banker* (Apr. 10, 2018), available at: <https://www.americanbanker.com/news/bank-of-america-harvard-form-group-to-promote-responsible-ai>.

160. See, e.g., Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (2016); Mikella Hurley and Julius Adebayo, *Credit Scoring in the Era of Big Data*, 18 *Yale J. L. & Tech.* 148 (2016).



or alternatively base decisions on proxies for illegal discrimination. Another key consideration is the appropriate role of humans in a decision-making process informed by algorithms that may be unable to provide an adequate explanation of its decision-making process nor self-correct for biases built into the data or model design.<sup>161</sup>

**Employment risks and opportunities:** Financial services firms expect the widespread adoption of AI and robotic automation processes to create significant demand for employees with applicable skills in AI methods, advanced mathematics, software engineering, and data science. However, executives also expect the application of these technologies to result in potentially significant job losses across the industry.<sup>162</sup>

### Data Privacy

The deployment of AI and machine learning models could result in a higher overall quality of financial services products being delivered to consumers. At the same time, the ubiquity and continuous flowing nature of data required to train AI and machine learning models can raise various data protection and privacy concerns. As data becomes ubiquitous, consumer's financial and nonfinancial data may be increasingly shared without their understanding and informed consent. Moreover, the power of AI and machine learning tools may expand the universe of data that may be considered sensitive as such models can become highly proficient in identifying users individually.<sup>163</sup>

### Regulatory Challenges Related to Transparency, Auditability, and Accountability

In the lending context and many other financial services use-cases, the underlying complexity of AI and machine learning-based models (often referred to as “black boxes”) raises challenges in the transparency and auditing of these models. Many U.S. laws or regulations have been designed around a baseline expectation of auditability and transparency that may not be easily met by these models. As these types of models are deployed in increasingly high-value decision-making use-cases, such as determining who gets access to credit or how to manage an investment portfolio, questions regarding how to maintain accountability become fundamental.

With respect to lending, for example, U.S. rules require that a creditor provide a notification when a borrower has been denied credit.<sup>164</sup> In light of the increasing complexity of machine learning, it can be challenging to express the underpinnings of these analytical insights to firms, borrowers, and regulators.<sup>165</sup>

161. See Nick Bostrom and Yudkowsky Eliezer, *The Ethics of Artificial Intelligence*, The Cambridge Handbook of Artificial Intelligence (Keith Frankish and William M. Ramsey, eds., 2014).

162. See Noonan AI in Banking.

163. *The Future: The Sunny and Dark Side of AI*, The Economist (Mar. 31, 2018).

164. Federal Trade Commission, *Big Data: A Tool for Inclusion or Exclusion?* (Jan. 2016), at 14, available at: <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>.

165. Eva Wolkowitz and Sarah Parker, Center for Financial Services Innovation, *Big Data, Big Potential: Harnessing Data Technology for the Underserved Market* (2015), available at: <https://s3.amazonaws.com/cfsi-innovation-files/wp-content/uploads/2017/02/13062352/Big-Data-Big-Potential-Harnessing-Data-Technology-for-the-Underserved-Market.pdf>.

In the investment management context, for example, machine learning-based algorithms and alternative data sources are currently being deployed in financial markets by a subset of quantitative-oriented funds, with the expectation of increased adoption by other such funds. While the application of these tools could yield valuable investment insights for some investment portfolios and activities, the opacity of the models may raise challenges for supervisors and users of these models to monitor risk and understand how they may interact with one another, particularly in times of broad market stress.<sup>166</sup>

### *Recommendations*

Treasury recognizes that the increased application of developing AI and machine learning technologies can provide significant benefits by improving the quality of financial services for households and businesses and supplying a source of competitive strength for U.S. firms. Regulators, therefore, should not impose unnecessary burdens or obstacles to the use of AI and machine learning and should provide greater regulatory clarity that would enable further testing and responsible deployment of these technologies by regulated financial services companies as the technologies develop.

The Administration has made harnessing AI and high-performance computing, including machine learning and autonomous systems, a federal research and development priority.<sup>167</sup> In May 2018, the White House hosted a summit of more than 100 senior government officials, technical experts, and business leaders to discuss policies to support continued American innovation in AI across industrial sectors.<sup>168</sup> Participants at the summit, including Treasury, recognized the importance of enabling high-impact, research and development efforts to advance AI. Treasury recommends that financial regulators engage with the Select Committee on Artificial Intelligence,<sup>169</sup> in addition to pursuing other strategic interagency AI efforts. Engagement in such efforts should emphasize use-cases and applications in the financial services industry, including removing regulatory barriers to deployment of AI-powered technologies. Other potential issues to consider as part of that engagement include: an appropriate emphasis on human primacy in decision making for higher-value use-cases relative to lower-value use-cases, the importance of cost-benefit assessments for regulatory actions, preparation of the work force for the trend toward digital labor, transparency of model use for consumers, robustness against manipulation (e.g., in market contexts), and accountability of human beings.

166. See Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications* (Nov. 1, 2017), at 18 and 33-34, available at: <http://www.fsb.org/wp-content/uploads/P011117.pdf>.

167. Office of Management and Budget, *Fiscal Year 2019 Analytical Perspectives*, at 236, available at: <https://www.whitehouse.gov/wp-content/uploads/2018/02/spec-fy2019.pdf>.

168. The White House Office of Science and Technology Policy, *Summary of the 2018 White House Summit on Artificial Intelligence for American Industry* (May 10, 2018), available at: <https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf>.

169. The Select Committee is chaired by the White House Office of Science and Technology Policy, the National Science Foundation (NSF), and the Defense Advanced Research Projects Agency (DARPA). Senior federal officials participating on the Select Committee include the Undersecretary of Commerce for Standards and Technology, the Undersecretary of Defense for Research and Engineering, the Undersecretary of Energy for Science, the Director of NSF, and the Directors of DARPA and the Intelligence Advanced Research Projects Activity as well as representatives from the National Security Council, the Office of the Federal Chief Information Officer, and the Office of Management and Budget.

# **Aligning the Regulatory Framework to Promote Innovation**





## Overview

Technological innovation in the provision of financial services is creating opportunities to serve customers and markets more efficiently. However, the regulatory framework, for banks and nonbanks alike, must evolve to enable innovation on an orderly and sustainable basis. Nonbank financial service providers generally operate within a largely state-based regulatory regime requiring compliance with a disparate set of standards across individual states and territories that can be cumbersome and produce conflicting guidance for entities operating on a national basis.<sup>170</sup>

Innovation will best flourish if the current federal and state regulatory models evolve to keep pace with technological change. This evolution could include efforts by the states to harmonize their regulatory and supervision regimes; the Office of the Comptroller of the Currency's (OCC) special purpose national bank charter; and encouragement of the bank partnership model with fintech firms.

As financial services continue to be shaped by new technologies and business models, the traditional distinctions between permitted banking activities and other information-intensive digital activities are being tested, which will require flexible and effective regulatory approaches. Existing bank regulations and supervision of a broad spectrum of third-party technology service providers and relationships require additional attention to enable innovative partnerships and provide for more streamlined and tailored oversight.

## Challenges with State and Federal Regulatory Frameworks

### State Oversight and Harmonization Challenges

State laws and regulations currently provide the primary regulatory framework for many types of nonbank financial services firms, including firms deploying new and innovative technologies and products. State banking departments and financial regulatory agencies oversee various types of nonbank firms and activities, including: consumer finance companies, money services businesses (MSBs), debt collection businesses, and mortgage loan originators. State financial regulators' authorities over these nonbank firms can include firm licensing requirements; safety and soundness regulation, including permissible investments and required reserves; product limitations; interest rate limits; examinations; and enforcement authority for violation of state and federal laws.

### Lending and Servicing

State financial regulators regulate nonbank consumer lenders primarily for purposes of consumer protection. Nonbank lenders that operate in multiple states must acquire lending or credit licenses for each applicable state. As a result, geographic expansion can only generally be accomplished through repeated licensing efforts, each with a state-specific regulatory regime. States' lending

---

170. With the passage of Dodd-Frank, the Bureau of Consumer Financial Protection was granted expansive federal regulatory powers over nonbank financial services companies, but Dodd-Frank did not preempt state laws that provided greater consumer protection. See 12 U.S.C. § 5551(a).

license applications often require submission of a business plan and financial statements, credit reports and fingerprints from the firm's officers, and a surety bond. State regulators oversee lenders active across a broad set of consumer lending segments, including short-term, small dollar, mortgage, auto, and other unsecured credit.

State-specific requirements would benefit from additional harmonization. For example, some states may require a physical office presence,<sup>171</sup> some require broker licenses or licenses for commercial loans,<sup>172</sup> and others set different maximum loan interest rate requirements.<sup>173</sup> Differences in usury limits imposed by states also materially impact which products are available to consumers.

### Payments and Money Transmission

Money transmitters are generally nonbank firms that transfer or receive funds on behalf of individuals. As with nonbank credit providers, individual states each license and supervise money transmitters with the general goals of maintaining the safety and soundness of these businesses, ensuring financial integrity, protecting consumers, and preventing ownership of money transmitters for illicit purposes (e.g., money laundering or fraud). The definition of money transmission can vary significantly by state (as can exceptions from the definition), posing operational challenges and potentially chilling economically beneficial money transmission activity — particularly innovative, technology-based money transmission. If a statutory exception does not apply, money transmitter licenses are required for numerous activities offered by nonbanking firms beyond just remittance services, to firms that could include online payment, digital wallet services, and bill payment services.<sup>174</sup>

As a general matter, any firm with a nationwide footprint (and especially those that have only a digital presence) will require a license in, and be subject to examination by, every state in which it operates. There are currently 49 states plus the District of Columbia and Puerto Rico that impose some sort of licensing requirement in order to engage in the business of money transmission or money services. As with lending and credit, money transmitter licensing requirements often vary by state, but generally include requirements to submit credit reports, business plans, and financial statements; and a requirement to maintain a surety bond to cover losses that might occur. Some states may also ask for information regarding policies, procedures, and internal controls. These

171. Arizona, Hawaii, Missouri, North Carolina, Nevada, South Carolina, and Texas require a physical office to obtain a license as a mortgage lender or broker.

172. California, New York, and Vermont require a license for commercial lenders, while most states only require a license for consumer loans.

173. See Loanback.com, *Usury Laws by State* (Mar. 2, 2011), available at: <http://www.loanback.com/category/usury-laws-by-state>.

174. Money transmitters are defined for federal purposes by FinCEN for purposes of the Bank Secrecy Act, 31 U.S.C. § 5311 et seq. Money transmitters generally include any person that provides money transmission services or is engaged in the transfer of funds. The term money transmission services means the acceptance of currency, funds, or other value that substitutes for currency and transmission to another location or person by any means. Money transmitters are considered to be a type of "money services business" (MSB). MSBs are certain nonbank financial institutions that do business in any of the following capacities: money transmitter; currency dealer or exchange, check casher, provider or seller of prepaid access, issuer or seller of traveler's checks, or money orders; U.S. postal service. See 31 C.F.R. § 1010.100(ff).

requirements do not apply to banks because state money transmitter statutes generally expressly carve them out.<sup>175</sup>

### Focus Areas for Improvement in the Regulatory Framework

Nonbank firms have raised concerns with the lack of regulatory harmonization among the current state-based regimes, particularly with respect to the provision of credit and money transmission activities. As innovation allows firms to more easily serve customers across a broad national market, these concerns are becoming more acute. The lack of harmonization could also perpetuate a disparate regulatory regime between nonbanks and banks otherwise competing in similar product and geographic markets.<sup>176</sup>

State licensing processes can create inefficiencies, including requirements for fingerprinting in multiple states (although this has been improved through coordination) and requests from states for the financial statements of the multinational parent company's individual board members. The applications for licenses require similar but sufficiently distinct information that forces firms to materially revise each application for each state.

Compliance across this fragmented state-regulatory landscape can be costly for firms (some firms report that all-in licensing costs range from \$1 million to \$30 million), separate and beyond the time lost from such efforts, which can result in forgone business opportunities.<sup>177</sup> In addition to these up-front costs, nonbank firms must actively monitor regulatory requirements across all the states in which they operate, pay fees to the applicable state regulators, and deploy significant resources to accommodate multiple state examinations, which can result in as many as 30 different state regulators per year examining a firm.<sup>178</sup> These cumulative challenges of operating in the state-based regulatory regime result not only in excessive regulatory costs, but also constrain the ability of nonbank firms, including start-ups, to innovate and to scale nationally.

Banks and credit unions also face regulatory challenges that may impede innovation. In contrast to the largely state-based regime facing nonbank financial services providers, banks and credit unions operate within a largely federal regulatory regime, which provides for greater levels of uniformity, and accordingly efficiency, on some dimensions. Yet banks face a substantially different regulatory regime, which is heavily focused on bank-specific activities. These regulations are structured to ensure the safety and soundness of the bank or credit union, and may include capital and liquidity standards, deposit insurance requirements, and limitations on permissible activities. This regulatory framework exists for multiple reasons, including the need to protect taxpayers because of banks' access to Federal Deposit Insurance Corporation (FDIC) insurance and the Federal Reserve's discount window. Additionally, banks and credit unions serve as the back-up source of

175. Each state may have different statutory language. See, e.g., National Conference of Commissioners on Uniform State Laws, *Uniform Money Services Act* (Feb. 25, 2005), at § 103(4), available at: [http://www.uniformlaws.org/shared/docs/money%20services/umsa\\_final04.pdf](http://www.uniformlaws.org/shared/docs/money%20services/umsa_final04.pdf).

176. For a discussion of how state-based regulation can result in inefficiency, unlevel competition, and differences in the availability of financial services across states, see Brian Knight, *Federalism and Federalization on the Fintech Frontier*, 20 Vanderbilt J. of Ent. & Tech. Law 129 (2017), at 185-198.

177. GAO Fintech Report, at 45.

178. *Id.*

liquidity for other financial firms, act as critical (though not exclusive) transmission vehicles for monetary policy, and have exclusive access to Fedwire and other payment systems.

The cumulative impact of these regulations, while critical for achieving public policy goals such as safety and soundness, can impede innovation at banking organizations. These limitations may impede the ability of banks and credit unions to partner with nonbank financial institutions, develop new platforms within the organization, or offer new and innovative services to customers.

## Modernizing Regulatory Frameworks for National Activities

### Improving the Clarity and Efficiency of Our Regulatory Operating Models

Treasury has identified several principles for updating the regulatory operating models available for firms in our financial services ecosystem. First, modernization needs to focus on producing efficient regulation to enable dynamic innovation. Second, any solution must provide sufficient flexibility to recognize the diversity of the scale, maturity, and activities of firms. Finally, any solution should recognize the benefits of both federal and state based-approaches to financial services oversight.

The diversity of U.S. financial services firms requires that any regulatory solution allow for recognition of a broad spectrum of business models. Some firms may be ready to absorb the costs of regulation that attach to a federally insured depository institution, whether through federally chartered banks or state-chartered banks, including traditional banks and industrial loan companies. Other firms may prefer having a primary federal regulatory regime but without the acceptance of federally insured deposits, such as through the OCC's proposed special purpose national bank charter. Still other firms may desire to partner with an existing bank, rather than pursue a banking charter themselves. Finally, firms may have business models that do not require national approaches and may prefer therefore to maintain a predominantly state-based system of regulation. Primary drivers of these decisions may include the type of activity engaged in, the maturity of the firm, and business strategies and objectives.

The United States has a long and complex history of state and federal regulation in financial services. The U.S. banking system began through state charters. In many ways, the state-based system acts as a laboratory of innovation for firms, which should be preserved. In fact, the state model has allowed for numerous nonbank firms to build a local product in a state, and then subsequently expand as the product gained broader market appeal. State regulators also have greater proximity to their constituents and can be more responsive to the needs and preferences of local consumers than regulators who do not have a local presence. Some of these advantages of local geographic experimentation and local government responsiveness should be preserved, particularly for firms that prefer the state-based approach.

Federal oversight would likely play a more prominent role in the regulation of fintech firms if these firms elect to pursue a banking charter. Federal banking regulations should be appropriately tailored to allow firms to provide financial services to drive economic growth while ensuring appropriate oversight. Thought should also be given to the appropriate regulatory structure taking into

consideration organizational structure, services provided, risk profile, and the need to promote fair competition between different types of organizations providing similar services.

### A Tailored Regulatory Solution

Treasury supports several specific regulatory approaches that would provide greater clarity and flexibility in the regulatory operating model for firms looking to provide financial services. Taken together, these approaches balance the key requirements for modernizing the regulatory operating model for U.S. firms. These approaches include:

- **State Harmonization.** An acceleration in state regulators' and legislatures' efforts to harmonize the existing patchwork of state licensing and oversight of nonbank financial services companies,
- **Bank Charters.** The OCC should move forward with thoughtful consideration of applications for special purpose national bank charters,
- **Partnerships.** Enabling further partnerships between banking organizations and fintech companies, and
- **Bank Innovation.** Updating existing bank regulations to enable innovations commensurate with the rapid changes in how banks are partnering with and investing in fintech and technology firms and how banks are themselves becoming increasingly like technology firms.

## Issues and Recommendations

### State Harmonization Efforts

State regulators have enhanced the regulatory efficiency of state regulation over the years. In the early 1980s, state regulators participated in a nationwide licensing system for the securities industry, known as the Central Registration Depository.<sup>179</sup> In the years leading up to nationwide banking, states were already working to move toward a more harmonized system. By 1991, for example, 33 states permitted nationwide banking and 13 permitted regional banking.<sup>180</sup>

Past and current efforts to promote greater state harmonization have spanned efforts to address differences across state laws, for example with regard to licensing and supervision.

### Model Law Adoption

One approach for state harmonization involves the drafting of a model law that state legislatures would then enact and implement in each respective state. This would ensure that each state has similar laws and requirements for each type of firm or activity. For example, in July 2017, the Uniform Law Commission approved and recommended for adoption by all states a Uniform

179. Conference of State Bank Supervisors, *Letter to Treasury on NonBank and Innovation Report* (Apr. 9, 2018), available at: <https://www.csbs.org/letter-treasury-non-bank-and-innovation-report> ("CSBS Letter").

180. See U.S. Department of the Treasury, *Modernizing the Financial System: Recommendations for Safer, More Competitive Banks* (Feb. 5, 1991) at 7, available at: [http://3197d6d14b5f19f2f440-5e13d29c4c016cf96cbbfd197c579b45.r81.cf1.rackcdn.com/collection/papers/1990/1991\\_0205\\_TreasuryBanks.pdf](http://3197d6d14b5f19f2f440-5e13d29c4c016cf96cbbfd197c579b45.r81.cf1.rackcdn.com/collection/papers/1990/1991_0205_TreasuryBanks.pdf).

Regulation of Virtual Currency Businesses Act.<sup>181</sup> The effectiveness of the model law approach turns on widespread adoption by the states. Previous efforts have met with mixed results. For example, the Commission's Money Services Act of 2000 has to date been enacted by only 10 states (plus Puerto Rico and the U.S. Virgin Islands).<sup>182</sup>

### Nationwide Multistate Licensing System

In more recent years, state regulators have been focused on developing greater cooperative approaches for the supervision of nonbank financial services companies. One of the primary efforts of state regulators to achieve such enhanced cooperation has been the Nationwide Multistate Licensing System (NMLS), which is a technology platform that functions as a system of record for the licensing activities (application, renewal, and surrender) of 62 state or territorial government agencies.<sup>183</sup> The NMLS is used by state regulators to reduce duplicative regulatory requirements, promote greater information sharing and coordination, and maintain consumer protections and the strength and resilience of regulated firms.

The NMLS began with a focus on the mortgage industry. The NMLS began operations in January 2008 and was formed by the Conference of State Bank Supervisors (CSBS) and the American Association of Residential Mortgage Regulators. At that time, the NMLS was originally the Nationwide Mortgage Licensing System and was primarily designed for the mortgage industry. The NMLS began in 2005 as a voluntary system used by seven state agencies and then expanded to 50 when it went live in 2008. Congress subsequently enacted the Secure and Fair Enforcement for Mortgage Licensing Act (SAFE Act), which established a registration requirement and minimum licensing requirements for mortgage loan originators and mortgage reporting.<sup>184</sup>

The CSBS and state regulators further built out the NMLS framework beyond the mortgage industry. For example, the CSBS and state regulators have expanded the scope of industries covered within the NMLS framework beyond even money transmitters, to also include consumer finance and debt collection. Some success has also been found using NMLS to manage licensing. As of year-end 2017, 38 states were using NMLS to manage their MSB licenses.<sup>185</sup> However, fewer state regulators participate in these other licensed activities than for the mortgage sector.<sup>186</sup> Beyond the scope of industries, NMLS has also enabled greater access to its data through the launch of a publicly available consumer access website in 2010 and through the sale of NMLS data to businesses that, in turn, sell data and loan origination products to mortgage market participants.

181. National Conference of Commissioners on Uniform State Laws, *Uniform Regulation of Virtual Currency Businesses Act* (July 2017), available at: [http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/2017AM\\_URVCBA\\_AsApproved.pdf](http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/2017AM_URVCBA_AsApproved.pdf).

182. See <http://uniformlaws.org/Act.aspx?title=Money%20Services%20Act> (website of the National Conference of Commissioners on Uniform State Laws tracking the status of enactment as of June 1, 2018).

183. State Regulatory Registry LLC, *2017 Annual Report*, available at: <https://nationwidelicencingsystem.org/NMLS%20Document%20Library/2017%20SRR%20Annual%20Report.pdf> ("NMLS 2017 Annual Report").

184. The SAFE Act was enacted as Title V of the Housing and Economic Recovery Act of 2008, Pub. L. No. 110-289, and codified at 12 U.S.C. §§ 5101-5116.

185. National Multistate Licensing System, *Money Services Businesses Fact Sheet* (Dec. 31, 2017), available at: <https://nationwidelicencingsystem.org/about/Reports/2017Q4%20MSB%20Fact%20Sheet.pdf>.

186. NMLS 2017 Annual Report.



### Efforts to Streamline Examinations

One example of how states have sought to harmonize examinations has been their approach to money transmitters and MSBs. Multi-state examinations started in earnest after the Money Transmitters Regulators Association (an association of state money transmitter regulators) executed a cooperative agreement in 2002 and an examination protocol in 2010<sup>187</sup> and FinCEN issued an MSB examination manual for the Bank Secrecy Act in 2008. As of March 2018, 48 states; Washington, D.C.; Puerto Rico; Guam; and the Virgin Islands have signed the Money Transmitter Regulators Association agreements.<sup>188</sup> The agreements provide for a taskforce that helps to coordinate the joint exams and determine which state will lead a joint exam. Joint exams generally include fewer than 10 states, and states that are not part of a joint exam will come in to do individual exams (or be a part of a different joint exam). State examiners generally jointly examine for common components such as Bank Secrecy Act/anti-money laundering, information technology, and corporate governance; there is a separate section of the exam for specific state law issues.

### Vision 2020 Commitment and Passporting

State regulators have launched a multi-step effort to develop a 50-state licensing and supervisory system by 2020, known as “Vision 2020.” Vision 2020 is largely a response to the various state regulatory harmonization challenges raised by firms regarding the current state-based regulatory regime for nonbank financial companies. The core components of this effort include:<sup>189</sup>

- Establishing a Fintech Industry Advisory Panel that would be a vehicle to provide state regulators important insight on the Vision 2020 and related efforts to improve state regulation.
- Re-designing the existing NMLS platform through further automation and enhanced data and analytical tools.
- Harmonizing multistate supervision processes through adoption of best practices and, critically, the development of a comprehensive state examination system that will allow state regulators to share various pieces of information including: exam schedules, ratings, supervisory concerns, and reports of examination. This system is tentatively scheduled to go live in the spring or summer of 2019.<sup>190</sup> For money-transmission oversight, according to the CSBS, “If one state reviews key elements of state licensing for a money transmitter — IT, cybersecurity, business plan, or background check<sup>191</sup> — then other participating

187. Conference of State Bank Supervisors and Money Transmitters Regulators Association, *The State of State Money Service Businesses Regulation and Supervision* (May 2016), at 11, available at: <https://www.csbs.org/sites/default/files/2017-11/State%20of%20State%20MSB%20Regulation%20and%20Supervision%202.pdf>.

188. CSBS Letter, at 15.

189. Conference of State Bank Supervisors, *Vision 2020 for Fintech and Non-Bank Regulation* (Jan. 7, 2018), available at: <https://www.csbs.org/vision2020>.

190. See NMLS 2017 Annual Report, at 15.

191. This effort would also include examinations for compliance with the federal Bank Secrecy Act.

states agree to accept the findings.”<sup>192</sup> Seven states have initially signed on to this agreement as an initial pilot program.<sup>193</sup>

- Other efforts to, for example, assist state banking departments and promote greater industry awareness.

One solution that could be accomplished through the Vision 2020 process is the idea of “passporting” and reciprocity of state licenses. Such a solution would involve the states harmonizing licensure and supervision laws and regulations, creating a system whereby a licensee in one state could have their home state’s license accepted, or passported, to other states within the reciprocity pact.<sup>194</sup> Passporting represents a path through which states could effectuate a system of licensing that is conducive to a national business model while still retaining oversight at the state level.

### *Recommendations*

State regulators play an important and valuable role in the oversight of nonbank financial services firms. Treasury supports state regulators’ efforts to build a more unified licensing regime and supervisory process across the states. Such efforts might include adoption of a passporting regime for licensure. However, critical to this effort are much more accelerated actions by state legislatures and regulators to effectively reduce unnecessary inconsistencies across state laws and regulations to achieve much greater levels of harmonization. Treasury recommends that if states are unable to achieve meaningful harmonization across their licensing and supervisory regimes within three years, Congress should act to encourage greater uniformity in rules governing lending and money transmission to be adopted, supervised, and enforced by state regulators. Congress has used a similar model previously, such as the establishment of minimum mortgage licensing requirements under the SAFE Act.<sup>195</sup>

### OCC Special Purpose National Bank Charter

The OCC’s special purpose national bank charter, proposed in 2016, presents an attractive option for firms interested in the benefits of having a single primary federal regulator. This type of banking charter may provide a more efficient, and at least a more standardized, regulatory regime, than the current state-based regime in which they operate. The OCC special purpose national bank charter, however, does present key policy and regulatory considerations, discussed below.

192. Conference of State Bank Supervisors, *Press Release – State Regulators Take First Step to Standardize Licensing Practices for Fintech Payments* (Feb. 6, 2018), available at: <https://www.csbs.org/state-regulators-take-first-step-standardize-licensing-practices-fintech-payments>.

193. Georgia, Illinois, Kansas, Massachusetts, Tennessee, Texas, and Washington.

194. Brian Knight, Mercatus Center, *Modernizing Financial Technology Regulations to Facilitate a National Market*, Mercatus Center (July 2017), at 5, available at: [https://www.mercatus.org/system/files/knight\\_-\\_mop\\_-\\_modernizing\\_fintech\\_regulations\\_-\\_v2\\_1.pdf](https://www.mercatus.org/system/files/knight_-_mop_-_modernizing_fintech_regulations_-_v2_1.pdf).

195. 12 U.S.C. §§ 5104-08



## Overview

The OCC released a proposal for a special purpose national bank charter for financial technology companies and solicited comments on that proposal in December 2016. As proposed,<sup>196</sup> the OCC special purpose national bank charter would allow charter applicants that make loans or engage in payments activities to:

- Adhere to a uniform set of national banking rules, rather than seeking state-by-state lending or money transmission licenses, with frequently conflicting requirements, or partnering with a bank to access bank charter benefits (e.g., the ability to export interest rates);
- Operate without FDIC deposit insurance, to the extent applicants would not take deposits; and
- Be subject to the same standards and level of supervision as similarly situated national banks, including capital, liquidity, consumer protection and financial inclusion requirements based on the business model and risk profile of the chartered company.

Marketplace lenders (MPLs) and payment companies are examples of fintech firms that may be interested in applying for the OCC special purpose national bank charter. MPLs may be attracted to an OCC special purpose national bank charter because it would reduce licensing and regulatory cost by consolidating supervision under one primary national regulatory structure, which would allow them to efficiently provide credit to consumers and businesses across the country. Payments companies might look to the charter to obviate the need to obtain money transmission licenses in all 50 states. The charter might also allow them to acquire potentially more efficient access to payment systems, reduce operating costs and provide national scalability.

## Chartering Authority

Under the National Bank Act (NBA), the OCC has authority to grant charters for national banks to engage in the “business of banking,” which the OCC has interpreted to include at least one of three “core banking functions” — taking deposits, paying checks, or lending money.<sup>197</sup> The OCC

196. The OCC special purpose national bank charter was proposed through a series of OCC announcements. See Office of the Comptroller of the Currency, *Exploring Special Purpose National Bank Charters for Fintech Companies* (Dec. 2016), available at: <https://www.occ.gov/topics/responsible-innovation/comments/special-purpose-national-bank-charters-for-fintech.pdf>; (“OCC Fintech Paper”); *Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective* (Mar. 2016), available at: <https://www.occ.gov/publications/publications-by-type/other-publications-reports/pub-responsible-innovation-banking-system-occ-perspective.pdf>; *Summary of Comments and Explanatory Statement: Special Purpose National Bank Charters for Financial Technology Companies* (Mar. 2017), available at: <https://www.occ.gov/topics/responsible-innovation/summary-explanatory-statement-fintech-charters.pdf> (“OCC Comment Summary”); *Draft Licensing Manual Supplement* (Mar. 2017), available at: <https://www.occ.gov/publications/publications-by-type/licensing-manuals/file-pub-lm-fintech-licensing-manual-supplement.pdf>.

197. See OCC Comment Summary, at 14. See also 12 U.S.C. § 24 (enumerating the powers of a national bank as “all such incidental powers as shall be necessary to carry on the business of banking”); 12 C.F.R. § 5.20(e)(1) (“A special purpose bank that conducts activities other than fiduciary activities must conduct at least one of the following three core banking functions: Receiving deposits; paying checks; or lending money.”).

has also exercised its authority to reach technology-based extensions of core-banking functions, such as facilitating programs electronically.<sup>198</sup>

### Key Regulatory Features

The OCC special purpose national bank charter could, as proposed, allow for the preemption of certain state laws and trigger baseline supervisory expectations that apply to any national bank including, for example: a business plan that must assess risks comprehensively; capital adequacy; liquidity; compliance risk management; consumer protection and fair lending compliance; financial inclusion; recovery and resolution planning; governance; and Bank Secrecy Act/anti-money laundering requirements.

The OCC could tailor compliance requirements under a special purpose national bank charter to better suit the safety and soundness risks posed by these institutions in light of the absence of FDIC insurance and potential business model differences.

- **Insured Deposit Related Differences (CRA, Resolution).** An OCC special purpose national bank chartered firm that does not obtain FDIC insurance (an uninsured national bank) would not present a direct risk to taxpayers through the FDIC's Deposit Insurance Fund. Moreover, under the terms of the CRA, such firms would not be subject to CRA requirements, nor be subject to resolution by the FDIC under the Federal Deposit Insurance Act. However, in its policy statement, the OCC noted that it would encourage special purpose national bank charter applicants to meet an ongoing financial inclusion standard of "provid[ing] fair access to financial services by helping to meet the credit needs of its entire community" through setting supervisory expectations and making such a commitment a condition for charter approval.<sup>199</sup> As to resolution, the OCC would, as provided for under the NBA, resolve such an uninsured national bank. The OCC issued a final rule in December 2016 that clarifies the framework for such a resolution.<sup>200</sup>
- **Potential Tailoring of Safety and Soundness Rules (Capital, Liquidity).** The OCC noted that it would consider adapting capital requirements for an applicant as necessary to adequately reflect the risks of the planned business model as it does with all national banks.
- **State Laws and Consumer Concerns.** The NBA preempts state usury laws for federally chartered national banks. However, certain other consumer protections and state contract law may apply, including state laws regarding foreclosure.<sup>201</sup>

Other key features of the OCC proposal that would require some clarifications are:

198. OCC's authority on these issues has been challenged in two lawsuits that have been dismissed on ripeness grounds. See *Conference of State Bank Supervisors v. Office of the Comptroller of the Currency*, No. 17-0763, 2018 WL 2023507 (D.D.C. Apr. 30, 2018); *Vullo v. Office of the Comptroller of the Currency*, No. 17-cv-3574, 2017 WL 6512245 (S.D.N.Y. Dec. 12, 2017).

199. See OCC Fintech Paper, at 12; see also 12 C.F.R. § 5.20(f)(1)(ii).

200. The OCC's resolution framework would apply to any type of uninsured national bank that the OCC charters. See *Receiverships for Uninsured National Banks* (Dec. 15, 2016) [81 Fed. Reg. 92594 (Dec. 20, 2016)].

201. See for example 12 U.S.C. § 7.4008 (non-real estate lending).

- **Regulatory Coordination.** National banks, including special purpose national banks, are required (with limited exceptions) to become members of the Federal Reserve System. The Federal Reserve would have to assess whether an OCC special purpose national bank would be given access to the Federal Reserve payment systems.<sup>202</sup>
- **Activities Incidental to the Business of Banking.** The OCC has authority to define what activities are part of the business of banking or incidental to the business of banking.<sup>203</sup> The OCC indicated it would consider the permissibility of new activities for a special purpose national bank charter on a case-by-case basis.<sup>204</sup>

### *Recommendations*

Treasury recommends that the OCC move forward with prudent and carefully considered applications for special purpose national bank charters. OCC special purpose national banks should not be permitted to accept FDIC-insured deposits, to reduce risks to taxpayers. The OCC should consider whether it is appropriate to apply financial inclusion requirements to special purpose national banks. The Federal Reserve should assess whether OCC special purpose national banks should receive access to federal payment services. It is important that a charter not provide an undue advantage to newly chartered firms relative to the banks that have operated within the existing regulatory system for years. Striking the right balance to appropriately enable a tailored regulatory framework is important.

### **Bank Regulatory Oversight of Third-Party Relationships**

Banking regulators' oversight of banking organizations' relationships with third-parties stems from (1) their general safety and soundness authority over the banking organization and (2) the Bank Service Company Act, which grants federal banking regulators authority to examine and regulate the provision of certain services that a third-party service provider, which may include fintech partners, performs for regulated institutions.<sup>205</sup>

This supervisory regime is generally designed to be comprehensive in overseeing how banking organizations interrelate with third-party vendors and service providers.

Banking regulators administer this oversight through:

- Regulation and supervision of banking organizations. This guidance directs banks to have a comprehensive, enterprise risk management process that addresses such third-party relationships (for example ensuring compliance with applicable laws and regulation); and
- Direct supervision of a subset of service providers (significant service providers and regional service providers).<sup>206</sup>

202. Governor Lael Brainard, *Where Do Banks Fit in the Fintech Stack* (Apr. 28, 2017), available at: <https://www.federalreserve.gov/newsevents/speech/brainard20170428a.htm>.

203. 12 U.S.C. § 24.

204. OCC Fintech Paper, at 4.

205. 12 U.S.C. § 1867(c).

206. Federal Financial Institutions Examination Council, *Supervision of Technology Service Providers* (Oct. 2012), at 1, available at: [https://ithandbook.ffiec.gov/media/274876/ffiec\\_itbooklet\\_supervisionoftechnologyserviceproviders.pdf](https://ithandbook.ffiec.gov/media/274876/ffiec_itbooklet_supervisionoftechnologyserviceproviders.pdf) ("FFIEC TSP Handbook").

Critically, a banking organization's use of a third-party service provider does not diminish the responsibility of the bank to ensure that the activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations, just as if the institution were to perform the activities in-house.

### Drivers of Third-Party Risk

Technological innovation, specialization, cost, and today's competitiveness all contribute to financial institutions' increased outsourcing to third parties. Some of this outsourcing includes specific functions (e.g., human resources, taxes, law, and information technology), customer related activities, and lines of business. This has led to new forms of risk as financial institutions become more reliant on others to perform business functions, support services, and technology provisioning. For example, as technology providers increase, cyber risks may increase because of the introduction of new vulnerabilities that may be exploited as vectors for intrusions. In recent years, regulators' and firms' attention to third-party risks and relationships have increased for a variety of reasons, including the following:

- **Consumer-Related Concerns.** Banks have increasingly been held responsible for the sales practices of third parties that marketed products on their behalf.<sup>207</sup> These incidents have heightened the importance of managing third-party risks related to consumer compliance and protecting a firm's reputation.
- **Information Security Concerns.** Several high profile data breaches have increased attention to cyber risks. In 2014, Target acknowledged that the payment information of 40 million customers, along with up to 70 million customers' personal information, had been breached as the result of a third-party vendor's systems being compromised.<sup>208</sup> In 2013, regulators notified banking customers of a serious data breach that occurred in 2011 at one of the largest payments information processors used by banks, Fidelity National Information Services.<sup>209</sup>
- **Other Operational Risks.** Dependence on third parties also raises concerns regarding concentration risk, the reliance on a few vendors to enable the execution of critical functions and services, and highlights the need for contingency planning for both the

207. See, for example, Bureau of Consumer Financial Protection, *Press Release – Consumer Financial Protection Bureau Orders Santander Bank to Pay \$10 Million Fine for Illegal Overdraft Practices* (Jul. 14, 2016), available at: <https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-orders-santander-bank-pay-10-million-fine-illegal-overdraft-practices/>; Bureau of Consumer Financial Protection, *Press Release – CFPB Orders American Express to Pay \$59.5 Million for Illegal Credit Card Practices* (Dec. 23, 2013), available at: <https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-american-express-to-pay-59-5-million-for-illegal-credit-card-practices/>; Bureau of Consumer Financial Protection, *Press Release – CFPB Orders Chase and JPMorgan Chase to Pay \$309 Million Refund for Illegal Credit Card Practices* (Sept. 19, 2013), available at: <https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-chase-and-jpmorgan-chase-to-pay-309-million-refund-for-illegal-credit-card-practices/>.

208. Testimony of John Mulligan, Executive Vice President and Chief Financial Officer of Target Corporation, before the Senate Judiciary Committee (Feb. 4, 2014), available at: [https://corporate.target.com/\\_media/TargetCorp/global/PDF/Target-SJC-020414.pdf](https://corporate.target.com/_media/TargetCorp/global/PDF/Target-SJC-020414.pdf).

209. Tracy Kitten, OCC: *More Third-Party Risk Guidance*, Bank Info Security (Aug. 26, 2014), available at: <https://www.bankinfosecurity.com/occ-more-third-party-risk-guidance-a-7233>.

financial firm and the vendor. A range of high-profile risk events, including large storms, have heightened the need to have up-to-date and well tested contingency plans in the event of an IT failure within the technology infrastructure. Such planning is critical to mitigate the consequences of power outages, flooding, and data redundancies. In addition to these risks, firms expressed concerns regarding resourcing, including facilities and workforce, and ensuring the availability of the requisite supporting services.

- **Financial Technology Partnerships.** Banking organizations have increasingly partnered with technology providers and other vendors to drive down costs (e.g., the adoption of cloud services or other IT outsourcing) or promote increased tech-enabled financial services (e.g., the growing partnership with digital lenders).

### Regulatory Responses

Regulators have also been responding to these developments. Since 2008, each of the prudential banking regulators have separately issued updated guidance with respect to third-party vendor risk management. The OCC and the Federal Reserve separately issued specific guidance on third-party risk in 2013, while the FDIC issued guidance in 2008 (and proposed guidance on third-party lending in 2016 that it never finalized).<sup>210</sup> The Federal Financial Institutions Examination Council, an interagency group, and other agencies have also taken relevant action.<sup>211</sup>

### Challenges Identified with the Current Approach

A number of challenges have been identified with the banking regulators' current approach to third-party vendors and service providers.

210. Office of the Comptroller of the Currency, Risk Management Guidance for Third Party Relationships, OCC Bulletin 2013-29 (Oct. 2013), available at: <https://www OCC.gov/news-issuances/bulletins/2013/bulletin-2013-29.html>; Office of the Comptroller of the Currency, *Supplemental Exam Procedures for Third Party Relationships*, OCC Bulletin 2017-7 (Jan. 2017), available at: <https://www OCC.gov/news-issuances/bulletins/2017/bulletin-2017-7.html>; Office of the Comptroller of the Currency, *Frequently Asked Questions to Supplement OCC Bulletin 2013-29*, OCC Bulletin 2017-21 (Jun. 2017), available at: <https://www OCC.gov/news-issuances/bulletins/2017/bulletin-2017-21.html>; Federal Reserve Board of Governors, *Guidance on Managing Outsourcing Risk* (Dec. 5, 2013), available at: <https://www federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf>; Federal Deposit Insurance Corporation, *Examination Guidance for Third-Party Lending* (July 29, 2016), available at: <https://www fdic.gov/news/news/financial/2016/fil16050a.pdf>; Federal Deposit Insurance Corporation, *Third-Party Risk – Guidance for Managing Third-Party Risk*, FIL-44-2008 (June 6, 2008), available at: <https://www fdic.gov/news/news/financial/2008/fil08044.html>.

211. Karen Ross and Doug Posey, Davis Wright Tremaine LLP, *FFIEC Releases New Booklet for the Supervision of Technology Service Providers* (Nov. 19, 2012), available at: <https://www paymentlawadvisor.com/2012/11/19/ffiec-releases-new-booklet-for-the-supervision-of-technology-service-providers/>; Brian J. Hurh, Davis Wright Tremaine LLP, *FTC Order Against Fraudulent Payment Processor Joins Growing List of Regulatory Actions Involving Third Party Service Providers* (Mar. 19, 2013), available at: <https://www paymentlawadvisor.com/2013/03/19/ftc-order-against-fraudulent-payment-processor-joins-growing-list-of-regulatory-actions-involving-third-party-service-providers/>; Bureau of Consumer Financial Protection, *Service Providers*, Bulletin 2012-03 (April 13, 2012), available at: [https://files.consumerfinance.gov/f/201204\\_cfpb\\_bulletin\\_service-providers.pdf](https://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf) (Dodd-Frank grants the Bureau supervisory and enforcement authority over supervised service providers); Compliance Bulletin and Policy Guidance; 2016-02, *Service Providers* (Oct. 19, 2016) [81 Fed. Reg. 74410 (Oct. 26, 2016)].

*Regulatory Efficiency and Uncertainties*

Both banks and service providers have raised concerns about the growing compliance costs related to third-party oversight. Significant service providers<sup>212</sup> have raised concerns about inefficiencies in oversight because they are overseen by both federal banking regulators and each bank to which they provide a service. Banks of all sizes have raised concerns about the cost of compliance because multiple banks subject the same vendors to similar third-party oversight, related due diligence, and other requirements.

Banking agencies' third-party guidance, while broadly similar, is also not entirely consistent. The inconsistencies can be compounded by the inconsistent application of standards by individual examination teams within agencies. Some areas of existing guidance that firms struggle to apply uniformly may include the scope of vendors or third-parties covered, the categorization of which partners should be subject to heightened risk-based attention, and the terms and conditions that banks are expected to require of these partners. Banks have also said there is some lack of clarity in how this regulatory framework applies to data aggregators (see the discussion on clarifying when data aggregators are subject to third-party guidance in the preceding chapter on Embracing Digitization, Data, and Technology).

Related to these inconsistencies in third-party oversight, banking organizations have raised concerns about the strict implementation of such guidance through the “trickle-down” of best practices (i.e., where the most stringent due diligence standards available are expected for many vendors). While the written guidance for third-party risk generally allows for risk-based or more tailored approaches, a number of factors contribute to more stringent de facto regulation. For example, banks looking to avoid criticism from their examiners might adopt a more uniformly stringent vendor oversight approach rather than trying to convince their examiners to permit a more tailored approach to vendor oversight.

*Technology Partnerships*

Smaller, nonbank fintech firms and banks have raised concerns that the overall burden of the third-party supervisory regime stifles the ability of new firms to partner with banks. For example, smaller and less mature nonbank start-up firms face requirements that are inappropriately tailored, such as having to complete the same due diligence information requests required of firms with significantly greater scale or complexity. Similarly, community banks have expressed concern about their capacity to undertake the requisite due diligence and ongoing vendor management (especially with larger vendors). At the same time, fintechs and banks have said that the third-party oversight framework is critical to overseeing risks in certain bank-fintech partnership activities, such as lending.

Cloud-related service relationships also appear to face some challenges. Some banking organizations have expressed difficulties in the deployment of cloud services because of the administrative burdens of getting multiple regulators on board or unclear recognition of independent audit and certification standards. Banks have noted that fintech partnerships may also be hindered by a lack of clarity about whether a third-party vendor's sub-contractors, such as a cloud-service provider

---

212. FFIEC TSP Handbook, at 1.



(i.e., a fourth party), must also meet due diligence requirements. Small fintech firms often lack a realistic ability to impose any such requirements upon such fourth-party vendors.

### *Recommendations*

Federal banking regulators should, in coordination, review current third-party guidance through a notice and comment process. U.S. banking regulators should further harmonize their guidance with a greater emphasis on (1) improving the current tailoring and scope of application of guidance upon third-party vendors to improve the efficiency of oversight and (2) enabling innovations in a safe and prudent manner. Such a review should specifically consider how to:

- Further develop the framework to regulate bank partnerships with fintech lenders to apply strong and tailored regulatory oversight while also supporting efforts by banks, particularly smaller community banks, to partner with fintechs.
- Provide greater clarity around the vendor oversight requirements for cloud service providers, including clarifying how third-party guidance should apply to a third-party's sub-contractors, like cloud service providers (i.e., fourth party vendors). Further discussion of cloud services oversight is addressed in the preceding chapter on Embracing Digitization, Data, and Technology.
- Support more secure methods for consumers to access their financial data, such as through API agreements between banks and data aggregators.
- Identify common tools banks can leverage as part of due diligence efforts, such as robust independent audits, recognized certifications, and collaboration among institutions in an effort to enhance efficiencies and reduce costs.
- Maintain ongoing efforts with other federal and state regulators to identify opportunities for harmonization as appropriate.

Looking ahead and recognizing the dynamic nature of financial technology developments, the banking regulators should be prepared to flexibly adapt their third-party risk relationships framework to emerging technology developments in financial services. Moreover, banking regulators should consider how to make examiners' application of interagency guidance on third-party relationships more consistent across and within the agencies.

### **Banks' Innovation Investments and the Scope of Permitted Activities**

The scope of permitted activities for banking organizations is generally very limited. Banks and their holding companies may only engage in activities specifically permitted by law and by their regulators. Federal banking laws that govern permissible activities, including investments in innovative financial technology partnerships, are varied and implemented through various federal and state regulators.

#### **Banks and Savings Associations**

In general, the National Bank Act establishes the scope of permissible activities for national banks, the Home Owners' Loan Act establishes the scope of permissible activities for federal savings associations, and the OCC can authorize additional permissible activities for both, in accordance

with applicable statutes.<sup>213</sup> The National Bank Act, in particular, allows national banks to engage in (1) the “business of banking” and (2) activities that are “incidental” to the conduct of such business.<sup>214</sup> The OCC has generally defined the statutory term “business of banking” dynamically over time, authorizing activities to allow national banks to keep pace with developments in the financial services marketplace and the needs of customers.<sup>215</sup>

The OCC, for example, recognized various financial market developments over time, including the authorization of various derivatives activities (e.g., advising, structuring and executing transactions in interest rate, equity swaps, currency, and commodity derivatives products), which enabled national banks to act as key intermediaries in the development of national and global derivatives markets to facilitate the hedging and transfer of risks. The OCC similarly recognized technology developments as it authorized various electronic, data storage and software-related activities (e.g., electronic bill payments).

The OCC has also indirectly affected the scope of permissible activities for state-chartered banks because state “wild card” laws, designed to maintain competitive parity between state banks and national banks, often grant state banks the same scope of permissible activities as has been made available to nationally chartered banks and savings associations.<sup>216</sup>

The Federal Deposit Insurance Act also augments permissible activities of state-chartered banks. It permits state-chartered banks to engage in certain activities permissible under state law but that are not permissible for national banks as long as the FDIC determines that “the activity would pose no significant risk” to the Deposit Insurance Fund and that the state bank meets “applicable capital standards prescribed by the appropriate Federal banking agency.”<sup>217</sup>

### Holding Companies

The Bank Holding Company Act (BHC Act) provides the statutory framework for the oversight of companies that control a bank with the aim of “protecting the safety and soundness of corporately controlled banks” and maintaining the general separation of banking and commerce.<sup>218</sup> As a result, the BHC Act authorizes a limited set of permissible activities for bank holding companies (BHC) and their affiliates, including (1) owning, managing, and controlling banks<sup>219</sup> and (2) engaging in activities that are “so closely related to banking as to be a proper incident thereto” (i.e., Section 4(c)(8) authorities).<sup>220</sup> BHCs that apply to become and qualify as a financial holding company

213. Office of the Comptroller of the Currency, *Activities Permissible for National Banks and Federal Savings Associations, Cumulative* (Oct. 2017), at 1, available at: <https://www.occ.gov/publications/publications-by-type/other-publications-reports/pub-other-activities-permissible-october-2017.pdf> (“OCC Cumulative”).

214. 12 U.S.C. § 24 (Seventh).

215. OCC Cumulative, at 1 (“[t]he business of banking is an evolving concept and the permissible activities of national banks similarly evolve over time”).

216. Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, *Report to the Congress and the Financial Stability Oversight Council Pursuant to Section 620 of the Dodd-Frank Act* (Sept. 2016), at 51, available at: <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20160908a1.pdf> (“Section 620 Report”).

217. 12 U.S.C. § 1831a(a)(1).

218. Section 620 Report, at 3.

219. 12 U.S.C. § 1843(a).

220. See 12 U.S.C. § 1843(c)(8).



benefit from a greater range of permissible activity under amendments made by the GLBA. The BHC Act, as amended by the GLBA, authorizes financial holding companies to engage in any activity that (i) the Federal Reserve, in consultation with the Secretary of the Treasury, determines is “financial in nature or incidental to such financial activity,” or (2) the Federal Reserve determines is “complementary to a financial activity and does not pose a substantial risk to the safety and soundness of depository institutions or the financial system generally.”<sup>221</sup> The BHC Act’s definition of “control” is critical to determining how the statute is applied and to which firms its activity restrictions apply. The BHC Act defines “bank holding company” as any company that controls a BHC or bank (not including Industrial Loan Companies).<sup>222</sup> A company generally controls a BHC or bank if the company: (1) owns more than 25% of any class of voting securities; (2) controls in any manner the election of a majority of the directors of the BHC or bank; or (3) exercises “a controlling influence” over the management or policies of the BHC or bank.<sup>223</sup> The Federal Reserve is responsible for determining what constitutes a “controlling influence.”

Figure 9: Overview of Authorities for Permitted Activities for Banking Organizations

Authorizing Federal Statute	Types of Permitted Activities	Interpreted by	Banking Organizations Subject to These Authorities
National Bank Act	Business of Banking	OCC	National Banks
	Incidental to the Business of Banking	OCC	National Banks
Federal Deposit Insurance Act	State-authorized activities that do not present risks to the Deposit Insurance Fund	State Regulators; FDIC	State-chartered Banks
Bank Holding Company Act (as amended by GLBA)	Managing and controlling an insured depository	Fed	All Bank Holding and Financial Holding Companies
	Closely related to banking or an incident thereto	Fed	All Bank Holding and Financial Holding Companies
	Financial in nature or incidental to a financial activity (e.g., securities and insurance)	Fed; Treasury	Financial Holding Companies
	Complementary to a financial activity and that does not present risks to inst. safety or the financial system generally	Fed	Financial Holding Companies

Source: National Bank Act, 12 U.S.C. §§ 24 and 24a; Federal Deposit Insurance Act, 12 U.S.C. § 1831a; Bank Holding Company Act, 12 U.S.C. § 1843. The permissible activities available to state-chartered banks is also determined by National Bank Act authorities because states have adopted laws that generally maintain parity with national banks’ scope of permitted activities.

221. 12 U.S.C. § 1843(k)(1); see also Section 620 Report, at 4-5.

222. 12 U.S.C. § 1841(a)(1).

223. 12 U.S.C. § 1841(a)(2).

### **Challenges with the Current Approach**

The restrictions on BHCs' permissible activities and investments present several interrelated challenges to innovation efforts by these firms.

Responding to market developments, BHCs have sought to invest in various financial technology-related firms to facilitate innovation. However, the current application of the BHC definition of "control" can discourage banks from such investments, because (1) fintech firms receiving BHC investments would like to avoid being considered a BHC affiliate because they would become subject to BHC-related regulations, including becoming subject to the applicable activities restrictions (discussed above); and (2) "control" can be difficult to determine because it relies upon Federal Reserve discretion under a process that is not sufficiently transparent. One of the considerations for defining "control" is the nature of the business relationship between the BHC and the firm receiving the equity investment. A BHC may seek to expand its business relationship with a successful fintech in which it has invested, yet doing so could then trigger "control" and the attendant BHC Act regulatory requirements.

More generally, banking organizations are increasingly required to deploy new technologies to serve customer needs and may do so through acquisitions, partnerships, or internal development. In particular, the highly dynamic nature of financial technologies today could result in banking regulators considering certain technology-based business activities impermissible or disagreeing on whether such an activity is permitted under each regulator's respective statutory authority.

### *Recommendations*

To support the ability of firms to flexibly adapt to new technology and market developments, Treasury recommends that the Federal Reserve consider how to reassess the definition of BHC control to provide firms a simpler and more transparent standard to facilitate innovation-related investments. This recommendation is consistent with public comments by Federal Reserve officials who have called for reassessing this issue. In addition, the banking regulators should interpret banking organizations' permitted scope of activities in a harmonized manner as permitted by law wherever possible and in a manner that recognizes the positive impact that changes in technology and data can have in the delivery of financial services.

# **Updating Activity-Specific Regulations**



## Overview

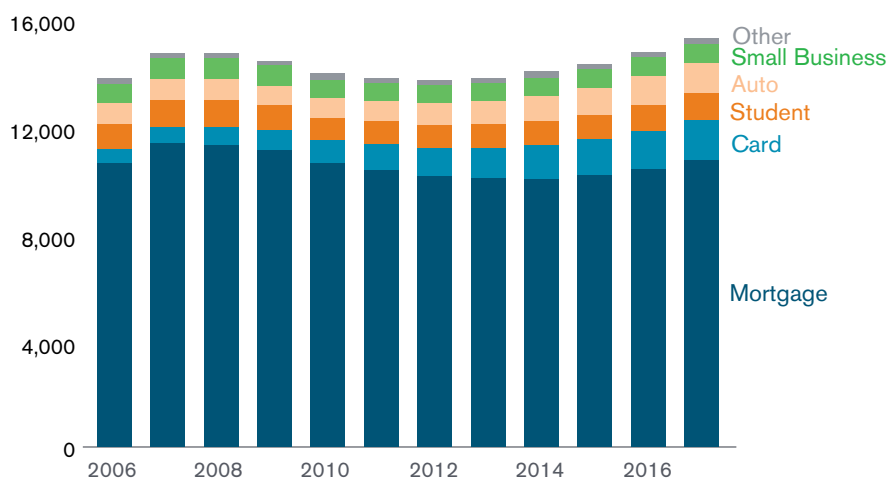
The U.S. regulatory framework for key financial service activities — lending, payments, and financial planning — requires meaningful reform to better enable the delivery of both digital and nondigital financial services to consumers and businesses. This chapter discusses these regulatory challenges and also identifies a number of specific recommendations aimed at improving the U.S. regulatory approach to lending, payments, and financial planning.

## Lending and Servicing

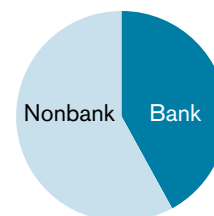
### Household and Small Business Lending

U.S. households and small businesses derive credit from a highly diverse mix of banks and nonbank firms. These firms provide secured and unsecured financing to their clients and perform a range of activities fulfilling that mission, including loan sourcing and origination, credit underwriting, and loan servicing. Although banks and nonbanks access securitization markets to monetize, through sale, pools of loans that they originate, the two sectors are generally differentiated by the ability to retain loans in portfolio. Banks are able to use deposit funding to reliably retain loans over their life in portfolio. By comparison, nonbanks generally have relatively limited balance sheet capacity that is provided by their equity capital and a combination of long-term debt and short-term secured borrowing. As such, they often take an approach that is typically referred to as an “originate to distribute” business model.

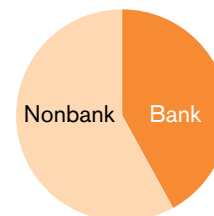
Figure 10: Mortgage, Consumer, and Small Business Credit Outstanding (\$ billions)



Financing of Mortgage



Financing of Nonmortgage Consumer Credit



Source: Federal Reserve Financial Accounts of the United States and Keith Horowitz and Jill Shea, Citi Research, *U.S. Banks and Credit Cards* (May 2018).  
Data as of Q4 2017. “Bank” denotes holdings by U.S.-chartered financial institutions.

Outstanding credit to households and small businesses exceeded \$15 trillion in 2017, of which residential mortgages accounted for \$10.6 trillion, cards and revolving credit accounted for \$1 trillion, student credit accounted for \$1.5 trillion, auto lending \$1.1 trillion, and small business lending \$700 billion. As shown in **Figure 10**, nonbank firms constitute a significant share of the overall funding provided across these lending segments. For example, nonbank companies account for 58% of the outstanding non-mortgage consumer loan market and 58% of the total residential mortgage market as of the first quarter of 2018.<sup>224</sup>

The share of nonbank lending in the U.S. residential mortgage market has been significant in recent decades due in part to the availability of warehouse financing and access to federally supported securitization programs for both private and government-supported loan programs, as conducted by Fannie Mae and Freddie Mac (the government-sponsored enterprises, or GSEs) and Ginnie Mae.<sup>225</sup> Of the \$1.8 trillion of mortgage originations in 2017, approximately 30% were retained in portfolio (generally by the originator).<sup>226</sup> Except for a relatively limited amount of issuance through private-label securities (PLS), most of the remaining 70% of 2017 volume was securitized by the GSEs or Ginnie Mae.<sup>227</sup> Nonbanks enjoy access to these securitization channels on largely equal footing to banks, which supports their ability to accommodate a large share of the origination market.

As discussed later in this chapter, the value proposition of marketplace lenders has resulted in their expansion, though these firms account for just a small fraction<sup>228</sup> of the much larger, multi-trillion dollar consumer credit market. Installment and payday lending activity have consistently been dominated by nonbanks, though banks and credit unions have historically provided some products that served similar short-term, small-dollar financing needs.

The U.S. capital markets are the largest, deepest, and most vibrant in the world. The nation's economy successfully derives a larger portion of business and consumer financing from its capital markets, rather than the banking system, than most other advanced economies. This includes reliable access to capital through securitization, a capital market evolution that has consistently been enabled by advances in information technology and the increased scope and cost-effectiveness of data storage and data management.

---

224. Keith Horowitz and Jill Shea, *Citi Research: U.S. Banks and Credit Cards* (May 2018).

225. For a discussion of how the rise of the secondary mortgage market and new federal regulation were contributors to a more unbundled housing finance system, see James R. Follain and Peter M. Zorn, *The Unbundling of Residential Mortgage Finance*, 1 J. of Housing Res. 63 (1990), available at: [https://www.innovations.harvard.edu/sites/default/files/jhr\\_0101\\_follain.pdf](https://www.innovations.harvard.edu/sites/default/files/jhr_0101_follain.pdf).

226. Treasury analysis based on data from Fannie Mae, Freddie Mac, the U.S. Department of Housing and Urban Development (HUD), and the U.S. Department of Veterans Affairs (VA).

227. Id.

228. Hannah Levitt, *Personal Loans Surge to a Record High*, Bloomberg (July 3, 2018), available at: <https://www.bloomberg.com/news/articles/2018-07-03/personal-loans-surge-to-a-record-as-fintech-firms-lead-the-way> (analyzing data from TransUnion).

### **Emerging Digitization of Lending**

Technological changes, including digitization, help drive changes to the lending landscape. Digital lending is increasingly prevalent throughout the household and small business lending market.

Nonbank digital lenders have gained outsized attention in recent years, driven in part by their rapid rate of growth and employment of new technology-intensive approaches to lending. These firms, such as marketplace lenders active in consumer and small business lending, have digitized the customer acquisition, origination, underwriting, and servicing processes. Moreover, these lenders are designing these digital services to provide customer experiences that are seamless and more timely than the techniques generally employed by traditional lenders. These changes also appear to reduce expenses, which lowers the cost of credit as well as providing greater access to credit.

In contrast, many financial institutions have yet to digitize their lending at a similar level.<sup>229</sup> For example, many banks have yet to fully digitize their origination processes. Banks report that less than half have digitized some aspects of their loan origination channels.<sup>230</sup> Moreover, the degree of digitization is much less comprehensive than new digital lenders. Even for banks that offer a digital origination channel, one industry survey found that the online features may vary, as 90% or more have digitized the application processes, but less than half provide for electronic signatures and document uploads, only a third provide online customer service, and less than 20% provide instant credit decisions.<sup>231</sup>

Key elements of digitization employed by new digital lenders are rapidly expanding across the wider banking and financial institution landscape and are expected to permeate all major lending segments over time. Within the mortgage industry, for example, Federal Reserve Bank of New York research staff estimates that stand-alone nonbank mortgage originators that offer a mortgage application process entirely online have expanded from 2% of the market in 2010 to 8% of the market in 2016.<sup>232</sup> Moreover, the partnerships between banks and new digital lenders have been expanding and are poised to increase over time, potentially serving to narrow the gap in practices between those two sectors for the benefit of both consumer and business segments.

### **Regulatory Landscape**

Lending is a highly regulated activity that is overseen by a large number of federal and state authorities in the United States.

Federal laws and regulations are extensive and cover fair credit reporting, fair debt collection, fair lending, credit practices, fair credit billing, consumer privacy, electronic signature, and electronic

229. See American Bankers Association, *The State of Digital Lending* (Jan. 2018), at 4-7, available at: <https://www.aba.com/Products/Endorsed/Documents/ABADigitalLending-Report.pdf> ("Traditional banks, particularly smaller ones, have typically lagged in technology adoption for lending, especially compared to up-and-coming fintech players"). Factors such as regulatory complexity and burdens, technology budgets, or third-party service provider reliance may contribute to the slow adoption of digitized lending by these institutions.

230. *Id.*

231. *Id.* at 9.

232. Andreas Fuster et al., *The Role of Technology in Mortgage Lending*, Federal Reserve Bank of New York Staff Report No. 836 (Feb. 2018), available at: [https://www.newyorkfed.org/medialibrary/media/research/staff\\_reports/sr836.pdf](https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr836.pdf).

transfer of funds, among others. Appropriately, there is a wide range of rules, such as consumer laws governing credit card issuers, mortgage lending and servicing, and automobile financing. At the federal level, the Bureau of Consumer Financial Protection (the Bureau) has authority to implement many federal statutes affecting consumers, in addition to requirements imposed by prudential regulators, namely the Board of Governors of the Federal Reserve System, OCC, FDIC, and National Credit Union Administration (NCUA). This multiplicity of regulatory authority is itself an outcome of a fragmented regulatory environment that at times can lead to overlap, duplication, and uncertainty.<sup>233</sup>

At the state level, there are licensing or registration requirements to operate within a state, state-specific maximum rates of interest on debt, state-specific loan value caps, and other consumer protections. State requirements are largely enforced by state financial regulatory authorities and state attorneys general.

Both federal and state regulators also have enforcement authorities that generally include authorities to prevent consumer financial service providers from engaging in unfair, deceptive, or abusive acts or practices.<sup>234</sup>

## Marketplace Lending

### Overview

A number of digitally focused lenders, often referred to as marketplace lenders or “fintech lenders,” have recently emerged and grown rapidly. Fintech lenders represented 36% of the unsecured consumer loan market in 2017<sup>235</sup> and around 2% of the small business market in 2014,<sup>236</sup> but in both instances are experiencing rapid rates of growth and market penetration. Marketplace lenders have generated significant attention due to many of the underlying features of these new lending models. Notable characteristics of the sector include newly branded firm and product launches; lack of reliance on brick-and-mortar branches for delivery of services; leverage of innovative technological approaches in marketing, sourcing, and fulfilling loan demand; and extensive use of data and data management techniques in credit underwriting processes.

Marketplace lenders operate with a diversity of business models that can generally be characterized by the asset classes and customer segments that they serve, the manner in which they access the national market, and their funding and risk-management strategies.

---

233. The FTC maintains some residual consumer protection authority over nonbank entities.

234. Dodd-Frank granted authority for the Bureau to bring enforcement actions against certain consumer financial service providers for “unfair, deceptive, or abusive” acts. See Dodd-Frank § 1031(a) [12 U.S.C. § 5531(a)]; see also Richard E. Gottlieb, Arthur B. Axelson, and Thomas M. Hanson, *Consumer Financial Services Answer Book*, Practising Law Institute (2016); American Bankers Association, *Consumer Lending, Seventh Edition* (2013) (discussing consumer laws impacting banking organizations).

235. Hannah Levitt, *Personal Loans Surge to a Record High*, Bloomberg (July 3, 2018), available at: <https://www.bloomberg.com/news/articles/2018-07-03/personal-loans-surge-to-a-record-as-fintech-firms-lead-the-way> (analyzing data from TransUnion).

236. Karen Gordon Mills and Brayden McCarthy, *The State of Small Business Lending: Innovation and Technology and the Implications for Regulation*, Harvard Business School Working Paper 17-042 (2016), at 48, available at: [https://www.hbs.edu/faculty/Publication%20Files/17-042\\_30393d52-3c61-41cb-a78a-ebbe3e040e55.pdf](https://www.hbs.edu/faculty/Publication%20Files/17-042_30393d52-3c61-41cb-a78a-ebbe3e040e55.pdf).



## Target Product Segments

The focus of marketplace lenders has primarily been the provision of unsecured credit to individuals (primarily utilized for the purpose of debt consolidation) and working capital to small businesses. However, business models are constantly evolving, and firms are beginning to expand into other product segments.

- **Unsecured Consumer.** Consumers access unsecured credit to pay down credit card or other debt, finance an online purchase, or manage variable expenses. A typical unsecured consumer loan in this market has a balance of \$14,000, an annual interest rate of 14.7%, and a 4-year term.<sup>237</sup>
- **Small-Dollar Consumer Lending.** A subset of unsecured consumer lenders focus on loans with shorter terms and higher interest rates that typically exceed a 36% annual percentage rate (APR), which is a widely used rate cap.<sup>238</sup> These loans typically have lower balances, below-average credit characteristics, and can be viewed as an alternative to other forms of lending, such as payday lending. These products serve a unique niche of consumers that may not have many alternatives to high-priced credit.
- **Student.** Student lenders primarily focus on refinancing traditional federal and private student loan debt with unsecured installment debt, generally focused on borrowers with prime FICO scores and several years of employment history who can qualify for lower rates (generally ranging from 3-7%).
- **Small Business.** Small business loans are typically less than \$500,000, with APRs that may average 7-48% and terms that range from six months to three years.<sup>239</sup>
- **Auto Finance.** This segment focuses on the \$1.1 trillion auto loan industry, which accounts for approximately 30% of nonmortgage consumer debt, and has been facilitated by the trend of migration of financing away from captive finance subsidiaries of manufacturers.<sup>240</sup>

## National Lending Business Model Strategies

Marketplace lenders currently lend to customers across the country through two primary models: (a) a bank partnership model in which a bank originates the loan, which is generally sourced and serviced by the marketplace lender and funded in a variety of manners; and (b) a direct lender model in which the marketplace lender acquires the applicable regulatory licenses in each U.S.

237. Testimony of Nathaniel L. Hoopes, Marketplace Lending Association, before the House Financial Services Committee (Jan. 30, 2018), at 3-4, available at: <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-nhoopes-20180130.pdf>.

238. The 36% rate cap for low-balance consumer lending emerged in the first half of the twentieth century in the United States and still exists today as a statutory maximum in many states. For additional information, see Lauren K. Saunders, National Consumer Law Center, *Why 36%? The History, Use, and Purpose of the 36% Rate Cap* (Apr. 2013), available at: <https://www.nclc.org/images/pdf/pr-reports/why36pct.pdf>.

239. S&P Global Market Intelligence, *2017 U.S. Digital Lending Landscape*, at 5-6 and company disclosures from Credibly, Kabbage, and OnDeck.

240. Financial Technology Partners, *Auto Fintech – The Emerging Fintech Ecosystem Surrounding the Auto Industry* (Dec. 2017), available at <https://www.ftpartners.com/fintech-research/auto-fintech>.



state in which it intends to do business. Under the bank partnership model, where, for example, a bank originates a loan and contracts with a marketplace lender to service the loan for the bank, federal law allows the bank, and federal jurisprudence allows the marketplace lender servicing the loan, to charge interest at the rate allowed by the laws of the state where the bank is located, even if the rate is higher than the rate allowed under the laws of the state where the loan is made.<sup>241</sup> Firms whose target loan products are at less of a risk of exceeding state usury limits, such as high-quality unsecured consumer installment loans, may find the direct licensing model relatively attractive.

### Other Business Model Features

Firms are differentiating themselves along other key dimensions from those cited earlier, including:

- **Credit Risk.** The predominant business model for marketplace lenders is an “originate to distribute” approach where there is limited long-term balance sheet retention of loans that they originate. This is similar to the business model of many traditional nonbank finance companies, such as independent mortgage bankers, that have consistently relied on securitization to fund their loan production. Most lenders, however, will retain servicing obligations on the outstanding loans — collecting payments from borrowers, remitting payments to creditors, and handling loss mitigation. Some firms may participate in the ongoing credit risk exposure by retaining a share of loans (or some proportional share of credit risk). This can arise from Dodd-Frank risk-retention requirements<sup>242</sup> or to better align interests with investing partners through a “skin-in-the-game” approach.
- **Funding Strategy.** Initially, marketplace lenders adopted a “peer-to-peer” funding model where individual loans were funded on digital platforms with individual investors, or “peers,” providing the majority of the capital. However, these distribution methods have evolved and now include a wide variety of both retail and institutional sources. While some firms have publicly traded equity, many are privately held. Marketplace lenders have a range of funding structures with a diverse set of investors such as banks, traditional asset managers, hedge funds, family offices, and high net worth individuals.
- **Credit Underwriting Models.** Nearly all marketplace lenders are built around online digital platforms designed to deliver rapid credit decisions. Some firms report the use of advanced analytical tools, such as machine learning, and various data sources such as bank transaction data, which includes real-time data linked from borrower accounts, model-based income estimates, and social media. An important element of underwriting for marketplace lenders is their use of aggregated data from third-party firms. Finally, many of the firms have departed from the strict use of credit ratings in favor of more data-driven techniques to drive their credit decision-making.

### Industry Growth

The growth of marketplace lending volumes and the corresponding securitization market has been on a strong upward trajectory since at least 2013. Estimates for cumulative loans originated since

---

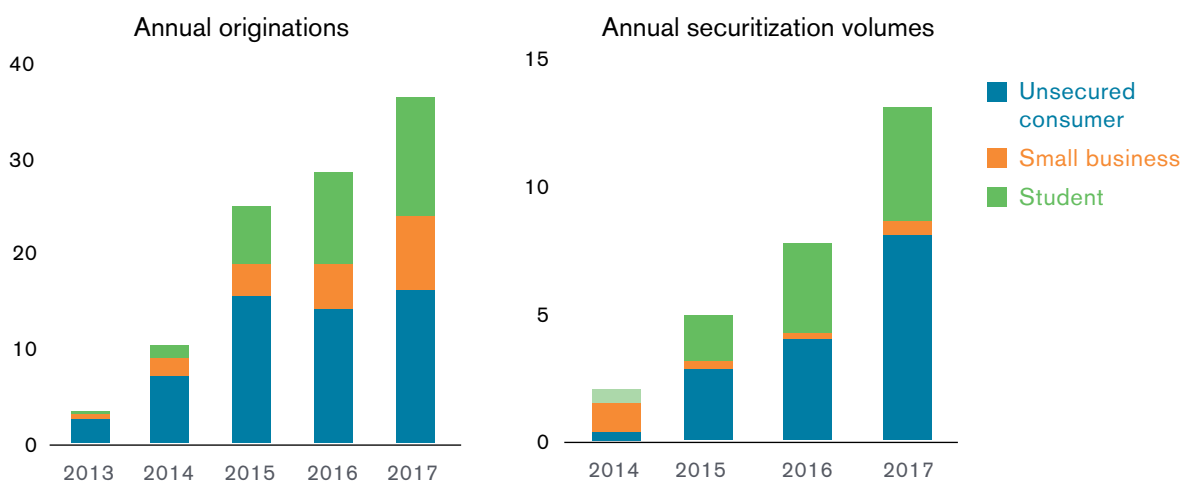
241. See 12 U.S.C. § 85; *Madden v. Midland Funding, LLC*, 786 F.3d 246, 250-253 (2d Cir. 2015), cert. denied, 136 S. Ct. 2505 (2016).

242. See 15 U.S.C. § 78o-11.

2014 total almost \$100 billion, according to industry data sources.<sup>243</sup> Of this amount, unsecured consumer lending is the largest category, amounting to about 50% of the total.<sup>244</sup> The securitization market for loans originated by marketplace lenders has similarly remained robust since securitization of this type of credit began to scale up in 2013.

In the first half of 2016, questions about the fragility of the funding model and the potential for conflicts of interest between investors and marketplace lenders led to a brief downturn in industry volumes. Since then, firms within the industry have worked to improve standards for their business models. In addition, better relationships with investors have allowed for concerns related to how loan characteristics are disclosed and how loans are allocated to investors to be addressed.

Figure 11: Market Growth of Marketplace Lending (\$ billions)



Source: S&P Global Market Intelligence for originations and PeerIQ for securitisation volumes. Each methodology is based on a different subset of marketplace lenders.

## Access to Credit

Early evidence indicates that these new lending channels have provided opportunities to expand credit to underserved segments. For example, a July 2017 study<sup>245</sup> found that new marketplace lenders have tended to expand credit in areas where bank branches have been on the decline. Moreover, this same study found that borrowers with similar credit risk profiles could obtain more favorably priced credit than alternatives such as credit cards. The study also found some evidence that the use of alternative credit data in this space allowed consumers with weaker traditional credit profiles to access credit. This study used data from the largest marketplace lender, Lending Club, and covered loans originated between 2007 and 2016.

243. S&P Global Market Intelligence, *2017 U.S. Digital Lending Landscape*.

244. *Id.*

245. Julapa Jagtiani and Catharine Lemieux, *Fintech Lending: Financial Inclusion, Risk Pricing, and Alternative Information*, Federal Reserve Bank of Philadelphia Working Paper 17-17 (2017), at 9-12, available at: <https://www.philadelphiafed.org/-/media/research-and-data/publications/working-papers/2017/wp17-17.pdf>.

The conclusions of this study, while preliminary, are not entirely unexpected given that the primary purpose of many marketplace loans is to refinance higher rate debt into less expensive debt. A number of marketplace lenders are specifically aiming to build underwriting models designed to achieve better results through providing lower priced credit for a given traditional FICO score. However, with only a few years of credit performance, these credit models have yet to be tested in various macroeconomic environments that would include either higher interest rates or a general economic downturn. Traditional financial institutions, including banks, have also begun sourcing deposits and extending credit through technology-enabled web platforms instead of utilizing their traditional brick-and-mortar footprint.

### Regulation and Supervision of Marketplace Lenders

Marketplace lenders may be supervised or overseen by federal and state agencies, directly or indirectly, depending on whether they utilize the bank partnership model or the direct lending model. Under the direct lending model, marketplace lenders must have licenses in most states where they do business and are subject to oversight in those states. Marketplace lenders that partner with banks may be subject to regulation and examination by federal banking regulators because they may be considered third-party service providers to a regulated banking entity<sup>246</sup> and by virtue of guidance pertaining to vendor management. Marketplace lenders that use the bank partnership model may remain subject to various state requirements, depending on the approaches used by state regulators.

All lenders, including banks and marketplace lenders, are subject to federal regulation in areas such as consumer protection, anti-money laundering, and securitization.

- **Consumer Protections:** For consumer lenders, a number of federal and state consumer protection requirements may apply, including the Truth in Lending Act, anti-discrimination requirements under the Equal Credit Opportunity Act, and provisions governing electronic transfers under the Electronic Funds Transfer Act. Marketplace lenders may also be subject to regulation under the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and other laws.
- **Anti-Money Laundering:** Marketplace lenders may have legal obligations to comply with the Bank Secrecy Act (BSA).
- **Securitization:** To the extent that marketplace lenders engage in securitization and offer those securities to the public, they may be subject to requirements under the Securities Act of 1933. These marketplace lenders must register the securities with the SEC, unless an exemption applies, and may be subject to risk-retention requirements.

Marketplace lenders, however, are not subject to numerous regulations that apply to banks, ranging from Community Reinvestment Act (CRA) requirements to prudential standards such as capital and liquidity requirements, deposit insurance requirements and assessments, resolution-planning requirements, and prompt corrective action requirements. These differences in regulation illustrate the challenge in determining an appropriate regulatory environment across providers of financial services.

---

246. See 12 U.S.C. § 1867(c)(1).

## Issues and Recommendations

### Key Considerations for the Bank Partnership Model

Some state regulators and consumer groups have expressed concern that the bank partnership model can harm consumers by allowing partnering firms to bypass state-based usury limits and other state requirements. Advocates note that some lenders operate with high-APR business models and offer loans whose APRs can exceed 100%, when fees are included.<sup>247</sup> Beyond enabling high-APR products, advocates note that in the past, such third-party partnerships have enabled some deceptive practices.<sup>248</sup>

Today's marketplace lenders, however, generally compete on the basis of providing a more affordable cost of credit (e.g., refinancing credit card and other debts) and an enhanced consumer experience. Many of these consumer-facing lenders generally operate below a 36% APR threshold and have stated that they would welcome a 36% APR cap for consumer lending, including loans originated through bank partnership arrangements.<sup>249</sup> Federal banking regulators are also paying closer attention to third-party service provider relationships, specifically lending arrangements, which should reduce the risk of potential abuse witnessed in past partnership arrangements.

Concerns about potentially harmful consumer lending practices also need to be considered against the possible benefits that such bank partnership relationships can provide to underserved borrower segments. Traditional lenders often provide lending experiences that are slower (e.g., because of extended wait times for credit decisions) and difficult due to cumbersome application and fulfilling processes. Many lenders may also not adequately serve certain lending segments, like smaller-balance, small business, or unsecured consumer borrowers with less-established credit histories.

Appropriately designed lending partnerships can leverage advantages from both banks and fintechs to improve upon the currently provided products. A recent study stated that 71% of banks were interested in partnering with a third-party digital platform for consumer loan origination and nearly 80% of banks were interested in using technology to support their small business lending.<sup>250</sup> For example, in the small-dollar lending segment, there appears to be market demand for banks to engage further in these markets<sup>251</sup>, as their cost of capital could be used to deliver products that are very competitive with rates charged by nonbank payday lenders.

247. Letter from the National Consumer Law Center et al. to the Federal Deposit Insurance Corporation, *Re: Comments on Proposed Financial Institutions Letter (FIL) 50-2106: Third-Party Lending* (May 2017), available at: <https://www.nclc.org/images/pdf/rulemaking/comments-fdic-3rdparty-lending.pdf>.

248. For example, the OCC took action in 2003 to address deceptive credit card programs marketed through a third-party vendor. Office of the Comptroller of the Currency, *News Release – OCC Concludes Case Against First National Bank in Brookings Involving Payday Lending, Unsafe Merchant Processing, and Deceptive Marketing of Credit Cards* (Jan. 21, 2003), available at: <https://www.occ.treas.gov/news-issuances/news-releases/2003/nr-occ-2003-3.html>.

249. Marketplace Lending Association, *Submission to the U.S. Department of the Treasury* (May 2018).

250. American Bankers Association, *The State of Digital Lending* (Jan. 2018), available at: <https://www.aba.com/Products/Endorsed/Documents/ABADigitalLending-Report.pdf>.

251. Pew Charitable Trusts, *Americans Want Payday Loan Reform, Support Lower-Cost Bank Loans* (Apr. 2017), available at: <http://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2017/04/americans-want-payday-loan-reform-support-lower-cost-bank-loans>.

Treasury recognizes that these existing bank partnership arrangements have generally enhanced the provision of credit to consumers and small businesses. Treasury makes the following specific recommendations to address constraints that would unnecessarily limit the prudent operation of partnerships between banks and marketplace lenders.

### Valid-When-Made/*Madden v. Midland*

Several legal issues have presented risks to the bank partnership model used by marketplace lenders. Specifically, in *Madden v. Midland Funding, LLC*, the Second Circuit held, in part, that the National Bank Act (NBA), which preempts state usury laws with respect to the interest a national bank may charge on a loan, did not preempt state-law usury claims against a third-party debt collector that had purchased the loan.<sup>252</sup> In its ruling, the court did not refer to the “valid when made” common law doctrine, which provides that a loan contract that is valid when it was made cannot be invalidated by any subsequent transfer to a third party. In an amicus brief at the certiorari stage, the United States took the view that the court of appeals “erred in holding that state usury laws may validly prohibit a national bank’s assignee from enforcing the interest-rate term of a debt agreement that was valid” when made under the applicable state law.<sup>253</sup> The Supreme Court declined to hear the case.

Because of *Madden*, the ability of nondepository third parties (e.g., marketplace lenders) to collect debts originated by depository institutions in reliance upon federal preemption of state usury law limits could be limited in the Second Circuit, ultimately restricting access to credit. In particular, unsecured consumer credit could be diminished because nonbank firms such as marketplace lenders may be discouraged from purchasing and attempting to collect on, sell, or securitize loans made in these states because of the risk of litigation asserting violations of state usury laws. One study of the impact of the *Madden* decision showed an observable relative decline in the growth of such loans in two states within the jurisdiction of the Second Circuit (New York and Connecticut),<sup>254</sup> compared to loans originated outside the Second Circuit.<sup>255</sup> If adopted more broadly, the rule announced in *Madden* could have broader implications well beyond marketplace lenders. Other credit markets that could be affected include bank/loan intermediary partnerships, debt collection activities, loan securitization activities, and simple loan transfers.<sup>256</sup> In response to *Madden*, some lenders are changing their lending and securitization activities by, for example, excluding loans from Second Circuit states in their pools altogether.<sup>257</sup>

---

252. See *Madden*, 786 F.3d at 249-53.

253. Am. Brief of the United States, *Midland Funding, LLC*, No. 15-610 (2016) (opposing certiorari). Although the United States argued that the Second Circuit erred, the government recommended that the petition for certiorari should be denied due to lack of a circuit split.

254. The Second Circuit encompasses New York, Vermont, and Connecticut.

255. Colleen Honigsberg, Robert J. Jackson, Jr., and Richard Squire, *How Does Legal Enforceability Affect Consumer Lending? Evidence from a Natural Experiment*, 60 J. L. & Econ. 673 (Nov. 2017).

256. *The Curious Case of Madden v. Midland Funding and the Survival of the Valid-When-Made Doctrine*, The Free Library. 21 N.C. Banking Inst. 1 (2017).

257. Honigsberg, Jackson, and Squire.

*Recommendations*

Treasury recommends that Congress codify the “valid when made” doctrine to preserve the functioning of U.S. credit markets and the longstanding ability of banks and other financial institutions, including marketplace lenders, to buy and sell validly made loans without the risk of coming into conflict with state interest-rate limits. Additionally, the federal banking regulators should use their available authorities to address challenges posed by *Madden*.

**True Lender**

Recent court decisions have exposed bank partnership models to uncertainty regarding whether the bank or nonbank partner is the “true lender” in providing credit.<sup>258</sup> Some of these decisions have deemed the nonbank partner as the true lender,<sup>259</sup> which subjects the nonbank partner to a range of state-based requirements including interest rate limits and licensing requirements.

The result of these decisions is a variety of standards for determining which entity is the true lender, leading to market uncertainties that harm the viability of the bank partnership model. For example, one court applied a “predominant economic interest” standard, under which the court analyzed the “totality of the circumstances to determine which entity had the predominant economic interest” in the loan.<sup>260</sup> However, compliance with such a standard on an ex-ante basis could be difficult because of nuances in how a court might determine the predominant economic interest. Firms enter into partnership arrangements in which they negotiate a range of terms and conditions based upon a variety of market, economic, and other considerations. The uncertainties created by these court cases create pressure to alter these partnership arrangements based upon nonmarket factors. Some marketplace lenders, for example, have already restructured their economic relationships with partnering banks to better account for the risks presented by these court cases. A fragmented legal structure creates an inefficient regulatory framework and significant compliance challenges for the bank partnership model.

**FDIC’s Proposed Third-Party Lending Guidance**

The FDIC published a letter on July 29, 2016, seeking comment on proposed guidance on third-party lending,<sup>261</sup> which was generally regarded as a response to the rise of online marketplace lenders establishing “bank partnership” funding models.

The proposed guidance would supplement and expand upon the principles outlined in the FDIC’s existing guidance for managing third-party risk by establishing specific expectations

258. See, e.g., *CashCall, Inc. v. Morrissey*, No. 12-1274, 2014 W. Va. LEXIS 587, at \*39-44 (W. Va. May 30, 2014).

259. See *id.*

260. See *id.*

261. Federal Deposit Insurance Corporation, *FDIC Seeking Comment on Proposed Guidance for Third-Party Lending*, FIL-50-2016 (July 29, 2016), available at: <https://www.fdic.gov/news/news/financial/2016/fil16050.html>. Financial Institution Letter 50-2016 is an unfinished proposal on third party lending from the FDIC.



for third-party lending arrangements.<sup>262</sup> For FDIC-supervised institutions that engage in significant lending activities through third parties, the proposal suggested increased supervisory attention, including a 12-month examination cycle, concurrent risk management and consumer protection examinations, offsite monitoring, and possible review of third parties on an ongoing basis.

Many marketplace lenders welcomed the FDIC's proposed guidance, as it would help affirm the validity of such bank partnerships by providing some federal supervision. Smaller banks note that such third-party lending guidance could also improve their ability to partner with fintech lenders. Banks more generally have raised concerns with the proposed guidance, such as with (1) the breadth of the proposed definitions of third-party lending, and (2) the potential for inconsistencies between banks where FDIC is the primary federal regulator and other types of banks because the FDIC would be the only regulator issuing such guidance.<sup>263</sup>

### *Recommendations*

Treasury recommends that Congress codify that the existence of a service or economic relationship between a bank and a third party (including financial technology companies) does not affect the role of the bank as the true lender of loans it makes. Further, federal banking regulators should also reaffirm (through additional clarification of applicable compliance and risk-management requirements, for example) that the bank remains the true lender under such partnership arrangements.

### **Credit Services**

An area of growing legal complexity for the bank partnership model is the provision of additional credit services. Some states apply licensing obligations to parties that are offering to arrange bank loans. In *CashCall, Inc. v. Maryland Commissioner of Financial Regulation*, the Maryland Court of Appeals ruled that CashCall, a payday loan broker, could not offer to arrange loans for Maryland residents for a fee without obtaining a license under the Maryland Credit Services Business Act (MCSBA).<sup>264</sup> In addition to requiring a license, the MCSBA prohibits a credit service business from assisting a consumer in obtaining a loan that exceeds the state's usury rate.<sup>265</sup> The MCSBA defines a "credit services business" to include any entity that obtains or assists a consumer in obtaining an extension of credit "in return for the payment of money or other valuable consideration,"<sup>266</sup> which the court interpreted to apply to the nonbank.<sup>267</sup> In a similar case in West Virginia, an online marketplace

---

262. The proposed guidance defines third-party lending as "a lending arrangement that relies on a third party to perform a significant aspect of the lending process." This is likely to include relationships with many online marketplace lenders. Further, the proposed guidance defines "significant" third-party lending arrangements as those, for example, that have a material impact on revenues, expenses, or capital; involve large lending volumes in relation to the bank's balance sheet; involve multiple third parties; or present material risk of consumer harm.

263. American Bankers Association, *Comment Letter Re: FIL-50-2016: FDIC Seeking Comment on Proposed Guidance for Third-Party Lending* (Oct. 26, 2016), available at: <https://www.aba.com/Advocacy/commentletters/Documents/ABACommentLetterFDICProposedThirdPartyLendingGuidance.pdf>.

264. *CashCall, Inc. v. Maryland Commissioner of Financial Regulation*, 139 A.3d 990, 1004-06 (Md. 2016).

265. Md. Code Com. Law § 14-1902(9).

266. Md. Code Com. Law § 14-1901(e).

267. *CashCall*, 139 A.3d at 1000.

lender entered into a settlement agreement with the West Virginia Attorney General for failing to obtain a credit service license and charging rates higher than permitted under state law.<sup>268</sup>

Since more than three-quarters of the states have a credit services organization law, these cases create legal uncertainty for the bank partnership model.<sup>269</sup> Instead of focusing on whether the nonbank is the true lender or whether the loan was valid when made by the bank, these cases inhibit the ability of the nonbank to partner with a bank.

### *Recommendations*

Treasury recognizes the role of state laws and oversight in protecting consumers, but such state regulation should not occur in a manner that hinders bank partnership models already operating in a safe and sound manner with appropriate consumer protections. Treasury recommends that states revise credit services laws to exclude businesses that solicit, market, or originate loans on behalf of a federal depository institution pursuant to a partnership agreement.

## **Mortgage Lending and Servicing**

### **Overview**

In the Banking Report, Treasury highlighted the steep increases in the cost to originate and service a mortgage loan as evidence of the burden of post-crisis mortgage regulation.<sup>270</sup> Treasury found that new regulations, combined with the use of enforcement actions, were effectively imposing a regulatory tax on the mortgage marketplace by requiring lenders to hold additional liability reserves and add compliance personnel, if not exit certain markets altogether. In response, Treasury offered recommendations to recalibrate and clarify rules where they were unnecessarily raising the cost and restricting access to mortgage credit.<sup>271</sup>

Concurrent with, and partially driven by, the introduction of the post-crisis regulatory regime, the primary mortgage market experienced a fundamental shift in composition and concentration. Traditional, deposit-based lender-servicers have ceded significant market share to specialty, nondepository mortgage lender-servicers, often referred to as nonbanks or independent mortgage banks, that are licensed and regulated for safety and soundness at the state level. In 2007, these mortgage banks originated just over 20% of all new single-family, first-lien mortgages and comprised 4 of the top 20 lenders.<sup>272</sup> By 2016, nondepository lenders accounted for just under half of new loans and 12 of the top 20 lenders.<sup>273</sup>

268. Chris Dickerson, *Morrissey's Office Reaches \$336K Settlement with Avant Online Lender*, W.V. Record (June 6, 2016), available at: <https://wvrecord.com/stories/510785558-morrissey-s-office-reaches-336k-settlement-with-avant-online-lender>.

269. Mike Whalen, Goodwin Procter LLP, *Bank Partnership Or Go It Alone?* (Aug. 23, 2016), available at: [https://www.goodwinlaw.com/publications/2016/08/08\\_23\\_16-bank-partnership-or-go-it-alone](https://www.goodwinlaw.com/publications/2016/08/08_23_16-bank-partnership-or-go-it-alone).

270. The Banking Report, at 92-102.

271. *Id.*

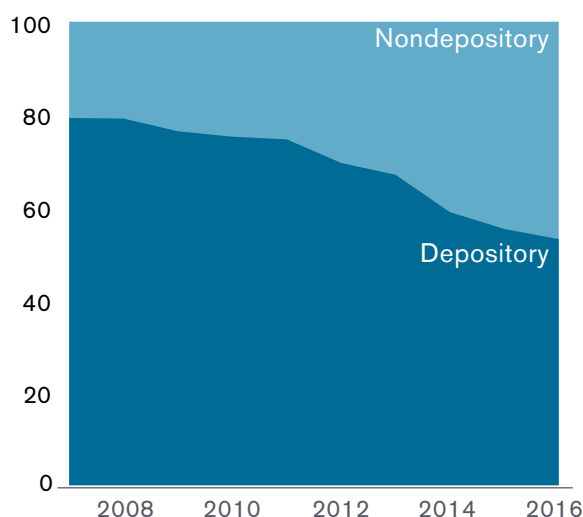
272. SNL and Home Mortgage Disclosure Act (HMDA) data.

273. *Id.*



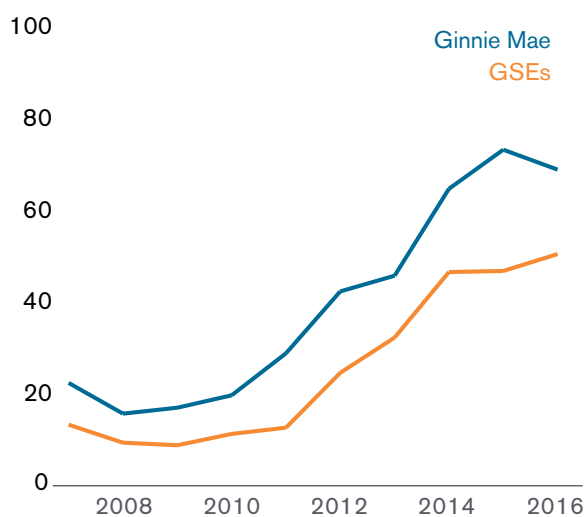
The growth of nonbank mortgage lenders and servicers has been facilitated by and is dependent on reliable access to the secondary mortgage market, mainly through federally supported securitization programs operated by the GSEs and Ginnie Mae. The increased market presence of nonbanks is evident in the share of originations delivered through these federally supported secondary market channels, with the nonbank share more than tripling between 2007 and 2016 to approximately 50% and 70% at the GSEs and Ginnie Mae, respectively.<sup>274</sup>

Figure 12: Depository v. Nondepository Share of All Mortgage Originations (percent)



Source: Home Mortgage Disclosure Act and Office of Financial Research analysis.

Figure 13: Nondepository Share of Mortgage Volume (percent)



Many of these nonbank lenders have also been early adopters of financial technology innovations that speed up and simplify loan application and approval at the front end of the mortgage origination process.<sup>275</sup> Metrics associated with the loan origination process highlight the degree to which speed and cost-saving enhancements are possible, with average closing timelines stretching well beyond a month and requiring hours of costly, labor-intensive processes even as digitized, automated technology exists to mitigate these challenges. Research examining the impact of financial technology on mortgage origination is limited given the nascent state of adoption; however, early evidence suggests positive impacts from the use of automated, digital processes, with a recent study

274. HMDA and Office of Financial Research analysis.

275. Marshall Lux and Robert Greene, *What's Behind the Non-Bank Mortgage Boom?*, Harvard Kennedy School M-RCBG Associate Working Paper Series No. 42 (June 2015), available at: [https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/working.papers/42\\_Nonbank\\_Boom\\_Lux\\_Greene.pdf](https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/working.papers/42_Nonbank_Boom_Lux_Greene.pdf).

finding that a digital front-end loan application shortened closing timelines by ten days or 20% of processing time without increasing default risk.<sup>276</sup>

While the growth of nondepository mortgage lenders and servicers has been supported by their early adoption of financial technology relative to their depository peers and access to the secondary mortgage market, nondepositories have also benefitted from the outright departure of many large depositories from certain segments of the mortgage market. This departure is concentrated in one of the key post-crisis channels to mortgage credit — the government-insured mortgage. Depositories have exited this market due to multiple factors that have unnecessarily raised the cost of engaging in this line of business, including substantial liability associated with the False Claims Act (FCA) and costly default servicing.<sup>277</sup>

Policymakers have an important role to play in the evolution of the mortgage lending and servicing marketplace by addressing regulatory challenges that discourage broad market participation and inhibit the adoption of beneficial technological developments. In its review of the impact of financial technology, innovation, and nonbanks on the mortgage market, Treasury has made the following findings:

- The adoption of financial technology and digital mortgage capabilities has the potential to improve the customer experience, shorten origination timelines, and deliver a more reliable, lower cost mortgage product;
- Current limitations on the acceptance of electronic mortgage promissory notes by key market participants limits the wider use and adoption of this technology, along with its attendant benefits for consumers and the marketplace;
- The mortgage production process is unnecessarily time intensive, with certain components prone to delays, which potentially could be relieved through policy changes conducive to further adoption of time- and cost-saving technology;
- State-level policy and regulatory differences across key components of the mortgage lifecycle create compliance uncertainty for lenders and servicers, increase costs, and inhibit the wider adoption of experience- and process-enhancing innovations;
- The use of the FCA to impose civil liability for violations of mortgage origination and servicing requirements has likely contributed to the exit of traditional commercial lenders from federal mortgage programs, raising the cost and limiting borrower access to mortgage credit for federally insured or guaranteed loans;
- Differences across loss mitigation programs and processes for federally supported mortgages, including those guaranteed or insured by the GSEs, Federal Housing Administration (FHA), U.S. Department of Veterans Affairs (VA), and U.S. Department of Agriculture (USDA), have the potential to negatively impact borrowers during periods

276. See Fuster et al., at 2.

277. See Neil Bhutta, Steven Laufer, and Daniel R. Ringo, Board of Governors of the Federal Reserve System, *The Decline in Lending to Lower-Income Borrowers by the Biggest Banks*, FEDS Notes (Sept. 28, 2017), available at: <https://www.federalreserve.gov/econres/notes/feds-notes/the-decline-in-lending-to-lower-income-borrowers-by-the-biggest-banks-20170928.htm>.

of financial hardship and could slow loss-mitigation responses during a subsequent period of sustained financial stress; and

- Federally supported mortgage programs exposed to nonbank counterparty credit risk could benefit from increased transparency into these counterparties' financial condition through greater standardization and reporting of key enterprise business and financial metrics.

## Mortgage Lending and the Digital Mortgage

Originating a mortgage loan requires a multitude of interactions across counterparties, vendors, intermediaries, investors, settlement agents, service and data providers, and, most importantly, the borrower. Navigating this process can be frustrating for the housing finance industry as well as for borrowers at the point of origination and over the life of the loan.

Lenders typically manage mortgage loan production through a proprietary or third-party loan origination system, which acts as a system of record for the origination process, helps sequence workflow, and integrates with vendor services. In some instances, services are required by law — such as property appraisals for depository institutions.<sup>278</sup> In other cases, the requirements of federal insurance and guaranty programs, federally supported secondary market securitization programs, and the Federal Home Loan Banks (FHLBs) set de facto industry standards. These standards are particularly important for originators dependent on the liquidity and reliable access to the secondary market provided through these programs.

Across credit markets, technological advances — including the development of machine learning, database capabilities, and the implementation of more automated processes — are changing the manner, speed, and security of transactions. The use of information technology in the mortgage market has existed for decades; however, the industry has been slow to adopt innovations common in other consumer credit markets. While there is growing use of digital platforms for borrowers to shop and apply for a mortgage online, further digitization of the origination process beyond this first step, including through the use of electronic notes, closings, and recordings, remains limited. Where the use of electronic files has occurred, it has often been by incorporating scanned images of paper documents as opposed to developing fully digital files.<sup>279</sup> However, the application of financial technology in the mortgage market is accelerating, challenging existing norms as the industry transitions toward automated, digital practices and processes that appeal to customer demands in today's digital age.

Both depository and nondepository lenders are increasingly moving toward a digital front-end, either through proprietary platforms or commercially available products, as evidenced by increased borrower use in recent years. According to a 2017 survey conducted by J.D. Power, the number of borrowers utilizing the initial component of a digital front-end by submitting a mortgage

---

278. See e.g., 12 C.F.R. § 323.3.

279. See Margo H.K. Tank and R. David Whitaker, DLA Piper LLP, *Enabled by Lenders, Embraced by Borrowers, Enforced by the Courts: What You Need to Know About eNotes* (updated as of May 1, 2018), at 1, available at: <https://www.mersinc.org/media-room-docman/1419-enote-white-paper-final-09062017/file>.

application online increased from 28% in 2016 to 43% in 2017.<sup>280</sup> Fewer lenders at present have the capability to complete the digital front-end, instead using a digital application to trigger referral to a loan officer to continue the process in a more traditional paper-based, as opposed to fully digital, fashion.<sup>281</sup>

The capabilities to support a digital back-end mortgage process are even less developed. This stage comprises the more time- and labor-intensive portion of the production timeline and encompasses originator-driven activities from processing through loan closing, vendor services such as property appraisal and title insurance, and, ultimately, funding and sale into the secondary market. Further development of, and integration with, digital capabilities across the back-end of the process is integral to the ability for lenders to offer an end-to-end digital mortgage product. At present, this integration is challenged by disparate rules and non-uniform recognition of electronic and remote online notarizations, reticence by some county land-recording offices to accept digital property and security records, and still-developing industry capabilities to accommodate new technologies.

### Challenges with Default Servicing, Loss Mitigation, and Foreclosure Practices

Post-crisis servicing rules administered by the Bureau have introduced a national standard for how delinquent loans are serviced; however, there remains significant differences in the loss mitigation products – such as loan modifications, short sales, and deeds-in-lieu of foreclosure – that are offered to delinquent borrowers. Generally, loss mitigation options made available to borrowers are established by the party most at risk for credit losses should the loan ultimately fail. In addition, loss mitigation options are influenced by other factors such as whether or not the loan is securitized and the requirements of the securitization program. Borrower and loan characteristics, as well as the level of market interest rates in relation to the borrower's current mortgage rate may also factor into the choice of an appropriate loss mitigation option. The fundamental differences between private investors, GSE guarantees, and government mortgage insurance programs result in a lack of standardization, which poses additional challenges for servicers when pursuing troubled loan workouts across servicing portfolios.<sup>282</sup> This inconsistency both directly impacts borrowers, who lack control over which entities purchase or service their loan, and ultimately dictates whether, and what type of, workout option is available in the event of financial hardship.

Servicers are additionally challenged by a lack of standardization in state-level foreclosure processes. Mortgage foreclosure processes are largely dictated by state law, which varies across the country. While some states have established statutory processes that permit a trustee to foreclose outside of court review, many other states require mediation and subject a foreclosure judgment to court review and approval, sometimes delaying the foreclosure process by years without improving borrower outcomes.

280. See J.D. Power, *Press Release – Despite a Rise in Use of Digital, Mortgage Customer Satisfaction Declines, J.D. Power Finds* (Nov. 9, 2017), available at: <http://www.jdpower.com/press-releases/jd-power-2017-us-primary-mortgage-origination-satisfaction-study>.

281. See Fuster et al., at 9.

282. See Laurie Goodman et al., *Government Loan Modifications: What Happens When Interest Rates Rise* (Jan. 2018), available at: [https://www.urban.org/sites/default/files/publication/95671/government-loan-modifications\\_2.pdf](https://www.urban.org/sites/default/files/publication/95671/government-loan-modifications_2.pdf).

For national mortgage servicers, managing to these unique requirements creates added costs when an aligned standard could deliver equally effective, or improved, outcomes for participants. In the face of these challenges, servicers may allocate resources to compliance as opposed to developing more effective mortgage-servicing platforms and deploying technology that would improve the borrower experience, particularly for those borrowers in default.

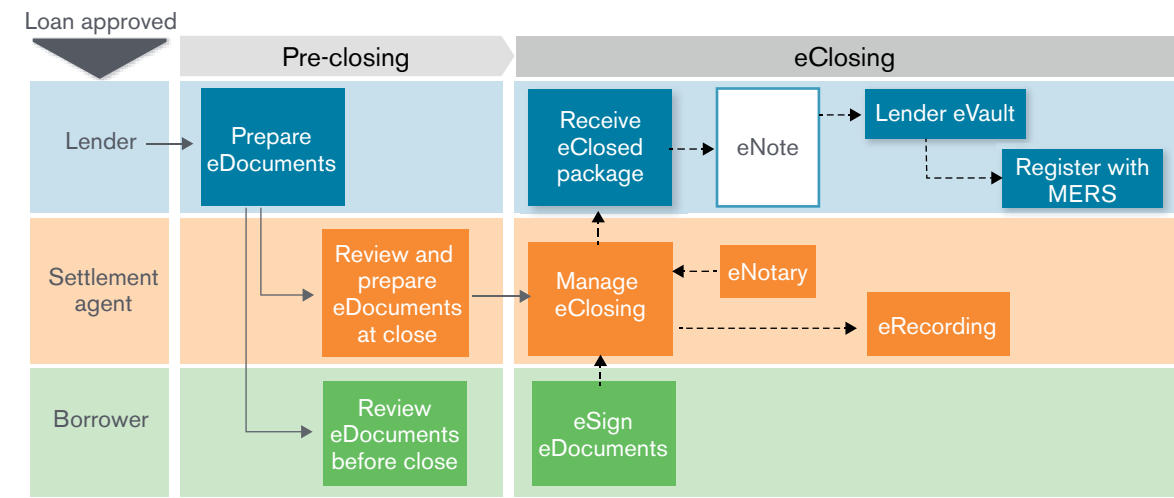
**Issues and Recommendations**

**Electronic Mortgage Notes**

The negotiable promissory note between lender and borrower is central to the mortgage origination process and establishes the borrower’s obligation to repay the lender for funds lent to purchase or refinance a home. At present, the vast majority of promissory notes are paper-based, “wet signed” by lender and borrower, and subsequently physically stored and transmitted. A fully electronic mortgage note, often referred to as an eNote, is an electronic version of the negotiable promissory note that is digitally signed and electronically transmitted and stored. The eNote forms the main digital component of an electronic mortgage, or eMortgage, which comprises a full end-to-end mortgage transaction that can be completed entirely through digital means.

Digital mortgage notes have a clear statutory basis in the Electronic Signatures in Global and National Commerce Act of 2000 (ESIGN), which recognized the legal validity of signatures and records executed with an electronic stamp as opposed to a wet signature on paper,<sup>283</sup> and in the 1999 Uniform Electronic Transactions Act (UETA), by which the National Conference of Commissioners on Uniform State Laws proposed uniform rules for state adoption of laws

Figure 14: Illustrative eNote Process



Source: Fannie Mae and Treasury.

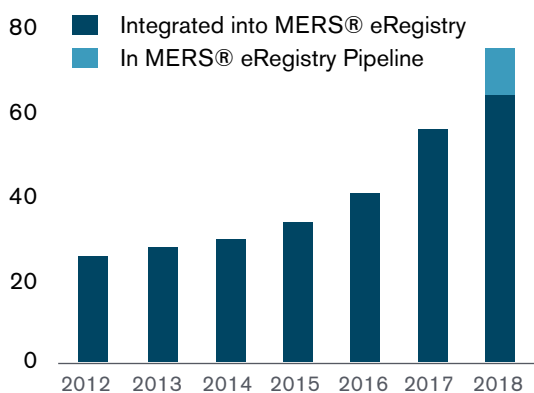
283. 15 U.S.C. §§ 7001-7031.

recognizing electronic records on an equal basis with paper ones.<sup>284</sup> Case law in the years since the passage of these eCommerce laws has upheld the legal enforceability of digital mortgage notes.<sup>285</sup>

eNotes require a digital promissory note to be electronically created, signed, secured, and registered, with maintenance in an electronic registry, or eRegistry, of the party in control of the note and the location of the authoritative copy of the registered note. Parties to an eNote, or their designated document custodian, store their versions of the eNote in a secure digital vault referred to as an eVault, with the location of the copy of record designated and maintained by the electronic registry itself. The MERS® eRegistry is utilized as the industry standard registry service for complying with the provisions of the eCommerce laws as a system of record for identifying the controller and location of the authoritative copy of the eNote and is recognized as such in the text of the Note itself.

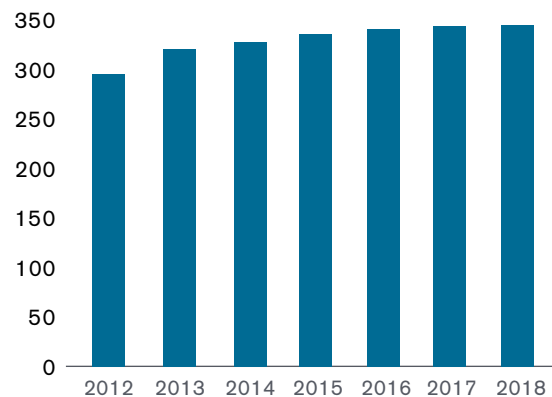
The framework, practices, and basis for eNotes is well established, even as adoption is limited. Secondary market investors Fannie Mae and Freddie Mac have had guidelines in place for approving a lender for and purchasing eNotes since the early 2000s. Primary market development of eNote capabilities was likely sidelined by the financial crisis and the subsequent wave of post-crisis regulations, which required capital resources and process updates. Today, there are 26 seller-servicers approved to deliver eNotes to the GSEs.<sup>286</sup> eNote deliveries represented less than 1% of 2017 GSE acquisition volumes.<sup>287</sup> However, as illustrated by **Figures 15** and **16**, both the number of companies integrated with the MERS® eRegistry and the number of eNotes registered on it has grown in recent years, consistent with the burgeoning interest in and development of this capability.

Figure 15: Number of Companies Active on the MERS® eRegistry



Source: MERSCORP Holdings, Inc.

Figure 16: Cumulative Number of eNotes Registered on the MERS® eRegistry (thousands)



Source: MERSCORP Holdings, Inc.

284. See National Conference of Commissioners on Uniform State Laws, *Uniform Electronic Transactions Act* (1999), available at: [http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta\\_final\\_99.pdf](http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf)

285. See Tank and Whitaker, at 9.

286. Data provided by the Federal Housing Finance Agency (FHFA).

287. Id.



Electronic promissory notes offer advantages over their analog versions that accrue to both the mortgage industry and borrowers. The ability to digitally execute this component of the origination process aligns with broader industry migration to digital capabilities and offers convenience, more efficient quality control, and, when integrated with a broader eMortgage solution, faster origination timelines. More specifically, eNotes are more readily transferred between holders as they are bought and sold in the secondary market, they cost less to store and transmit than paper notes, and they offer greater protection against unauthorized tampering, alteration, or loss.

Primary market development of the capability to originate eNotes represents one barrier to their wider adoption. An additional reason for their limited use is their lack of acceptance by other key secondary market participants. For federally insured mortgages from the FHA and VA, lenders generally prefer to securitize and issue Ginnie Mae mortgage securities. However, Ginnie Mae stated in an All Participant Memorandum in February 2014 that it was concerned with maintaining the liquidity and negotiability of its pools and would not allow electronic signatures or electronic documents on promissory notes, security instruments, or loan modification agreements.<sup>288</sup> More recently, Ginnie Mae has stated its commitment to developing its digital capabilities, including the eventual acceptance of digital promissory notes into its pools.<sup>289</sup>

Both FHA and VA have accepted digital signatures on notes since 2014 and 2013, respectively.<sup>290</sup> However, FHA in particular is challenged by an aging technology infrastructure that limits its ability to process and store digital loan files, mitigating the use of eNotes or broader digital mortgage files, and inhibiting lenders from offering this capability for government-supported loans.<sup>291</sup> As loans insured or guaranteed by FHA and VA comprise nearly a quarter of new originations, any limited functionality with regard to digital mortgage files acts as a barrier on wider industry adoption.

The FHLBs' lack of acceptance of eNotes represents an additional barrier to their further use. The FHLBs' primary business is providing secured advances to member institutions that support mortgage lending activity. The FHLBs currently do not accept eNotes as eligible, pledged collateral from their members for securing an advance.<sup>292</sup> While the FHLBs have expressed interest moving toward the acceptance of eNotes, they have identified two primary issues to address: (1) the current limited depth of a secondary market for eNotes; and (2) the appropriate representation for the FHLBs in the MERS® eRegistry where they have an interest in, but are not the owner of, eNotes as pledged collateral. In response to this concern, MERSCORP Holdings, Inc., is pursuing

---

288. Ginnie Mae, *All Participant Memorandum 14-01: Electronic Notes and Mortgages* (Feb. 27, 2014), available at: [https://www.ginniemae.gov/issuers/program\\_guidelines/Pages/mbsguideapmslibdisppage.aspx?ParamID=24](https://www.ginniemae.gov/issuers/program_guidelines/Pages/mbsguideapmslibdisppage.aspx?ParamID=24).

289. Ginnie Mae, *Ginnie Mae 2020* (June 2018), available at: [https://www.ginniemae.gov/newsroom/publications/Documents/ginniemae\\_2020.pdf](https://www.ginniemae.gov/newsroom/publications/Documents/ginniemae_2020.pdf).

290. U.S. Department of Housing and Urban Development, *Electronic Signatures*, Mortgagee Letter 2014-03 (Jan. 30, 2014), available at: <https://www.hud.gov/sites/documents/14-03ML.PDF>; Veterans Benefits Administration, *Use of Electronic Signatures in Conjunction with Department of Veterans Affairs (VA) Guaranteed Home Loans*, Circular 26-13-13 (Aug. 22, 2013), available at: [https://www.benefits.va.gov/homeloans/documents/circulars/26\\_13\\_13.pdf](https://www.benefits.va.gov/homeloans/documents/circulars/26_13_13.pdf).

291. See *FHA Annual Management Report: Fiscal Year 2017* (Nov. 27, 2017), available at: <https://www.hud.gov/sites/documents/FHAFY2017ANNUALMGMNTRPT.PDF>.

292. See Federal Home Loan Bank of Des Moines, *Collateral Quarterly* (Aug. 24, 2017), available at: [https://members.fhlbdm.com/media/cms/pages\\_fhlbdm\\_com\\_rs\\_171\\_ZQM\\_109\\_ima\\_09B7E4A798CA0.pdf](https://members.fhlbdm.com/media/cms/pages_fhlbdm_com_rs_171_ZQM_109_ima_09B7E4A798CA0.pdf).

the addition of a new Secured Party field to its eRegistry, which will enable certain parties, such as FHLBs and warehouse lenders, to be more appropriately represented in alignment with their position in the mortgage process today.<sup>293</sup>

### *Recommendations*

Treasury recommends that Ginnie Mae pursue acceptance of eNotes and supports the measures outlined in its *Ginnie Mae 2020* roadmap to more broadly develop its digital capabilities.

FHA is limited by its congressionally-appropriated budget but is in need of technology overhauls beyond the narrower discussion of digital mortgage capabilities. Treasury recommends that Congress appropriate for FHA the funding it has requested for technology upgrades in the President's Fiscal Year 2019 Budget — a portion of which FHA would use to improve the digitization of loan files.<sup>294</sup> In addition, FHA, VA, and USDA should explore the development of shared technology platforms, including for certain origination and servicing activities.

Finally, Treasury recommends the FHLBs explore ways to address their concerns regarding eNotes with the goal of accepting eNotes on collateral pledged to secure advances.

### Appraisals

Property appraisal practices, including a perceived lack of appraiser independence from loan originators and insufficiently stringent qualification requirements, were criticized in connection with the housing bubble and subsequent collapse in home prices. In response, lawmakers and regulators enacted changes to appraisal requirements that have fundamentally affected the appraisal industry. In recent years, lenders and homebuyers have pointed to the appraisal component of the origination process as a frequent source of delays and a driver of extended closing timelines.<sup>295</sup>

Concurrently, advances in financial technology, particularly with regard to automated valuation models (AVMs), have pushed appraisals in a new and innovative direction. The application of this technology has already begun to disintermediate the traditional appraisal process and, notably, has been adopted by both GSEs. The digitization of this component of the origination process, facilitated through electronic property records, development of large databases capable of holding millions of individual property records, and improvement of advanced valuation algorithms, holds promise to lower cost and expedite closing timelines.

Property appraisal standards for federally related real-estate transactions are governed by Title XI of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA).<sup>296</sup> In order to protect deposit insurance funds and to promote prudent lending, FIRREA assigned to the Appraisal Subcommittee of the Federal Financial Institutions Examination Council the

293. This new field, as described by MERSCORP Holdings, Inc., would represent the entity that has been assigned or granted an interest in the eNote by the Controller.

294. See U.S. Department of Housing and Urban Development, *FY 2019 Congressional Justification*, at 26-1 to 26-7, available at: [https://www.hud.gov/program\\_offices/cfo/reports/fy19\\_CJ](https://www.hud.gov/program_offices/cfo/reports/fy19_CJ).

295. See National Association of Realtors, *Realtors Confidence Index Survey* (Apr. 2018), at 7, available at: <https://www.nar.realtor/research-and-statistics/research-reports/realtors-confidence-index>.

296. Public Law No. 101-73, Title XI [codified at 12 U.S.C. §§ 3331-3355].



responsibilities to monitor state-level appraiser standards and credentialing, maintain a national registry of certified and licensed appraisers, and oversee the practices, procedures, and activities of the Appraisal Foundation, among other duties.<sup>297</sup>

FIRREA delegated to the Appraisal Foundation — a nonprofit industry organization — authority to set property valuation standards and minimum appraiser qualification requirements.<sup>298</sup> The Appraisal Foundation fulfills this mandate through two independent boards — the Appraisal Standards Board (ASB), which sets appraisal practices, and the Appraiser Qualifications Board (AQB), which establishes minimum state-level credentialing requirements.<sup>299</sup> These standards are binding for transactions by lenders subject to FIRREA, but are also used broadly throughout the housing finance system, including by the FHA and the GSEs.

The ASB maintains the Uniform Standards of Professional Appraisal Practice (USPAP), which sets ethical and professional standards for appraisers operating in the United States.<sup>300</sup> The AQB dictates minimum qualification criteria, with credentials tiered into classifications, with most real-estate transactions requiring appraisal by either a state-licensed residential real property appraiser or a state-certified real property appraiser, with each classification becoming progressively more selective.<sup>301</sup> Until May 2018, to become a certified residential appraiser, an individual would need to have completed a minimum four-year bachelor's degree, while licensed appraisers were subject to lesser college-level education requirements.<sup>302</sup> The AQB has recently implemented changes to ease the education requirements by removing the college education requirement for licensed appraisers and reducing the bachelor's level requirement for certified appraisers.<sup>303</sup>

The prudential banking regulators have, in the years since FIRREA's enactment, established numerous exemptions from the statutory appraisal requirement.<sup>304</sup> Through these Interagency Appraisal and Evaluation Guidelines, financial institutions subject to FIRREA may undertake a property evaluation in lieu of an appraisal for prescribed transactions, including single-family residential transactions where the market value is less than \$250,000, commercial real estate transactions less than \$500,000, certain refinancings, and where the transaction is guaranteed by or eligible for guarantee by a U.S. government agency or government-sponsored agency.<sup>305</sup>

---

297. 12 U.S.C. § 3332.

298. 12 U.S.C. §§ 3339, 3345.

299. See The Appraisal Foundation, available at: [https://www.appraisalfoundation.org/imis/TAF/About\\_Us/TAF/About\\_Us.aspx?hkey=52dedd0a-de2f-4e2d-9efb-51ec94884a91](https://www.appraisalfoundation.org/imis/TAF/About_Us/TAF/About_Us.aspx?hkey=52dedd0a-de2f-4e2d-9efb-51ec94884a91).

300. See Appraisal Standards Board, *2018-2019 Uniform Standards of Professional Appraisal Practice (USPAP)*, available at: <http://www.uspap.org/files/assets/basic-html/page-1.html#>.

301. See The Appraisal Foundation, *The Real Property Appraiser Qualification Criteria* (May 1, 2018), available at: <https://appraisalfoundation.sharefile.com/share/view/scbea7640298440aa>.

302. See Appraiser Qualifications Board, *Summary of Changes to the Real Property Appraiser Qualification Criteria* (May 1, 2018), available at: <https://appraisalfoundation.sharefile.com/share/view/s40e607fb0d64915a>.

303. *Id.*

304. See Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of Thrift Supervision, and National Credit Union Administration, *Interagency Appraisal and Evaluation Guidelines* (Dec. 2, 2010), available at: <https://www.fdic.gov/news/news/financial/2010/fil10082a.pdf>; see also 12 C.F.R. § 323.3.

305. *Id.*

The GSEs and federal housing programs, administered, for example, by FHA, act as de facto standard setters for mortgage appraisal requirements performed by both depositories, through the FIRREA exemption, and the large segment of nondepository lenders not subject to FIRREA. Lenders originating government mortgage loans, such as those insured by FHA or guaranteed by the VA or USDA, are required to comply with the appraisal policies established by these programs.<sup>306</sup> Fannie Mae's and Freddie Mac's seller-servicer guides similarly establish minimum eligibility standards for appraisals to qualify for purchase by the respective GSE. Both FHA and the GSEs require a USPAP-compliant appraisal for nearly all purchase and refinance loans.<sup>307</sup>

In 2017, Fannie Mae and Freddie Mac began offering originators appraisal waivers on a limited population of purchase and refinance loans.<sup>308</sup> The GSEs offer these waivers by leveraging their proprietary appraisal models and databases aggregating public records, multiple listing services, and millions of appraisal reports delivered electronically to the GSEs since 2012. For loans that qualify for the waiver, the originator may forego the appraisal component of the loan production process, potentially shortening timelines by as much as 10 days, and reducing origination costs by up to \$700.<sup>309</sup>

Independent appraisers highlight post-crisis changes as exacerbating a mismatch between lender demand for appraisal servicers and the number of independent appraisers qualified and willing to meet this demand. Post-crisis appraiser independence standards enacted under Dodd-Frank have resulted in lenders channeling appraisal requests through appraisal management companies (AMCs) to subcontract with a state-licensed or state-certified appraiser.<sup>310</sup> Partly as a result of more widespread use of AMCs as a market intermediary, independent appraisers report being paid relatively less than they earned prior to the introduction of the appraisal independence standard that gave rise to increased use of AMCs. Appraisers in some areas may be reticent to accept appraisal requests due to the compensation passed through to them. Delays in completing an origination or upcharges for rush appraisals to meet closing timelines may result and are ultimately borne by the borrower through higher origination costs.

Against this backdrop, the development of new appraisal technology offers the potential, when used responsibly, to relieve some of the pressures in the appraisal market and reduce the time and cost necessary to complete a property appraisal. This technology ranges from approaches that supplement traditional appraisals with remote evaluation technology to the deployment of AVMs to remotely estimate property value without recourse to in-person appraisers. AVMs

306. See U.S. Department of Housing and Urban Development, *FHA Single Family Housing Policy Handbook 4000.1* (Dec. 30, 2016), at Section II.D, available at: <https://www.hud.gov/sites/documents/40001HSGH.PDF> ("FHA Single Family Handbook").

307. See Fannie Mae, *Selling Guide* (June 5, 2018), at Part B4-1, available at: <https://www.fanniemae.com/content/guide/selling/b/index.html>; see Freddie Mac, *Single-Family Seller/Servicer Guide* (June 13, 2018), at Ch. 5601, available at: <http://www.freddie.mac.com/singlefamily/pdf/guide.pdf>.

308. See Fannie Mae, *Property Inspection Waiver*, available at: <https://www.fanniemae.com/singlefamily/property-inspection-waiver>; Freddie Mac, *Automated Collateral Evaluation Now Available for Purchase Transactions*, available at: [http://www.freddie.mac.com/singlefamily/news/2017/0818\\_ace\\_purchases.html](http://www.freddie.mac.com/singlefamily/news/2017/0818_ace_purchases.html).

309. See Freddie Mac, *Automated Collateral Evaluation (ACE)*, available at: <http://www.freddie.mac.com/singlefamily/loanadvisorsuite/pdf/ACEMatrixDoc.pdf>.

310. 15 U.S.C. § 1639e.

have existed for several decades but their use and accuracy has improved in recent years due to advances in machine learning, database technologies, and the proliferation of large datasets composed of proprietary and public records with detailed property-specific information. At present, AVMs are not permitted in place of traditional in-person appraisals for most loans sold to the GSEs, endorsed by FHA or insured by other government loan programs, or for real-estate transactions subject to FIRREA.

Critics of traditional appraisals argue that they represent an outdated and costly approach relative to new digital tools. Critics of AVMs argue that they are dependent on detailed data provided by an appraiser in order to maintain AVM accuracy, and that the disintermediation of traditional appraisals will degrade AVMs as a result. Another form of property appraisal exists between these two approaches to combine aspects of traditional appraisals with the automation and database capabilities of AVMs. So-called hybrid or desktop appraisals leverage property history data, comparable sales data, photographs or video of the interior and exterior of a property, and a licensed or certified appraiser. As the name would imply, desktop appraisals are able to be executed from a single remote location, and offer the potential to save appraisers considerable time that would otherwise be spent in transit to and from properties.

### *Recommendations*

Treasury recommends that Congress revisit Title XI FIRREA appraisal requirements to update them for developments that have occurred in the market during the past thirty years. Recent data has illustrated that approximately 90% of residential mortgage originations are eligible for appraisal exceptions established since the enactment of FIRREA by the designated federal regulatory agencies.<sup>311</sup> An updated appraisal statute should account for the development of automated and hybrid appraisal practices and sanction their use where the characteristics of the transaction and market conditions indicate it is prudent to do so.

Treasury supports the GSEs' efforts to implement standardized appraisal reporting, the GSEs' and FHA's adoption of proprietary electronic portals to submit appraisal forms, and the GSEs' limited adoption of appraisal waivers. While Treasury acknowledges that automated valuation engines and appraisal waivers should apply to a defined and limited subset of loans, and that they may compete with traditional appraisers, these innovations offer borrowers upside through lower cost originations and faster closings, without sacrificing accuracy. However, further application of digital, automated property valuations must be carefully monitored and integrated with rigorous market standards where they are used in lieu of traditional appraisals.

Treasury recommends FHA and other government loan programs develop enhanced automated appraisal capabilities to improve origination quality and mitigate the credit risk of overvaluation. These programs may also wish to consider providing targeted appraisal waivers where a high degree of property standardization and information about credit risk exists to support automated valuation, and where the overall risks of the mortgage transaction make such a waiver appropriate. Treasury supports legislative action where statutory changes are required to authorize granting

---

311. See Federal Financial Institutions Examination Council, *Joint Report to Congress: Economic Growth and Regulatory Paperwork Reduction Act* (Mar. 2017), available at: <https://www.occ.gov/news-issuances/news-releases/2017/nr-ia-2017-33a.pdf>.

limited appraisal waivers for government programs. Treasury further recommends that government loan programs explore opportunities to leverage industry-leading technology capabilities to reduce costs to taxpayers and accelerate adoption of new technology in the government-insured sector.

Finally, Treasury supports the AQB's recently updated appraisal certification guidelines that ease the education requirements to obtain that credential, with the understanding that providing off-ramps for the education requirement in favor of on-the-job training or other education credits can attract qualified appraisers to this industry and relieve appraiser supply challenges without jeopardizing valuation credibility.

### Electronic Closing and Recording

Mortgage closing, or settlement, represents the last step for a borrower in financing a home, and comprises the execution of the financial and title documents that form the basis for the mortgage loan and transfer of claim to the property. A key component of the closing process is the notarization of real estate transfer documents, such as the deed, which are subsequently filed, or publicly recorded, with local county land records. Traditionally, the loan closing is completed in one sitting, with the borrower and parties to the transaction physically present in the same location.

Notarization methods have expanded along with the rest of electronic commerce in recent decades and can now be accomplished either in-person through a digital document and notary seal or remotely through online interaction via webcam and using knowledge-based identification to confirm the borrower's identity. According to the Bureau's 2015 eClosing pilot, the ability to electronically complete the mortgage process through digital notarization represents one of the key remaining impediments to the digital process and offers additional borrower convenience and satisfaction if executed seamlessly versus a paper-based closing.<sup>312</sup>

While the UETA and E-SIGN eCommerce laws establish the validity of electronic signatures on consumer credit transactions, additional legal clarity is needed to ensure compliance with state notary laws for use of electronic notarizations, specifically the sanctioning of digital notarizations in lieu of a physical signature and notarization. To date, 39 states have enacted laws establishing the legality of such eNotarization.<sup>313</sup> In 2010, in part to account for the development of eNotarization capabilities, the National Conference of Commissioners on Uniform State Laws (also known as the Uniform Law Commission, or ULC) promulgated a revised model statutory framework for notarial acts, updating its original 1982 model act and aimed at facilitating interstate recognition of various types of notarizations.<sup>314</sup> To date, 11 states have enacted the revised Uniform Law Commission framework.<sup>315</sup>

312. See Bureau of Consumer Financial Protection, *Leveraging Technology to Empower Mortgage Consumers at Closing* (Aug. 2015), available at: [https://files.consumerfinance.gov/f/201508\\_cfpb\\_leveraging-technology-to-empower-mortgage-consumers-at-closing.pdf](https://files.consumerfinance.gov/f/201508_cfpb_leveraging-technology-to-empower-mortgage-consumers-at-closing.pdf).

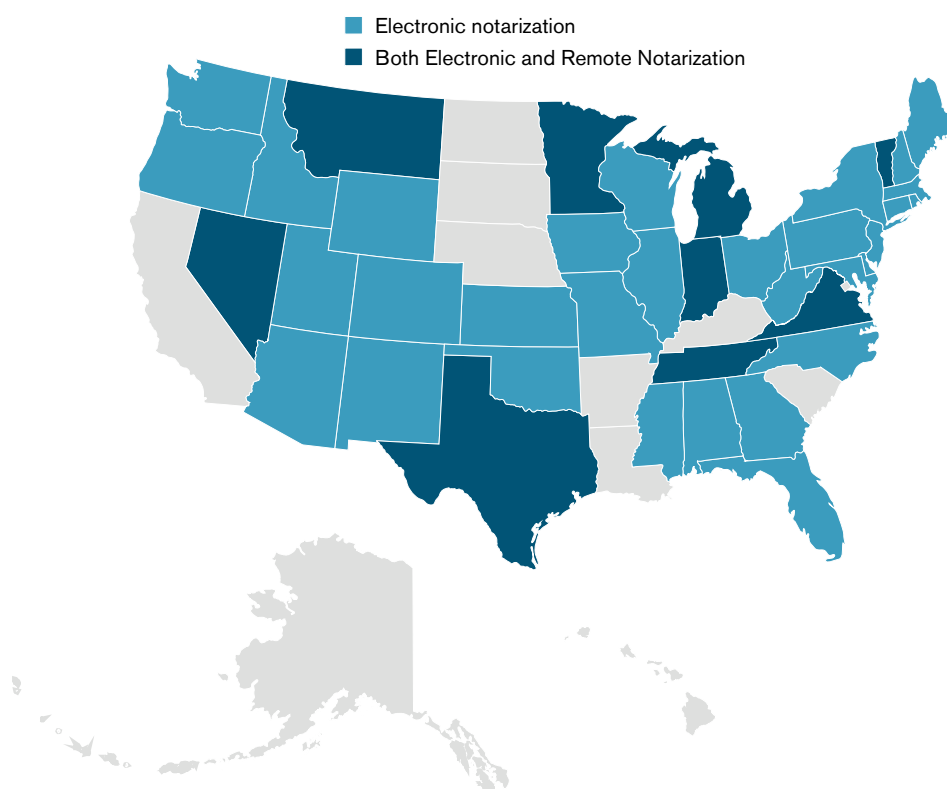
313. Based on information provided by the American Land Title Association to Treasury.

314. See Uniform Law Commission, *Revised Uniform Law on Notarial Acts* (2010), available at: <http://www.uniformlaws.org/Act.aspx?title=Law%20on%20Notarial%20Acts,%20Revised>.

315. Id.

These electronic notarization statutes, enabling digital notary signature for in-person notarizations, provide insufficient legal certainty for the use of remote notarization conducted electronically via webcam, with the latter permitting both signatory and notary to be in different locations. Virginia became the first state to officially sanction remote online notarization when it passed legislation to that end in 2012. Seven other states have followed suit, while an additional four states have remote online notarization bills pending, with the potential for passage in 2018.<sup>316</sup> In 2017, the American Land Title Association and the Mortgage Bankers Association (MBA), in an effort to address legal uncertainty and to facilitate further development of eMortgage capabilities, published model legislation providing a framework for states to use in adopting remote online notarization for real-estate transactions.<sup>317</sup>

Figure 17: Electronic and Remote Notarization by State



Source: American Land Title Association and Treasury staff analysis.

316. See Mortgage Bankers Association, *Remote Online Notarization*, available at: <https://www.mba.org/audience/state-legislative-and-regulatory-resource-center/remote-online-notarization> (last accessed June 14, 2018).

317. See American Land Title Association, *ALTA, MBA Develop Model Legislation for Remote Online Notarization* (Dec. 19, 2017), available at: <https://www.alta.org/news/news.cfm?20171219-ALTA-MBA-Develop-Model-Legislation-for-Remote-Online-Notarization>.

Despite state-level progress toward wider recognition of electronic notarization, the absence of a broad statutory acceptance across the country and uneven standards for remote and electronic notarization implementation has created confusion for market participants, slowing adoption of digital advances in mortgage technology by limiting the ability for lenders to complete a digital mortgage with an eClosing. Non-uniform state rules create a cost barrier for electronic notarization system vendors developing their platforms and creates uncertainty for investors considering purchasing digital mortgages. In 2006, the National Association of the Secretaries of State adopted standards for state use in implementing in-person, electronic notarizations. Amendments to these standards, accounting for the advance of remote notarizations, were recently adopted in February 2018 to support secure and technology-neutral implementation of remote notarization capabilities.<sup>318</sup>

County-level acceptance of digital security instruments is a key determinant of whether a lender will pursue an electronic closing, as lack of acceptance of these documents renders such critical eMortgage components, such as electronic notarization, moot. In 2004, the Uniform Law Commission promulgated the Uniform Real Property Electronic Recording Act (URPERA), representing a model statutory framework to provide county clerks and recorders the authority to accept electronic recording of real property instruments. Today, 33 states and U.S. territories have enacted URPERA; however, implementation remains a county-level exercise.<sup>319</sup> As of May 31, 2018, just over half of the 3,600 recording jurisdictions—primarily, but not exclusively counties—in the United States offer electronic recording.<sup>320</sup> Greater digitization of property records at the county level may, in the future, facilitate further advances in mortgage technology, including the potential application of distributed ledger technology to more expeditiously perform property record checks and expedite title review services.

### *Recommendations*

Treasury recommends that states yet to authorize electronic and remote online notarization pursue legislation to explicitly permit the application of this technology and the interstate recognition of remotely notarized documents. Treasury recommends that states align laws and regulations to further standardize notarization practices.

Treasury further recommends that Congress consider legislation to provide a minimum uniform national standard for electronic and remote online notarizations. Such legislation would facilitate, but not require, this component of a fully digital mortgage process and would provide a greater degree of legal certainty across the country. Federal legislation is not mutually exclusive with continued efforts at the state level to enact a framework governing the use of electronic methods for financial documents requiring notarization.

318. See National Association of Secretaries of State, *NASS Support for the Revised National Electronic Notarization Standards* (amended and readopted on Feb. 19, 2018), available at: <https://www.nass.org/node/1327>.

319. See Uniform Law Commission, *Real Property Electronic Recording Act*, available at: <http://www.uniformlaws.org/Act.aspx?title=Real%20Property%20Electronic%20Recording%20Act>.

320. See Property Records Industry Association, available at: <https://www.pria.us/i4a/pages/index.cfm?pageid=1> (last accessed on June 14, 2018).



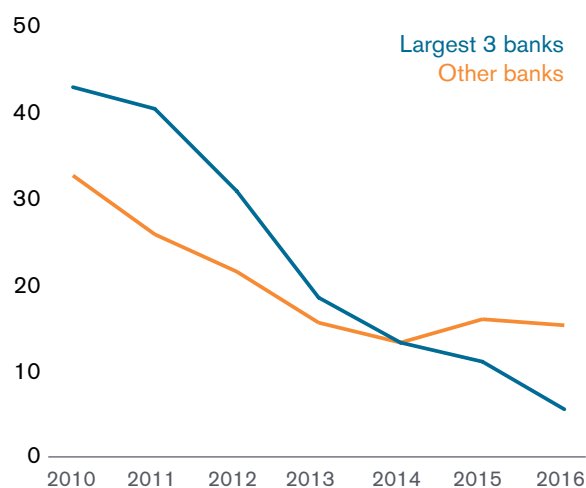
Treasury recommends that recording jurisdictions yet to recognize and accept electronic records implement the necessary technology updates to process and record these documents and to pursue digitization of existing property records.

### False Claims Act

Civil actions brought under the authority of the False Claims Act (FCA) — a Civil War-era statute — have been closely associated with the mortgage industry since the financial crisis. Beginning in 2011, the U.S. Department of Justice (DOJ), often based on a referral from the Inspector General for the U.S. Department of Housing and Urban Development (HUD), has pursued numerous claims under the FCA against lenders of government mortgages where it was determined that the lenders knowingly submitted for government insurance mortgages that did not meet federal eligibility standards.

DOJ has recovered approximately \$7 billion related to FCA housing fraud settlements and judgments to date.<sup>321</sup> The cost of FCA liability for lenders and servicers, and the ongoing fear of future action by the government is often cited as a factor in the shift away from depositories and toward nondepository mortgage banks in the government mortgage loan market.<sup>322</sup> The departure of depositories from federally insured mortgages has likely had negative impacts on borrower access to credit by reducing the available lending universe and encouraging remaining lenders to add credit and risk overlays to their underwriting to mitigate lower credit quality, but nonetheless creditworthy, borrowers.

Figure 18: FHA Share of Originations (percent)



Source: Federal Reserve (see Bhutta et al.) using HMDA data.

An entity that violates the FCA by knowingly submitting false claims to the government is subject to substantial civil remedies: penalties between \$11,181 and \$22,363 per false claim as well as triple the amount of damages to the government — known as treble damages.<sup>323</sup> Furthermore, it has been standard practice for DOJ to determine the percentage incidence of errors on a sample size of loans that have gone to claim and then extrapolate the incidence of violations to a broader population of loans that went to claim to capture what DOJ alleges to be the full extent of the false claims submitted by lenders and servicers. Because the FCA only allows a recovery when a loan defaults and results in a claim for mortgage insurance, the samples selected in FCA actions are only drawn from the

321. See U.S. Department of Justice, *Fact Sheet: Significant False Claims Act Settlements & Judgments, Fiscal Years 2009–2016*, available at: <https://www.justice.gov/opa/press-release/file/918366/download>.

322. See Bhutta, Laufer, and Ringo.

323. 31 U.S.C. § 3729(a)(1).

universe of loans that went to claim. Thus, the samples are not intended, and cannot be interpreted, to be representative of a lender's overall portfolio.

Before liability or damages may be imposed under the FCA, the FCA requires that any false claim be both knowing and material.<sup>324</sup> Consistent with this latter requirement, DOJ and HUD have a practice of reaching mutual agreement on resolving claims, even though the process by which agreement is reached has been characterized as lacking clarity. DOJ's FCA settlements have often been accompanied by admitted statements of facts by the settling lenders, and these statements have confirmed the lenders' knowledge of the materiality of the defects that were the subject of the settlements.<sup>325</sup> Nevertheless, HUD and DOJ have been criticized for not sufficiently differentiating knowing and material errors from those that would not have affected approval of the loan for a federal program or servicer actions during the foreclosure process.<sup>326</sup> Distinguishing knowing and material errors from clerical defects is particularly important to lenders and servicers. Even if lenders and servicers strive to ensure the information they collect and submit to FHA is complete and accurate, minor errors are to be expected. Industry concerns about being held liable under the FCA for these types of defects may affect the decision to participate, and at what price, in government loan programs.

HUD has taken steps in recent years to provide additional clarity around the severity across violations and to provide lenders greater certainty that loans they originate and service are insurable by the FHA. Administrative changes to loan-level certifications and implementation of a loan quality review taxonomy were executed in an attempt to encourage lenders to re-enter the FHA market by clarifying a materiality threshold for errors.

FHA lenders are required to certify annually that they meet established HUD-FHA approval standards. Additionally, lenders must certify at the loan-level that loans meet FHA eligibility requirements. In 2016, HUD updated its loan-level certification, which attempted to apply a materiality threshold to instances where violations would trigger the rescission of FHA insurance by defining liability as errors that would have altered the decision to approve a loan.<sup>327</sup> More significantly, in 2017, FHA announced the implementation of its Loan Review System, incorporating the Loan Quality Assessment Methodology (Defect Taxonomy).<sup>328</sup> The Defect Taxonomy classifies nine defect areas by category, identifies the source and cause of the defect, and classifies them into four severity tiers based on the nature of the error, with errors moving from most severe in tier

324. *Id.*; *Universal Health Services v. United States ex rel. Escobar*, 136 S. Ct. 1889 (2016).

325. See *The False Claims Act & Federal Housing Administration Lending* (March 15, 2016), available at <https://www.justice.gov/archives/opa/blog/false-claims-act-federal-housing-administration-lending>.

326. See Paul Compton, Jr., U.S. Department of Housing and Urban Development, *New Era of Cooperation and Coordination* (Apr. 30, 2018), available at: [https://www.hud.gov/press/speeches\\_remarks\\_statements/Speech\\_043018](https://www.hud.gov/press/speeches_remarks_statements/Speech_043018).

327. See U.S. Department of Housing and Urban Development, *Revised HUD 92900-A HUD/VA Addendum to Uniform Residential Loan Application*, Mortgagee Letter 2016-06 (Mar. 15, 2016), available at: <https://www.hud.gov/sites/documents/16-06ML.PDF>.

328. See U.S. Department of Housing and Urban Development, *Federal Housing Administration (FHA) Loan Review System – Implementation and Process Changes*, Mortgagee Letter 2017-03 (Jan. 11, 2017), available at: <https://www.hud.gov/sites/documents/17-03ML.PDF>.



one to the least severe in tier four.<sup>329</sup> With this taxonomy, FHA intended to clarify the severity of loan-level violations — distinguishing material defects from errors that would not impact the insurability of the loan.

While industry participants have been supportive of providing additional clarity around what constitutes a manufacturing defect and the nature of the defect, stakeholders have called for HUD and FHA to take the further administrative step of providing a prescribed remedy for each violation in the taxonomy and a safe harbor for violations at the lower tiers of the taxonomy and for those at the higher tiers that have been cured. Furthermore, many market participants feel that action by FHA alone is insufficient to relieve lender concerns about liability tail risk. For example, the Defect Taxonomy has not altered the eligibility rules for HUD loans, which means it does not govern when DOJ can or should bring appropriate FCA claims. To market participants seeking to mitigate risk of FCA liability, the fact that FHA may differentiate violations based on materiality in its own administrative proceedings offers no guarantee that DOJ, or a whistleblower litigating a qui tam action in place of the government, will adopt the same posture. Since the Supreme Court's decision in *Universal Health Services v. United States ex rel. Escobar*, the views of the agency making payment decisions significantly affect determinations of materiality (or lack thereof).<sup>330</sup> Even following the Escobar ruling, the industry would benefit from additional clarity on the common standards applied by HUD and DOJ.

Material errors in manufacturing and servicing government loans should continue to be subject to enforcement by FHA and DOJ and bad actors who knowingly defraud the government should face significant fines and penalties. But when industry is reluctant to originate or service government loans in light of the FCA enforcement risk, this serves the counterproductive end of increasing the cost of credit and potentially limiting borrower access to federal loan programs.

### *Recommendations*

Enforcement of the FCA is critical to ensuring the integrity of any federal program and protecting it against knowing violations. At the same time, FCA enforcement actions can impose significant costs on a defendant both in terms of financial and reputational damages. Accordingly, it is important that an appropriate balance be struck between what program requirements an agency considers to be material — and therefore subject to potential FCA enforcement when knowing violations of these requirements occur — and what requirements are not material, and are appropriately addressed through actions outside of the FCA.

To address the perception associated with the use of the FCA on mortgage loans insured by the federal government, Treasury recommends that HUD establish more transparent standards in determining which program requirements and violations it considers to be material to assist DOJ in determining which knowing defects to pursue. In doing so, Treasury recommends that FHA clarify the remedies and liability lenders and servicers face, which could include, where appropriate, remedies such as indemnification and/or premium adjustments. Remedies should be correlated to

---

329. See FHA's Single Family Housing Loan Quality Assessment Methodology, available at: [https://www.hud.gov/sites/documents/SFH\\_LQA\\_METHODODOLOGY.PDF](https://www.hud.gov/sites/documents/SFH_LQA_METHODODOLOGY.PDF).

330. See Escobar, 136 S. Ct. at 1989.

the Defect Taxonomy. FHA should continue to review and refine its lender and loan certifications and its loan review system, including the Defect Taxonomy. Lenders that make errors deemed immaterial to loan approval should receive a safe harbor from a denial of claim and forfeiture of premiums. Lenders should receive a similar safe harbor for material violations that are cured based on remedies prescribed by FHA absent patterns which indicate a systemic issue. In determining the appropriate remedies for violations of its program requirements, HUD should consider the systemic nature of the problem, involvement or knowledge of the lender's senior management, overall quality of the originations of a specific lender, and whether or to what extent the loan defect may have impacted the incidence or severity of the loan default.

Treasury recommends DOJ ensure that materiality for purposes of the FCA is linked to the standards in place at the agency administering the program to which the claim has been filed, and that DOJ and HUD work together to clarify the process by which mutual agreement is reached on the resolution of claims. Where a relator pursues *qui tam* action against a lender for a nonmaterial error or omission, DOJ, in consultation with HUD and FHA, should consider exercising its statutory authority to seek dismissal.<sup>331</sup>

Distinguishing materiality, providing clear remedies to cure discovered defects, and linking the Defect Taxonomy to the FCA could provide a measure of certainty that could attract lenders back into this market and reduce costly overlays without constraining the government's ability to punish bad actors and prosecute knowingly fraudulent activity. However, if the recommended administrative actions are unsuccessful at achieving the desired result of increasing lender and servicer participation in federal mortgage programs, Congress should consider appropriate remedial legislation.

### Aligned Federal Mortgage Loss Mitigation Standards

The Bureau has implemented multiple servicing rules and rule revisions during the past five years, requiring numerous changes to servicer procedures, particularly concerning procedures for how to engage delinquent borrowers when evaluating them for loan modifications or other loss mitigation options. The federal government has not promulgated rules to prescribe a national loss mitigation standard. Crisis-era loss mitigation programs offered a degree of standardization and transparency for servicers, borrowers, and mortgage investors around loss mitigation options. In the absence of such a de facto federal loss mitigation standard, some market participants have cited concerns with the variance in options across different federal mortgage programs.

In recent years, market participants, including the GSEs, FHA, and the MBA, which represents certain market participants, have established loss mitigation standards to memorialize successful components of crisis-era programs or to encourage a degree of standardization for servicers across the private, federally supported, and federally insured mortgage markets. The GSEs' Flex Modification (FlexMod), implemented in 2017, closely aligns with MBA's One Modification

---

331. 31 U.S.C. § 3730(c)(2). Pursuant to a January 10, 2018 memorandum from Michael Granston, Director, Frauds Section of the Commercial Litigation Branch, DOJ attorneys have assessed whether declined *qui tam* cases are appropriate for dismissal.

proposal published in 2016.<sup>332</sup> Both the FlexMod and the MBA proposal reflect many of the lessons learned and standards adopted following the financial crisis. For example, both evaluate borrower hardship (short-term versus longer-term), offer solutions appropriate to that hardship that include retention and nonretention options, and aim to offer the most sustainable longer-term solution through the use of a waterfall of steps to achieve a modification that provides payment relief to the borrower and positive economic outcomes for the investor. Finally, FHA's loss mitigation program, which includes FHA-Home Affordable Modification Program (FHA-HAMP), shares many of the same features of the GSEs' present modification program, but utilizes different steps to achieve payment reduction.<sup>333</sup>

Despite agreement by most participants on the guiding themes for successful loss mitigation, the GSEs, FHA, VA, USDA, bank portfolio servicers, and private-label securities servicers continue to offer different loss mitigation programs. These differences are rooted in a number of underlying factors, including fundamental differences in the business models, regulatory and statutory mandates, and the borrower segments served by the range of private and federally-backed sources of mortgage financing. The main area in recent years where standardization and transparency has been achieved is across Fannie Mae and Freddie Mac with the implementation of their FlexMod – alignment facilitated by the GSEs' fundamentally similar business models and conservatorship under FHFA. FHA has a statutory mandate to hold capital and act as a fiduciary for the Mutual Mortgage Insurance Fund (MMIF).<sup>334</sup> Undertaking this fiduciary responsibility to the MMIF requires prompt liquidation of any assets assigned to it as a result of insurance claim payments (i.e., unlike the GSEs, FHA generally does not hold mortgage assets) — a program restriction that may constrain certain loss mitigation options.

Mortgage servicers cite the differences in loss mitigation programs as a particular challenge. Servicers, particularly specialty servicers who focus on delinquent and defaulted loans, will seldom service just one type of loan (e.g., all conventional or all government mortgages). Managing multiple standards limits efficiency and the ability to automate certain processes, restricts a servicer's ability to assess risk, and adds additional costs.

Furthermore, except for federal mortgage programs administered by FHA, VA, and USDA, a borrower does not necessarily know at origination whether his or her mortgage will be sold to a private credit investor or securitized through the GSEs — yet that same borrower faces two different experiences in the event of financial hardship that requires a loan workout solution. Borrowers, particularly during periods of hardship, benefit from clarity, and servicers benefit from certainty and scalability in terms of what assistance to offer a borrower who has experienced a hardship.

---

332. See Federal Housing Finance Agency, *Statement of FHFA Deputy Director Sandra Thompson on New Loan Modification Offering for Delinquent Borrowers* (Dec. 14, 2016), available at: <https://www.fhfa.gov/Media/PublicAffairs/Pages/Statement-of-FHFA-Deputy-Director-Sandra-Thompson-on-New-Loan-Mod-Offering-for-Delinquent-Borrowers.aspx>; see Mortgage Bankers Association, *Press Release – MBA Task Force Proposes Loan Modification Program to Provide At-Risk Homeowners Payment Relief* (Sept. 2016), available at: <https://www.mba.org/2016-press-releases/september/mba-task-force-proposes-loan-modification-program-to-provide-at-risk-homeowners-payment-relief>.

333. See HUD Mortgagee Letter 2009-23 and HUD Mortgagee Letter 2016-14.

334. 12 U.S.C. § 1708.

As such, mortgage loss mitigation is one part of the market that would benefit from a degree of alignment that does not presently exist.

Having a greater degree of standardization and transparency in place across the federal housing footprint would also accelerate the ability to respond in a future period of sustained market stress, as servicer, borrower, and mortgage investors would have procedures in place and an understanding of the exposures to more quickly administer loss mitigation solutions to struggling borrowers. Given the tendency of the housing market to exacerbate weakness during an economic downturn, having such a coordinated response in place could help mitigate the impact of housing market weakness on the broader economy.

In addition to potential benefits of greater alignment around loss mitigation programs, servicers have suggested a number of opportunities to increase efficiencies and reduce costs in FHA default servicing. Mortgage servicers believe that FHA servicing rules are complex and, in some cases, conflicting or outdated when compared to current industry practice reflected in GSE and PLS servicing and other regulatory requirements. Areas of potential enhancement include simplification of foreclosure timelines, restructuring of penalties associated with the failure to meet required timelines, and streamlining the foreclosed property conveyance process. These issues have been identified by HUD in its efforts to review and address needlessly burdensome and costly regulations.

#### *Recommendations*

Treasury recommends that federally supported mortgage programs explore standardizing the most effective features of a successful loss mitigation program across the federal footprint. Such standardization should broadly align a loss mitigation approach that facilitates effective and efficient loan modifications when in the financial interest of the borrower and investor, promotes transparency, reduces costs, and mitigates the impact of defaults on housing valuations during downturns. It should also establish parameters such as a standardized application package, affordability standards (e.g., suggested housing-expense-to-income ratios and minimum payment reductions), modification waterfall standards that specify suggested acceptable loss mitigation steps, and referral of delinquent borrowers to financial counseling. At the same time, these standards should not prescribe a specific modification product.

Additionally, Treasury recommends HUD continue to review FHA servicing practices with the intention to increase certainty and reduce needlessly costly and burdensome regulatory requirements, while fulfilling FHA's statutory obligation to the MMIF. In particular, Treasury recommends that FHA consider administrative changes to how penalties are assessed across FHA's multi-part foreclosure timeline to allow for greater flexibility for servicers to miss intermediate deadlines while adhering to the broader resolution timeline, as well as to better align with federal loss mitigation requirements now in place through the Bureau. Additionally, Treasury recommends FHA explore changes to its property conveyance framework to reduce costs and increase efficiencies by addressing frequent and costly delays associated with the current process. As an additional measure, Treasury recommends that FHA continue to make appropriate use of, and consider expanding, programs which reduce the need for foreclosed properties to be conveyed to HUD, such as Note Sales and FHA's Claim Without Conveyance of Title.

## State Foreclosure Practices

Foreclosure practices are one of the most divergent state-level policies across the mortgage industry, and one for which certain housing markets have paid a high price in the decade since the housing market collapse. Foreclosure processes vary for each state but largely adhere to some combination of two formats: judicial and nonjudicial.

In a state with a requirement for a judicial review process, the owner of a mortgage note, typically the lender, is required to file a lawsuit in local court to foreclose on a defaulted borrower. Other states permit the lender to foreclose without going through the court system when a power of sale clause is present in the mortgage or deed of trust — a process referred to as a nonjudicial review. Some states allow both judicial and nonjudicial foreclosures but favor one or the other depending on the type of security instrument — mortgage or deed-of-trust — with judicial foreclosures more common with mortgages, and nonjudicial foreclosures with deeds-of-trust.

In states requiring judicial review, typically once the lender files a foreclosure lawsuit in court, the homeowner receives a summons and a copy of the foreclosure complaint. The homeowner can let the foreclosure proceed or contest it in court. If the homeowner chooses to contest, the court holds a hearing and a judge decides whether to let the foreclosure sale proceed and, if approved, sets an auction date. In states without a required judicial process, existing statutes establish the process required for a trustee to foreclose on a defaulted property. State law, and not the courts, determine the timeline and milestones in the foreclosure process. Some states have imposed additional required steps and remediation requirements regardless of judicial or nonjudicial review designed to afford additional protections to defaulted borrowers.

Since the financial crisis, foreclosure timelines have increased regardless of state foreclosure practices, with the national average timeline to complete a foreclosure climbing from approximately 6 months in 2007 to approximately 33 months by the end of 2017.<sup>335</sup> These timelines are generally considerably longer for those states that require judicial review.<sup>336</sup> While the national share of loans in the foreclosure process has returned to pre-crisis levels, the foreclosure rate in judicial review states remains elevated relative to both nonjudicial review states and the pre-crisis level,<sup>337</sup> with timelines in some judicial review states such as Florida and New Jersey exceeding 3 years on average.<sup>338</sup> In certain documented cases, borrowers in judicial review states have been able to remain in a property for over 5 years without making payments before a foreclosure is completed.<sup>339</sup>

---

335. ATTOM Data Solutions, *US Foreclosure Activity* (Apr. 2018), available at: <https://www.attomdata.com/news/market-trends/foreclosures/q1-2018-u-s-foreclosure-market-report/>.

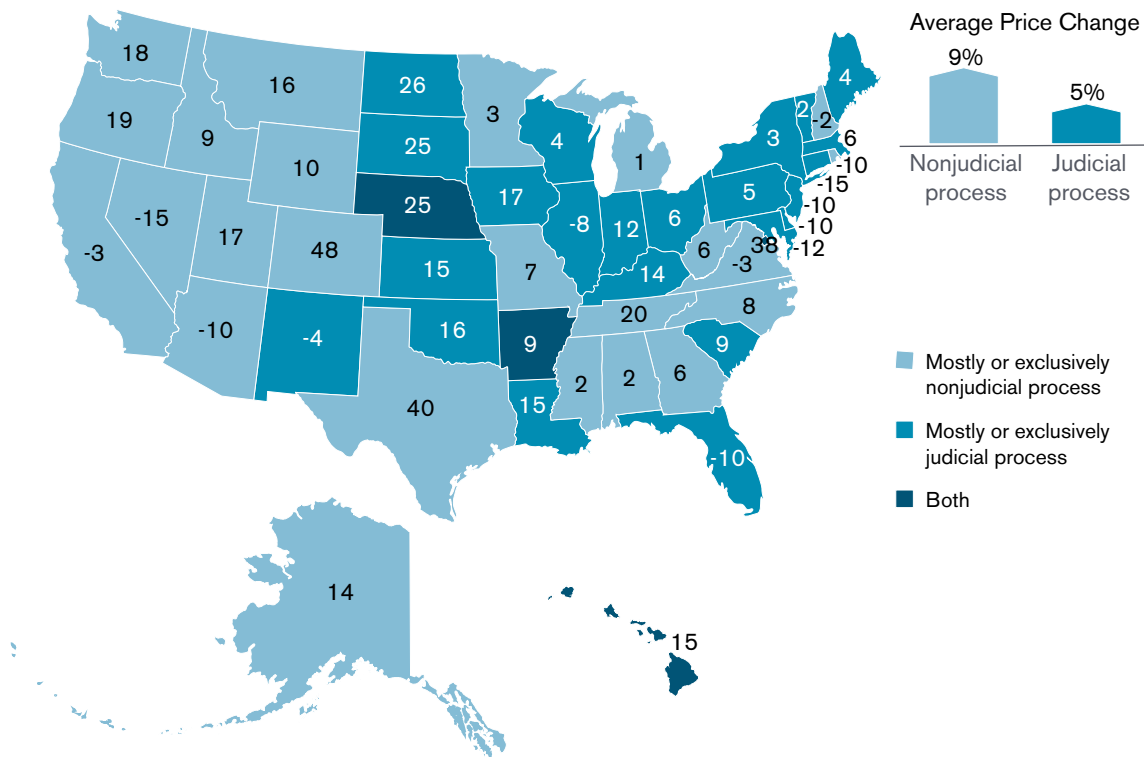
336. See Hamilton Fout et al., *Foreclosure Timelines and Housing Prices*, working paper (July 2017), available at: <http://www.fanniemae.com/resources/file/research/datanotes/pdf/foreclosure-timelines-and-house-prices-working-paper.pdf>.

337. Molly Boesel, CoreLogic, *Foreclosure Report Highlights: November 2016*, blog post (Jan. 10, 2017), available at: <https://www.corelogic.com/blog/2017/01/foreclosure-report-highlights-november-2016.aspx>.

338. See ATTOM Data Solutions.

339. Michael Corkery, *Homeowners Facing Foreclosure May Instead be Home Free*, Boston Globe (Mar. 30, 2015).

Figure 19: Foreclosure Process and Home Price Change Peak-to-Current by State (percent change)



Source: FHFA All Transactions Price Index, ATTOM Data Solutions Foreclosure Processes by State, and Treasury staff analysis.

Due to the high-cost of servicing nonperforming loans, borrowers in states with protracted foreclosure timelines will likely bear a portion of the cost of delays through a risk premium embedded in interest rates for loans made in that state.<sup>340</sup> Additionally, prolonged foreclosure timelines create a negative externality on home prices, which may harm nearby property values and dampen home price appreciation.<sup>341</sup> Since their pre-crisis peak, housing prices in states with a primarily nonjudicial review foreclosure process have appreciated twice as much as prices in states with a judicial review process.<sup>342</sup>

There is evidence that the judicial review foreclosure process leads to higher rates of persistent delinquency than nonjudicial review foreclosures, without measurably improving foreclosure

340. See Laurie Goodman, Urban Institute, *Servicing Costs and the Rise of the Squeaky-Clean Loan* (Feb. 2016), available at: <https://www.urban.org/sites/default/files/publication/77626/2000607-Servicing-Costs-and-the-Rise-of-the-Squeaky-Clean-Loan.pdf>.

341. See Eliot Anenberg and Edward Kung, *Estimates of the Size and Source of Price Declines due to Nearby Foreclosures*, 104 *American Economic Review* 2527–2551 (2014).

342. Treasury calculations based upon ATTOM Data Solutions foreclosure processes by state and FHFA Quarterly All-Transactions Home Price Index.



outcomes for borrowers.<sup>343</sup> Standardizing and moving away from a judicial review foreclosure process could reduce the time and resources involved in foreclosures and support home prices, without compromising borrower protections provided by federal and state regulation.

For federally supported housing programs that impose a degree of national pricing, such as the GSEs and FHA, some of the added cost from long foreclosure timelines is borne by borrowers in states with shorter timelines—effectively imposing a cross-subsidy from faster foreclosure states to slower ones. In response to state level differences in mortgage loss severities attributable to foreclosure process differences, the Federal Housing Finance Agency (FHFA) considered requiring the GSEs to impose an up-front fee in specific states where foreclosure costs exceeded the national average.<sup>344</sup> While FHFA elected not to pursue these charges, it did direct the GSEs in 2013 to maintain a quarter-point guaranty fee surcharge for four states — Connecticut, Florida, New Jersey, New York — where the foreclosure costs were more than two standard deviations above the national average.<sup>345</sup> All four states require judicial review foreclosure processes.<sup>346</sup> However, in January 2014, under a new director, FHFA reversed this decision and suspended any surcharge based on state foreclosure costs.<sup>347</sup>

### *Recommendations*

Treasury recommends that states pursue the establishment of a model foreclosure law, or make any modifications they deem appropriate to an existing model law,<sup>348</sup> and amend their foreclosure statutes based on that model law. Treasury recommends federally supported housing programs, including those administered by FHA, USDA, VA, and the GSEs, explore imposing guaranty fee and insurance fee surcharges to account for added costs in states where foreclosure timelines significantly exceed the national average.

### Nondepository Counterparty Transparency

Ginnie Mae guarantees the timely payment of principal and interest to investors in its securities, which are issued by lenders approved by Ginnie Mae and backed by government-guaranteed or insured mortgages. With the departure of credit investors in the wake of the housing collapse, Ginnie Mae experienced a surge in volume, as lenders and borrowers moved to access mortgage credit through government loan programs. Issuance of Ginnie Mae mortgage-backed securities (MBS) jumped from \$97 billion in 2007 to \$454 billion two years later, and has averaged over

---

343. See Kristopher Gerardi, Lauren Lambie-Hanson, and Paul S. Willen, *Do Borrower Rights Improve Borrower Outcomes? Evidence from the Foreclosure Process*, 73 J. of Urban Econ. 1 (2013).

344. See State-Level Guarantee Fee Pricing (Sept. 19, 2012) [77 Fed. Reg. 58991 (Sept. 25, 2012)].

345. See Federal Housing Finance Agency, *Press Release – FHFA Takes Further Steps to Advance Conservatorship Strategic Plan by Announcing an Increase in Guarantee Fees* (Dec. 9, 2013), available at: <https://www.fhfa.gov/Media/PublicAffairs/Pages/FHFA-Takes-Further-Steps-to-Advance-Conservatorship-Strategic-Plan-by-Announcing-an-Increase-in-Guarantee-Fees.aspx#>.

346. See ATTOM Data Solutions, *Foreclosure Laws and Procedures by State*, available at: <https://www.realtytrac.com/real-estate-guides/foreclosure-laws/> (last accessed June 15, 2018).

347. See FHFA Guarantee Fees History, available at: <https://www.fhfa.gov/PolicyProgramsResearch/Policy/Pages/Guarantee-Fees-History.aspx>.

348. See Uniform Law Commission, *Home Foreclosure Procedures Act* (2015), available at: <http://www.uniformlaws.org/Act.aspx?title=Home%20Foreclosure%20Procedures%20Act>.

\$400 billion in the years since.<sup>349</sup> Between 2007 and 2017, the remaining principal balance of pools guaranteed by Ginnie Mae increased fourfold to \$1.96 trillion.<sup>350</sup>

Ginnie Mae's issuer base has changed dramatically in both type and concentration, with nondepository issuers stepping into the market vacated by depositories exiting government loan programs. By the beginning of 2018, dedicated mortgage banks accounted for over 80% of Ginnie Mae issuance.<sup>351</sup> The GSEs, too, have seen their seller-servicer counterparty mix shift toward nondepositories, with nondepository lenders accounting for approximately half of the origination volume in 2017.<sup>352</sup> Market observers and participants, including Ginnie Mae, have asserted that the rapid increase in nondepository origination and servicing activity, combined with a less standardized approach to safety and soundness regulation, poses heightened counterparty risk. The disparity in banks and nonbanks prudential regulatory regimes has caused some market observers to question nonbank durability through the economic cycle and posit that nondepositories pose a systemic risk in general and a taxpayer risk in particular through the high share of nondepositories servicing Ginnie Mae pools.<sup>353</sup>

Nonbank servicers, like their bank competitors, are subject to a range of federal financial oversight. The Bureau, for example, supervises adherence to mortgage lending and servicing rules in addition to broader compliance with federal consumer financial laws. In addition, nondepositories are subject to oversight through counterparty minimum net worth, capital, and liquidity requirements imposed by the GSEs and Ginnie Mae.<sup>354</sup> As nonbanks are more dependent on execution through securitization, which at present is dominated by the GSEs and Ginnie Mae, compliance with GSE and Ginnie Mae counterparty requirements functions as an additional industry standard.

However, bank and nonbank lender-servicers face different safety and soundness regulatory standards. Insured depository institutions must abide by federal prudential regulation which includes standardized capital and liquidity regimes. Nondepositories are chartered and regulated at the state level and similarly face safety and soundness regulation, albeit by individual state banking examiners, despite the fact that these nondepositories may have a national footprint. While state regulators, facilitated by the Conference of State Bank Supervisors, have made progress in recent years toward developing more aligned standards for nonbank supervision, concerns about differing standards persist and have prompted calls for additional alignment.

349. See Ginnie Mae, *Monthly Issuance Reports – March 2018 Issuance Summary* (Apr. 13, 2018), available at: [https://www.ginniemae.gov/data\\_and\\_reports/reporting/Pages/monthly\\_issuance\\_reports.aspx](https://www.ginniemae.gov/data_and_reports/reporting/Pages/monthly_issuance_reports.aspx)

350. See Ginnie Mae, *Monthly UPB Reports – March 2018* (Apr. 13, 2018), available at: [https://www.ginniemae.gov/data\\_and\\_reports/reporting/Pages/monthly\\_rpb\\_reports.aspx](https://www.ginniemae.gov/data_and_reports/reporting/Pages/monthly_rpb_reports.aspx).

351. See Urban Institute, *Housing Finance at a Glance* (May 2018), available at: [https://www.urban.org/research/publication/housing-finance-glance-monthly-chartbook-may-2018/view/full\\_report](https://www.urban.org/research/publication/housing-finance-glance-monthly-chartbook-may-2018/view/full_report).

352. *Id.*

353. See U.S. Government Accountability Office, *Nonbank Mortgage Services: Existing Regulatory Oversight Could Be Strengthened* (Mar. 2016), available at: <https://www.gao.gov/assets/680/675747.pdf>; Office of Inspector General, U.S. Department of Housing and Urban Development, *Ginnie Mae Did Not Adequately Respond to Changes in its Issuer Base* (Sept. 21, 2017), available at: <https://www.hudoig.gov/sites/default/files/documents/2017-KC-0008.pdf>.

354. See Fannie Mae, *Seller Guide* (June 5, 2018), at Part A4-1; Freddie Mac, *Seller/Servicer Guide* (June 13, 2018), at Chapter 2101; Ginnie Mae, *MBS Guide* (Jan. 25, 2018), at Chapter Three.



Furthermore, during periods of sustained financial stress, traditional depository lenders have access to sources of liquidity that nonbanks lack, such as insured customer deposits and FHLBs advances. Nondepositories are instead funded mainly through lines of credit and repurchase agreements, which, due to their short-term nature are subject to roll-over risk and margin requirements in the event of a deteriorating credit environment.<sup>355</sup>

High among concerns about nondepositories is the durability of these funding structures for nonbank servicers. When borrowers stop making mortgage payments, servicers of those loans continue to advance scheduled payments to investors and other parties until the delinquency has been resolved or the loan has been purchased out of its securitized pool. While servicers may be able to seek reimbursement for these advances depending upon the federal insurance or guaranty program, they must make them out of their own funds in the interim. Servicers of both GSE and Ginnie Mae securities face this risk; however, the higher delinquency rates and longer foreclosure timeline for FHA-insured loans underlying Ginnie Mae pools, as well as differences in delinquent loan buyout practices, may subject Ginnie Mae servicers to extended periods of liquidity strain exactly when financing may be most challenging. As counterparty risk represents Ginnie Mae's main financial exposure, its leadership is reasonably concerned with potential challenges from a sustained period of economic stress that tests the financial capacity of these nonbanks to continue to make servicing advances.

Ginnie Mae has multiple counterparty risk-management tools in use today, including on-site reviews, assignment of proprietary risk grades, and performance profiles. Additionally, Ginnie Mae, as well as the GSEs, have quarterly visibility into nonbank counterparty financial information, including debt facilities, through required submission of information through the Mortgage Bankers Financial Reporting Form.<sup>356</sup> However, data quality and the present fields required for reporting may be insufficient to provide the level of transparency needed to assess counterparty financial health. Ginnie Mae continues to pursue improvements to its counterparty risk management framework, including subjecting its servicers to a liquidity stress test to gauge the durability of their access to capital during a period of sustained financial stress.<sup>357</sup>

While the size of Ginnie Mae's portfolio and the nature of its counterparty risk has changed dramatically in recent years, Ginnie Mae lacks flexibility to adjust its MBS fees and hire additional staff to manage this risk. Under Ginnie Mae's charter, the maximum fee it can charge for its MBS guaranty is set at 6 basis points,<sup>358</sup> and is not permitted to be adjusted based on risks arising from changes in the housing market or from Ginnie Mae's counterparty exposure specifically. Additionally, Ginnie Mae's permanent staffing resources remain constrained, with approximately 150 permanent employees overseeing a \$2 trillion portfolio. At present, Ginnie Mae depends on annual congressional appropriations to pay permanent staff. While Ginnie Mae is able to utilize its revenues to contract with outside firms for support services, stakeholders, including Ginnie

---

355. See Office of Financial Research, *Monitoring GNMA/GSE Pipeline Liquidity*, slide deck presentation (July 28, 2016), available at: [https://www.financialresearch.gov/frac/files/FRAC-meeting\\_GSE-Working-Group-Presentation\\_07-28-2016.pdf](https://www.financialresearch.gov/frac/files/FRAC-meeting_GSE-Working-Group-Presentation_07-28-2016.pdf).

356. See Fannie Mae Seller Guide, Freddie Mac Seller/Servicer Guide, and Ginnie Mae MBS Guide.

357. See Ginnie Mae 2020.

358. 12 U.S.C. § 1721(g)(3)(A).

Mae leadership, have highlighted the need for flexibility to hire permanent staff with the requisite experience, and compensated at competitive rates, to complement existing resources in providing risk management appropriate to oversee Ginnie Mae's considerable taxpayer exposure.<sup>359</sup>

### *Recommendations*

Treasury recommends that Ginnie Mae collaborate with FHFA, the GSEs, and the Conference of State Bank Supervisors to expand and align standard, detailed reporting requirements on nonbank counterparty financial health, including terms and covenants associated with funding structures, to provide confidence that taxpayers are protected during a period of severe market stress. Additionally, Treasury supports Ginnie Mae's consideration of enhancing its counterparty risk mitigation approach, including through the imposition of stress testing requirements that can provide information on the financial health of servicer counterparties across an economic cycle. Furthermore, in order to protect taxpayers, Treasury recommends Ginnie Mae have sufficient flexibility to charge guaranty fees appropriate to cover additional risk arising from changes in the overall market or at the program level.

Treasury recommends a comprehensive assessment of Ginnie Mae's current staffing and contracting policies, including the costs and benefits of alternative pay and/or contracting structures. Ginnie Mae would be better equipped to manage its program and monitor counterparty risk if it were able to more readily attract personnel with requisite expertise by paying salaries comparable to those at other financial agencies with premium pay authority. Additionally, being able to adopt similar contracting procedures as other agencies that are outside of federal acquisition statutes and regulations would enable Ginnie Mae to more effectively monitor and respond to changing market conditions and needs. However, any change to Ginnie Mae's personnel or contracting policies should be informed by a comprehensive assessment of current challenges. The potential benefits of alternative pay and/or contracting structures should be weighed against the additional federal costs that would be incurred.

For nondepositories, providing greater transparency about their financial health should be a welcome step toward addressing concerns about their sustainability throughout the cycle and the risk they pose to taxpayers relative to their participation in federally supported loan and securitization programs. Furthermore, greater standardization of requirements and reporting could benefit nondepositories by reducing disparate state-level and principal counterparty requirements.

## **Student Lenders and Servicers**

### **Overview**

The majority of student loans are originated by the federal government through the U.S. Department of Education's (Education) Direct Loan Program. In 2010, Education fully moved to the Direct Loan Program, under which Education originates loans to students. At the same time, Congress ended a legacy guaranteed-loan program where private lenders were compensated by the

359. See HUD Office of Inspector General *Monitoring of Nonbank Issuers Presents Challenges for Ginnie Mae* (Mar. 13, 2017), available at: <https://www.hudoig.gov/reports-publications/topic-briefs/monitoring-of-nonbank-issuers-presents-challenges-ginnie-mae>.

federal government to originate and service federal student loans with guarantees of 97%. Today, the federal loan portfolio has nearly \$1.4 trillion in outstanding student loans to nearly 43 million borrowers.<sup>360</sup> Federal student loan interest rates are set at a spread to the last 10-year Treasury note auction prior to June 1, with statutory caps by loan program. Federal student loans are originated at fixed rates. However, since interest rates fluctuate based on the interest rate on the relevant 10-year Treasury note, a student who has multiple loan types from multiple school years will have loans that carry different interest rates.

Figure 20: Federal Student Loan Interest Rates and Origination Fees

Loan Type	2017-18 Interest Rate	2018-19 Interest Rate	Statutory Interest Rate Cap	2017-18 Origination Fee
Subsidized Undergrad	4.45%*	5.05%	8.25%	1.066%
Unsubsidized Undergrad	4.45%	5.05%	8.25%	1.066%
Unsubsidized Graduate	6%	6.6%	9.5%	1.066%
Graduate PLUS	7%	7.6%	10.5%	4.264%
Parent PLUS	7%	7.6%	10.5%	4.264%

\*Subsidized loans do not accrue interest while the borrower is in school and during a six-month grace period when the borrower leaves school.

Source: U.S. Department of Education and Treasury staff analysis.

Education provides both subsidized and unsubsidized loans to undergraduate borrowers, unsubsidized loans to graduate students, and higher interest loans with higher origination fees to both graduate and parent borrowers who do not have an adverse credit history. Undergraduate borrowers must comply with strict loan limits of \$31,000 for dependent students and must demonstrate financial need. To manage repayment for the loans it has originated, Education hires and manages contractors who perform servicing and collections on the Direct Loan portfolio.

The private student loan market is small relative to the size of the federal portfolio at an estimated \$113 billion, or about 8% of all outstanding student loans originated by banks, credit unions, and nonbanks.<sup>361</sup> The private student loan market also offers loans to undergraduates, graduate students, and parents but differs from the federal portfolio in that these loans are underwritten. The majority of private student loans are cosigned, with nearly all undergraduate loans in recent years requiring a cosigner; 92% in the 2017-18 award year, and 62% of graduate students requiring a cosigner in the same award year.<sup>362</sup>

In the past five years, more nonbanks have entered the student lending market with a focus on refinancing both private and federal loans into lower interest rate loans. While interest rates on

360. Office of Federal Student Aid, U.S. Department of Education, *Federal Student Aid Portfolio Summary*, available at: <https://studentaid.ed.gov/sa/about/data-center/student/portfolio> (as of the end of first quarter 2018) (last accessed June 15, 2018).

361. MeasureOne, *Private Student Loan Report – Q3 2017*, available at: <https://www.measureone.com/psl.php>.

362. *Id.* at 24.

these products may be lower than those on some federal student loans, the federal student loan program continues to provide borrower protections that are unmatched by private loan products. Federal student loan borrowers considering refinancing into private loans should carefully consider whether they will potentially utilize these federal benefits including: a variety of repayment plans including plans based on income, forbearances available for borrowers facing economic hardship, loan forgiveness programs after 20 or 25 years of income-driven repayments, Public Service Loan Forgiveness, and loan discharges for borrowers who become totally and permanently disabled.

Figure 21: Features of Federal Student Loans

	Description	Feature of Private Student Loans?	Feature of Other Consumer Credit Products?
<b>Need based program</b>	Federal student loans are not underwritten and instead are based on demonstrated financial need and in some cases cost of attendance.	No	No
<b>Loan limits</b>	Loan limits for undergraduate borrowers are based on whether borrower is considered “dependent” or “independent” not based on tax filing status but rather the borrowers age, marital status, military status, and children and other dependents.	No	No
<b>Delayed repayment</b>	Payment is not required while a borrower is in school or during a 6-month grace period after the borrower leaves school or drops below half-time enrollment.	Yes	No
<b>Credit reporting</b>	Delinquency on Direct Loans is not reported to the consumer credit bureaus until day 90 of delinquency.	No, delinquency reported begins as early as day 30.	No, all others report delinquency as early as day 30.
<b>Late fees</b>	Direct loans have no late fees	No	No
<b>Interest capitalization</b>	Interest capitalizes with every change in status on a federal student loan, including: entering repayment, leaving the grace period, switching repayment plans, use of deferments or forbearances, default, rehabilitating a defaulted loan, or consolidating existing loans. Interest capitalization increases the borrower’s principal balance and interest expense paid over the life of the loan.	No	No
<b>Interest accrual</b>	Interest accrues on a daily basis, meaning the interest balance changes each day.	Yes	Daily interest accrual generally used in credit cards; monthly accrual is used in mortgages.
<b>Repayment plans</b>	Direct loans are eligible for up to eight repayment plans, some of which are dependent on eligibility requirements related to loan balance and date of loan origination. Some repayment plans cause negative amortization.	Generally only one amortizing repayment plan is offered.	No

Source: Treasury staff analysis.

## Program Complexity and Impact

The federal student loan program is immensely complex due to: (1) the variety of loan types offered and outstanding legacy loan types that continue to require servicing; (2) eight repayment plans each with different eligibility requirements, repayment structures, and features; and (3) product features that differ from nearly all other consumer finance products. The natural consequence of this complexity is that it is difficult for borrowers, even those who are sophisticated, to navigate the program and effectively manage their repayment responsibilities. Because the program is difficult to understand, borrowers rely on servicers to answer questions about repayment, enroll borrowers in an appropriate and sustainable repayment plan, and assist borrowers when they struggle to make their payments. Federal student loan servicers have indicated to Treasury that the program's complexity not only makes loans more difficult to service, but also increases the cost of servicing. For example, call center staff at each federal student loan servicer must be well versed on all of the current and legacy loan types and repayment plans, as each have features with financial consequences and tradeoffs for borrowers.

## **Issues and Recommendations**

### Student Loan Servicing Standards

Due to the federal student loan program's complexity and Education's limited guidance on servicing standards, servicers have largely relied on internal business practices to determine how to effectively service federal student loans. While this was intended to promote innovation, it has caused difficulty for servicers in that (1) borrowers may be treated differently by different servicers, causing financial disparities, (2) Education's website provides generic information but each servicer must maintain its own website, (3) federal and state regulators have raised concerns with servicing practices, and (4) both the cost of servicing and difficulty of oversight have increased.

Borrowers in the same financial situation who contact two different servicers in the federal student loan program to enroll in a more affordable repayment plan may end up with different results and advice, which may result in a financial impact on the borrowers. Federal student loan servicers are instructed to enroll borrowers looking to reduce their payments into the plan that will cost the borrower the least over time. This sounds simple, but the servicer's call center agent may have only limited information from a borrower and may make decisions about tradeoffs between two similar repayment plans (e.g., Pay As You Earn and Revised Pay As You Earn) that confer slightly different benefits. Federal borrowers have also faced financial harm in even more straightforward circumstances, such as the application of over- and underpayments. Some servicers have not provided borrowers the ability to direct payments to a specific loan or have not fully implemented guidance from Education on how to process over- and underpayments.

Each servicer uses a proprietary format for its monthly statements and certain correspondence. Because of these disparities, Education's website lacks basic financial literacy information about how to read a monthly statement or plain language explanations of different letters sent by servicers with action steps on how to address the correspondence. To address this issue, servicers have created extensive proprietary websites aimed at serving their customers. Borrowers searching online for advice may get different information depending on their search results from Education's website and the servicer's website.

Federal student loan servicing currently lacks effective minimum servicing standards. This has created difficulties for federal student loan servicers when they communicate with regulators about their servicing practices. For example, a servicer may discuss a specific servicing practice with Education and gain approval for that practice but run into consumer protection concerns about the same practice in examinations or discussions with the Bureau. If Education prescribed minimum servicing standards, Education could vet these standards with other relevant agencies so servicers do not face conflicting guidance from multiple federal agencies. Further, a public, common servicing manual, like the servicing manual used in the federal guaranteed student loan program, would be helpful for state legislators and regulators considering additional regulation. With effective minimum servicing standards in place, states may decline to regulate federal student loan servicers further.

Finally, servicing standards could reduce the expense of servicing for taxpayers, as Education would not need to rely so heavily on contract change orders. In the current Direct Loan servicing contract, change orders are used to require servicers to take specific actions, for example to require servicers to conduct outreach to borrowers who must provide updated income information to remain in an income-driven repayment plan, but at a cost to the taxpayer. Servicing standards would reduce the need for these ad hoc contract changes, which are more expensive and difficult for servicers to implement than if built into the contract requirements up front. With common servicing standards, contract oversight would be easier for Education to conduct because both the servicer and Education would have clear, written guidance describing expectations.

#### *Recommendations*

Education should establish guidance on minimum standards specifying how servicers should handle decisions with significant financial implications (e.g., payment application across loans, prioritizing repayment plans, and use of deferment and forbearance options), minimum contact requirements, standard monthly statements, and timeframes for completing certain activities (e.g., processing forms or correcting specific account issues). Treasury applauds the required use of Education branding on servicing materials in the new Direct Loan servicing procurement to reduce borrower confusion.

#### **Student Loan Borrower Communication**

In the federal student loan program, servicers under contract with Education begin contacting borrowers directly following the disbursement of the borrower's first loan and will continue to contact the borrower at minimum on a quarterly basis while the borrower is in school and on a monthly basis while the borrower is in repayment. Federal student loan servicers rely heavily on U.S. mail, phone calls, and email to communicate with borrowers.

When loans enter repayment, borrowers generally create an online account with their student loan servicer. At this point, the servicer may receive the borrowers' email address for the first time as borrowers are not required to provide this information while applying for federal financial aid. Federal student loan servicers employ emails that many borrowers and consumer advocates feel are of limited utility as they often contain messages similar to, "A new message is available on your online account," rather than more substantive emails.



Federal student loan servicing also lacks e-signature capability, creating unnecessary cost and inefficiency for federal student loan servicers. Without e-signature, borrowers must access computers, find forms online, print physical copies of documents, sign those documents, then send those documents by mail, for processing and scanning in a servicer mail facility. This adds several steps for borrowers. To more successfully receive forms back from borrowers, some student loan servicers have mailed borrowers prepopulated forms and included an addressed and stamped envelope. The expense that servicers incur in using the U.S. mail for is significant relative to the monthly compensation federal student loan servicers receive per borrower. E-signature technology could expedite the process of completing forms and help borrowers more responsibly manage their student loan accounts, while reducing servicer costs. A reduction in servicer costs could also yield savings to the U.S. taxpayer in the form of lower servicer contract costs.

### *Recommendations*

In Education's new Direct Loan servicing contract, Education should require student loan servicers to make greater use of emails and provide guidance to servicers on how to use email appropriately to balance privacy and security concerns with the need for effective and timely communication. All emails sent to federal student loan borrowers should provide enough information for borrowers to easily discern whether action must be taken on their account. Education should contract with providers of secure e-signature software and cloud technology for use by federal student loan servicers on all forms.

### **Data Quality**

With a \$1.4 trillion federal student loan portfolio, it is critical that Education monitor and manage the taxpayer investment in higher education carefully. Under the existing Direct Loan servicing contract, servicers maintain the majority of loan level data about the portfolio. Because data about the student loan portfolio comes from many different sources (e.g., borrowers, schools, legacy lenders and servicers, and nine current servicers), the data is often in incompatible formats and housed in separate, antiquated systems. This limits Education's ability to appropriately monitor trends in performance that should be addressed through servicing changes and manage the federal student loan portfolio. Further, Education releases very limited data about the performance of the portfolio. Taxpayers deserve greater insight into how this large investment is performing.

### *Recommendations*

Education must improve its data quality and portfolio management. Education's Office of Federal Student Aid, which operationalizes the \$1.4 trillion federal student loan portfolio, should include in its management team individuals with significant expertise in managing large consumer loan portfolios.

Education should take steps to address existing data quality issues to better monitor and manage portfolio performance. Education should increase transparency by publishing greater portfolio performance data, servicer performance data, and cost estimation analysis on its website to give stakeholders greater insight into Education's management of the taxpayer investment in higher education.

### Institutional Accountability

Treasury remains concerned about the lack of institutional accountability in student lending. Colleges and universities have very few accountability requirements related to the performance of the loans their students receive through the federal student loan program. The existing metric used by Education, the cohort default rate, does not capture other problematic loan statuses that show the borrower may be struggling to repay (e.g., significant delinquencies and extended forbearances) and the metric is easily gamed by institutions. Treasury analysis of Education data indicates that principal repayment after five years is highly predictive of future loan performance. Treasury is concerned about schools that do not provide student loan borrowers good value, often leading to indebtedness the borrower cannot repay in a reasonable time period.

### Recommendations

Treasury supports legislative efforts to implement a risk-sharing program for institutions participating in the federal student loan program based on the amount of principal repaid following five years of payments. Schools whose students have systematically low loan repayment rates should be required to repay small amounts of federal dollars to protect taxpayers' growing investment in the federal student loan program. Congress should consider how to address schools with systematically low repayment rates but large populations of disadvantaged students.

## Short-Term, Small-Dollar Installment Lending

### Overview

Short-term, small-dollar loans, which typically range from \$300 to \$5,000, account for nearly \$90 billion in annual lending.<sup>363</sup> These products, offered by nonbank lenders and some depository institutions, include lump-sum loans, with terms of 1 month or less, as well as installment loans with terms of up to 2 years. The demand for short-term, small-dollar products is high because many households struggle with income volatility, thin or no credit files or a subprime score, or lack of access to mainstream financial products that meet their needs. According to the FRB, 40% of Americans say they could not easily cover an emergency expense of \$400.<sup>364</sup> FDIC data also indicates that almost 20% of U.S. households are considered underbanked because of their use of alternative financial services.<sup>365</sup>

363. See Center for Financial Services Innovation, *2017 Financially Underserved Market Size Study* (Dec. 2017), at 44–47, available at: [https://s3.amazonaws.com/cfsi-innovation-files-2018/wp-content/uploads/2017/04/27001546/2017-Market-Size-Report\\_FINAL\\_4.pdf](https://s3.amazonaws.com/cfsi-innovation-files-2018/wp-content/uploads/2017/04/27001546/2017-Market-Size-Report_FINAL_4.pdf) (for revenue and volume data on pawn loans, online payday loans, storefront payday loans, installment loans, title loans, and marketplace personal loans).

364. Board of Governors of the Federal Reserve System, *Report on the Economic Well-Being of U.S. Households in 2017* (May 2018), at 21–22, available at: <https://www.federalreserve.gov/publications/files/2017-report-economic-well-being-us-households-201805.pdf>.  
Board of Governors of the Federal Reserve System, *Report on the Economic Well-Being of U.S. Households in 2016* (May 2017), at 26–27, available at: <https://www.federalreserve.gov/publications/files/2016-report-economic-well-being-us-households-201705.pdf>.

365. Federal Deposit Insurance Corporation, *2015 FDIC National Survey of Unbanked and Underbanked Households* (Oct. 20, 2016), available at: <https://www.fdic.gov/householdsurvey/>.



### **Regulatory Framework**

Nonbank, short-term, small-dollar lenders are regulated at both the federal and state levels. At the federal level, Dodd-Frank authorized the Bureau to supervise nondepository covered persons offering or providing payday loans to consumers for compliance with federal consumer protection laws.<sup>366</sup> As noted previously, the Bureau also has authority to prohibit certain acts or practices that are unfair, deceptive, or abusive.

State laws set product feature limitations and may require licensing of nonbank lenders to make loans in the state. Based on the product (e.g., payday or installment), product feature restrictions may include loan size caps, interest rate limits, repetitive use restrictions, and even outright prohibitions. These restrictions are often enforced by state banking agencies or state attorneys general. According to the National Conference of State Legislatures, 37 states have laws allowing payday lending in some form. Thirteen states have prohibited payday lending outright.

Banks providing short-term, small-dollar loans may be regulated by state or federal law, depending on the type of bank. Prudential regulators and the Bureau have authority to evaluate these product offerings for compliance with federal consumer protection laws. Additionally, as depository institutions, banks offering these products must meet safety and soundness requirements.

### **Issues and Recommendations**

In November 2017, the Bureau issued a final rule entitled “Payday, Vehicle Title, and Certain High Cost Loans” (Payday Rule) that applies to lenders that extend credit with terms of 45 days or less as well as longer-term credit with balloon payments (Covered Loans).<sup>367</sup> Lenders making Covered Loans are required to determine that the borrower has the ability to repay the loan. This ability to repay is based on a determination that the consumer can make payments on the loan and still meet major financial obligations and basic living expenses without needing to re-borrow over the next 30 days. When underwriting a Covered Loan, the lender is required to obtain and verify the consumer’s net income and financial obligations and ensure that the loan will not result in the consumer having a sequence of more than three Covered Loans within 30 days of each other. A failure to comply with the ability to repay underwriting standard is an unfair and/or abusive practice. In January 2018, the Bureau announced its intention to engage in further rulemaking to reconsider the Payday Rule.

The Bureau’s rule raises two primary concerns. First, states maintain authority to regulate short-term, small-dollar lending, which raises questions regarding the need for additional federal regulation. In 2016, the House Financial Services Committee held a hearing to evaluate the Bureau’s proposed Payday Rule and its interaction with state authority. Testimony highlighted the extensive action taken by states to pass laws authorizing, restricting or prohibiting payday lending. Similarly, in 2016, a bipartisan group of 16 state attorneys general sent a letter to then Bureau Director Cordray cautioning him against restricting state authorities by moving forward with the Payday Rule. Specifically, these attorneys general highlighted how states were best positioned to regulate

366. 12 U.S.C. § 5514(a)(1)(E).

367. Payday, Vehicle Title, and Certain High-Cost Installment Loans (Oct. 5, 2017) [82 Fed. Reg. 54472 (Nov. 17, 2017)].

these sometimes high-priced products, and to understand the credit and consumer protection needs of the consumers in their states.

Second, the Payday Rule would further restrict consumer access to credit and decrease product choices. According to the Bureau's estimates, the Payday Rule would reduce overall payday loan volume by as much as two-thirds.<sup>368</sup> This reduction in access to regulated, short-term, small-dollar loans may leave these consumers vulnerable to dangerous alternatives such as unscrupulous, unlicensed, offshore or otherwise illegal lenders.<sup>369</sup> This is especially true as short-term, small-dollar lending activity has been largely pushed out of the traditional banking system.

Banks can operate as additional sources of credit for consumers who otherwise may be unbanked or underbanked and lead to "a path to more mainstream financial products."<sup>370</sup> However, in 2013, the OCC and FDIC issued guidance on direct deposit advance products, which identified supervisory risks with the offering of these products.<sup>371</sup> Following the release of the guidance, banks withdrew these products from the market. Stakeholder feedback highlighted that the low margin and heightened maintenance of these products did not offset the increased regulatory scrutiny. This outcome further restricted short-term, small-dollar lending from the traditional banking system.

Last year, the OCC recognized the consumer demand for these products. In October 2017, the OCC rescinded its guidance because "consumers who would prefer to rely on banks and thrifts for these products may be forced to rely on less regulated lenders and be exposed to the risk of consumer harm and expense."<sup>372</sup> The OCC has also issued a bulletin providing guidance to OCC-supervised banks on core lending principles for short-term, small-dollar installment lending.<sup>373</sup> The FDIC has yet to rescind its previous guidance.

### *Recommendations*

Treasury recognizes and supports the broad authority of states that have established comprehensive product restrictions and licensing requirements on nonbank short-term, small-dollar installment lenders and their products. As a result, Treasury believes additional federal regulation is unnecessary and recommends the Bureau rescind its Payday Rule.

Additionally, Treasury recommends that federal and state financial regulators take steps to encourage sustainable and responsible short-term, small-dollar installment lending by banks. Specifically,

368. *Id.* at 54817.

369. Sudhir Venkatesh, *Off the Books: The Underground Economy of the Urban Poor* (2006); Todd J. Zywicki, Mercatus Center, *The Case Against New Restrictions on Payday Lending*, working paper (July 2009), available at: [https://www.mercatus.org/system/files/WP0928\\_Payday-Lending.pdf](https://www.mercatus.org/system/files/WP0928_Payday-Lending.pdf).

370. Office of the Comptroller of the Currency, *Core Lending Principles for Short-Term, Small-Dollar Installment Lending*, OCC Bulletin 2018-14 (May 23, 2018), available at: <https://www.occ.treas.gov/news-issuances/bulletins/2018/bulletin-2018-14.html> ("OCC Core Lending Principles").

371. Direct Deposit Advance products, offered by banks, are a "small-dollar, short-term loan or line of credit that a bank makes available to a customer whose deposit account reflects recurring direct deposits." Rescission of Guidance on Supervisory Concerns and Expectations Regarding Deposit Advance Products (Oct. 5, 2017) [82 Fed. Reg. 47602 (Oct. 12, 2017)].

372. *Id.*

373. OCC Core Lending Principles.

Treasury recommends that the FDIC reconsider its guidance on direct deposit advance services and issue new guidance similar to the OCC's core lending principles for short-term, small-dollar installment lending.

## Debt Collection

Debt collectors and debt buyers are important market participants for the continued functioning of the consumer credit markets and other industries that rely on the recoveries from debt collection or the sale of delinquent debt to minimize losses.<sup>374</sup> Debt collectors can be segmented into two categories: first-party debt collectors and third-party debt collectors. By reducing losses from unpaid balances, debt collectors and debt buyers increase efficiency in the consumer credit markets through the reduced cost of credit, which can yield greater access to credit.

## Issues and Recommendations

The Fair Debt Collection Practices Act (FDCPA), was enacted in 1977 to eliminate abusive, deceptive, and unfair conduct by third-party debt collectors working to collect consumer debt incurred primarily for personal, family, or household purposes, thereby excluding business, corporate, or agricultural debt.<sup>375</sup> Dodd-Frank provided the Bureau rulemaking authority for the FDCPA, as well as supervision and enforcement authority for the entities under the Bureau's jurisdiction.<sup>376</sup> The Bureau's supervision manual for the FDCPA makes clear that an institution is not considered a debt collector under the FDCPA, "when it collects: another's debts in isolated instances; its own debts it originated under its own name; debts it originated and then sold, but continues to service (e.g., mortgage and student loans); debts that were not in default when they were obtained; and debts that were obtained as security for a commercial credit transaction."<sup>377</sup> These exclusions from the FDCPA allow creditors who have originated the debt (first-party debt collectors) to attempt recovery on that debt without the restrictions and potential liability associated with the FDCPA.

Debt collectors and debt buyers are of continued interest to policymakers, as they are frequently the source of consumer complaints and yielded one of the most frequent types of consumer complaints of any industry to both the Federal Trade Commission (FTC)<sup>378</sup> and the Bureau<sup>379</sup> in the

---

374. The majority of debt collected is related to healthcare, student loans, and debt owed to state, local, and federal governments. See Ernst & Young, *The Impact of Third-Party Debt Collection on the US National and State Economies in 2016* (Nov. 2017), at 5, available at: <https://www.acainternational.org/assets/ernst-young/ey-2017-aca-state-of-the-industry-report-final-5.pdf>.

375. Bureau of Consumer Financial Protection, *Fair Debt Collection Practices Act Supervision Manual* (Oct. 2012), available at: [https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/102012\\_cfpb\\_fair-debt-collections-practices-act-fdcpa\\_procedures.pdf](https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/102012_cfpb_fair-debt-collections-practices-act-fdcpa_procedures.pdf) ("FDCPA Supervision Manual").

376. Dodd-Frank §§ 1002(12)(H), 1024(b)-(c), and 1025(b)-(c) [12 U.S.C. §§ 5481(12)(H), 5514(c), and 5515(c)].

377. FDCPA Supervision Manual, at 1.

378. Federal Trade Commission, *Consumer Sentinel Network Data Book 2017* (Mar. 2018), at 4, available at: [https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer\\_sentinel\\_data\\_book\\_2017.pdf](https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf).

379. Bureau data from Consumer Complaint Database, available at: <https://www.consumerfinance.gov/data-research/consumer-complaints/> (filtered for complaints received during 2017).

last year. Stakeholders representing a variety of interests, including consumer advocates, lenders, debt collectors and debt buyers, and the FTC, have expressed concerns about the adequacy of information transferred with the sale of debt to third-party debt collectors. Data provided by industry indicates there is an inefficiency in this market as well. According to a survey of debt collectors and buyers, consumers request verification on nearly one in five accounts referred to debt collectors, with approximately 10% of consumers filing a formal dispute.<sup>380</sup> While FTC data shows fewer disputes, the FTC reports that debt buyers indicate they are only able to verify about half of the debts that consumers dispute, demonstrating that debt buyers are not receiving sufficient information about the debt to prove to the consumer that the debt they are attempting to collect is valid.<sup>381</sup>

In 2013, the Bureau published an advance notice of proposed rulemaking on debt collection practices.<sup>382</sup> In the proposal, the Bureau indicated concern about the amount of information that is transferred with a debt when it is sold to a third-party collector, and requested comment on what type of information should be provided in three critical areas and the adequacy of that information: (1) the correct person; (2) the correct amount owed; and (3) the correct documentation provided with the debt.<sup>383</sup> To date, the Bureau has not issued a notice of proposed rulemaking following the 2013 proposal. In the absence of minimum federal standards for the information creditors must provide to debt collectors and buyers, certain companies and trade groups have committed to higher standards for this information prior to debt collection or sale. Additionally, some states have enacted laws concerning data quality standards for debt buyers and required disclosures. For example, California law prohibits debt buyers from contacting consumers about a debt unless it possesses information about the debt balance, date of default, and original creditor. Illinois, Texas, and New York statutes require disclosure of specific information to consumers by debt collectors.

### *Recommendation*

Treasury recommends the Bureau establish minimum effective federal standards governing the collection of debt by third-party debt collectors. Specifically, these standards should address the information that is transferred with a debt for purposes of debt collection or in a sale of the debt. Further, the Bureau should determine whether the existing FDCPA standards for validation letters to consumers should be expanded to help the consumer assess whether the debt is owed and determine an appropriate response to collection attempts.

Treasury does not support broad expansion of the FDCPA to first-party debt collectors absent further Congressional consideration of such action.

---

380. Ernst and Young, at 5.

381. Federal Trade Commission, *The Structure and Practices of the Debt Buying Industry* (Jan. 2013), at iv, available at: <https://www.ftc.gov/sites/default/files/documents/reports/structure-and-practices-debt-buying-industry/debtbuyingreport.pdf>.

382. Debt Collection (Regulation F) (Nov. 5, 2013) [78 Fed. Reg. 67848 (Nov. 12, 2013)].

383. *Id.*

## IRS Income Verification

### Overview

The federal government plays a role not only supporting policies that advance the prudent application of financial technology in credit markets, but also, at times, by furnishing information integral to the consumer and small business underwriting process itself. In this capacity, the government needs to take care that it is not inhibiting innovation in practice that it supports in policy. One commonly cited credit industry challenge is the interaction with IRS's income verification system, including the lack of an interface, such as an Application Programming Interface (API), to perform this function in an automated fashion.

As part of assessing a loan applicant's financial capacity for assuming a credit obligation, lenders for consumer and small business credit often request that a loan applicant provide tax return information to verify income information submitted by the applicant. For some credit decisions, such as mortgages, lenders perform income verification to adhere to regulatory requirements to assess a borrower's ability to repay the debt. For other classes of credit, particularly those served by marketplace lenders, income verification is an important credit risk assessment tool as it helps develop a more complete picture of a borrower's overall risk assessment and the likelihood for that borrower to be able to fulfill the terms of the loan.<sup>384</sup>

Lenders assess financial capacity using a range of information and tools. Some information is provided directly by the borrower. Other information is provided by third parties, some of which requires the consent of the borrower before such information can be provided to the lender. For credit decisions, loan terms are largely determined by applicant-submitted information and data purchased from private credit bureaus that document the credit histories of millions of Americans. Official tax return documentation obtained pursuant to authorization provided by the borrower is a critical source of information and is used by lenders to verify that loans comply with existing regulations (e.g., the Ability to Repay/Qualified Mortgage rule) and to confirm information provided by the borrower during the underwriting process. Lenders generally determine a borrower's creditworthiness before utilizing official income data, due in part to challenges with quickly and securely obtaining tax return information from the IRS once the borrower authorizes the IRS to disclose such information to the lender.

### Issues and Recommendations

In the present system, a credit applicant facilitates income verification by completing a request for a copy of his or her tax transcripts through IRS Forms 4506, 4506-T, 4506T-EZ, or 8821 through the IRS.<sup>385</sup> Through these forms, a borrower gives consent for the IRS to disclose his or her summarized tax transcript to a third party.<sup>386</sup> Lenders often utilize third-party vendors to process these

---

384. See Marketplace Lending Association, *Update the IRS 4506-T API*, available at: <http://marketplacelendingassociation.org/wp-content/uploads/2017/08/Build-an-API-for-the-IRS-4506-T.pdf>.

385. See IRS Income Verification Express Service at <https://www.irs.gov/individuals/international-taxpayers/income-verification-express-service>.

386. Federal law prohibits disclosure or use of federal tax return information except as authorized by that title. See 26 U.S.C. § 6103. Violations are subject to criminal penalty. Federal law [26 U.S.C. §6103(c)] permits the IRS to disclose tax return information to third parties with consent of the taxpayer.

transcript requests. To protect the confidentiality of federal tax return information, third-party vendors must meet strict security and technology requirements set by the IRS.

The IRS typically processes transcript requests submitted through its Income Verification Express Service and provides borrower tax summary data to the authorized third party within two to three days, although lenders report it can take considerably longer during periods of high volume. Credit decisions can be delayed pending receipt. Given the millions of credit transactions that depend on IRS verification, delays in this process may impose added costs on borrowers and the economy from the collective delays in completing these transactions. In a financial system increasingly adopting real-time information transfer and access to borrower bank and asset profiles, the delay in receiving IRS income verification can be particularly frustrating for lenders and borrowers.

The IRS currently fulfills 4506-T requests by transmitting borrower tax summary data to an authorized third party's secure mailbox. In other data aggregation situations, such as gathering borrower bank balances, lenders are able to obtain the needed borrower financial information through an API to instantaneously and safely transfer data. However, for lenders to gather federal tax data, they must rely on slower IRS verification technology that lacks the key type of digital interface enabled by an API. Given existing IRS priorities and funding levels, developing such a digital interface capability at the IRS would require multiple levels of front-end as well as back-end enhancements, including development of an e-signature capability and an authorization solution.

Enabling faster, more reliable income verification could facilitate lenders' ability to better incorporate historical income data earlier into credit pricing, as opposed to using it for verification purposes at the back-end of the underwriting process. Further, this data could potentially expand access to credit by providing lenders a broader view into a credit applicant's creditworthiness, where an otherwise incomplete credit picture, or on-the-border credit score, could lead a lender to decline an applicant. This is particularly true for small businesses, as it could improve the ability to consolidate debts incurred on personal credit cards into a consolidated business loan, as a lender would be able to more immediately analyze income history and observe patterns of growth that indicate creditworthiness.

### *Recommendation*

It is important that the IRS update its income verification system to leverage a modern, technology-driven interface that protects taxpayer information and enables automated and secure data sharing with lenders or designated third parties. Such an interface would bring a critical component of the credit process up to speed with broader innovations in financial technology. Borrowers, and the broader economy, stand to benefit through lower operational costs for lenders, elimination of paperwork and delays, incorporation of important credit information into credit pricing, and potentially expanded access to credit as tax information can be more easily incorporated into determinations of creditworthiness. Any changes must balance faster access with security controls that ensure that only information that borrowers choose to share with lenders is shared, that lenders and vendors have security controls in place to protect taxpayer data, and that significant security protections are put into place to protect sensitive taxpayer information.

While the IRS is working to update its technology, including technology used by lenders for income verification, these efforts are dependent on funding in light of other IRS mission-critical priorities.



Treasury recommends Congress fund IRS modernization, which would include upgrades that will support more efficient income verification.

## New Credit Models and Data

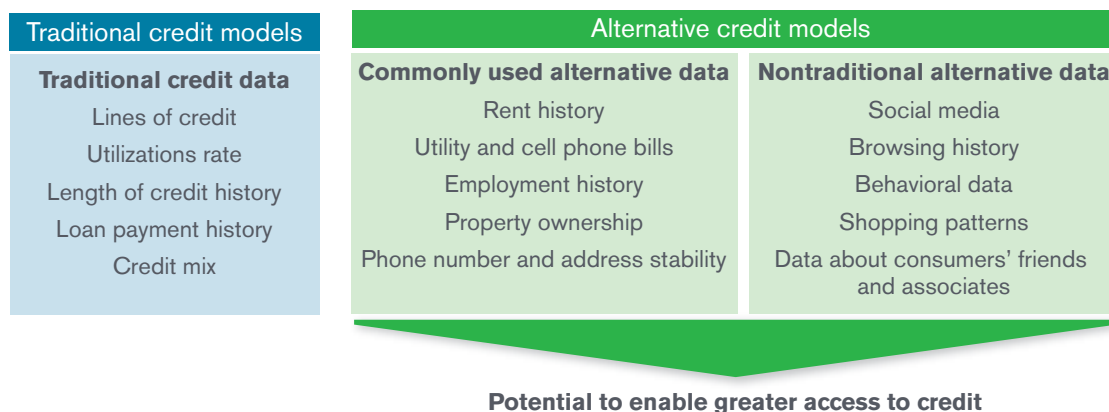
### Overview

U.S. financial institutions have traditionally relied upon a common set of credit information for purposes of extending consumer credit. This generally standardized credit data, which consists primarily of consumer debt and payment history, is consolidated by national credit bureaus and is fed into a common set of credit models which generate consumer credit scores that are widely used across U.S. financial institutions. One of the most dominant existing credit score models is the one used by FICO to generate the widely used FICO score, which is reportedly used by some 90% of top lenders.<sup>387</sup>

With the explosion in available data and advances in modeling methods, a growing number of firms — existing and new entrants — have begun to use or explore a wide range of newer data sets or advanced algorithms (including those based upon machine-learning practices) to support credit underwriting decisions. This interest in newer data and models has taken place across the unsecured consumer, small business lending, and mortgage lending segments.

The types of data being considered may differ significantly in their apparent relationship to traditional credit criteria. Some data are considered more proximate because they provide more meaningful information on the credit profile of borrowers (e.g., utility and rental payments), while

Figure 22: Types of Credit Data



Note: Represents select examples from comment letters to CFPB regarding use of alternative data and modeling technologies in credit process by Equifax, TransUnion, American Bankers Association, Consumer Bankers Association, FICO, Independent Community Bankers Association, and California Nevada Credit Union League.  
 Source: CFPB public comment file. See Robinson + Yu, *Knowing the Score: New Data, Underwriting, and Marketing in the Consumer Credit Marketplace* (Oct. 29, 2014), at 15.

387. See Mercator Advisory Group, *Press Release – FICO® Scores Used in over 90% of Lending Decisions According to New Study* (Feb. 27, 2018), available at: <http://paymentsjournal.com/fico-scores-used-90-lending-decisions-according-new-study/>.

other data sources' relationship to credit risk may be less apparent (e.g., technology usage patterns, social networking information and website tracking).

The types of credit models also vary meaningfully, for example, by the degree to which firms employ machine learning based algorithms. Some of the new credit models are largely based upon existing modeling approaches but with new forms of data that closely approximate other credit data, while other firms may employ both new modeling approaches (i.e., machine learning) and some of the newest forms of data (e.g., technology use patterns). These newer credit models could be used by firms on a proprietary basis to underwrite borrowers for their own businesses, or could also be used by firms to generate a credit score product that could be sold to other firms for their loan underwriting processes.

Nonbank financial firms, such as marketplace lenders, generally report greater use of less-traditional data sources and newer modeling approaches, including ones based upon machine learning. Such lenders may rely upon new data sources to support the underwriting of loans through authenticating borrowers' identity online, assessing borrower default risk, and reducing instances of fraud. The provision of such scoring information also allows such lenders to often extend credit to borrowers below traditional FICO score thresholds or with little FICO score information.<sup>388</sup> Various new credit scoring companies have also formed that are generally more active in leveraging these new data sources, though the degree to which some might employ machine-learning models can vary substantially.<sup>389</sup>

### **Issues and Recommendations**

These approaches have the potential to enable greater access to credit and improve the quality of financial products. However, the applications of these more novel approaches raise important policy considerations.

### **Opportunities to Expand and Improve Access to Credit**

There are potential opportunities to expand access to credit for borrowers: (1) consumers who have thin credit files or no credit files (up to 45 million U.S. adults)<sup>390</sup> with the consumer credit bureaus, and (2) small businesses, which are important engines of the economy and job creation. For example, a 2017 study found some evidence that the use of "alternative" credit data has allowed consumers with more limited traditional credit profiles (i.e., based on FICO scores) to access credit.<sup>391</sup> Additional information on credit card usage, such as whether consumers are carrying balances

388. See Letter from the Online Lenders Alliance to the Bureau of Consumer Financial Protection, *Response to Request for Information Regarding Use of Alternative Data Modeling Techniques in the Credit Process*; Records Docket No.: CFPB-2017-0005 (May 19, 2017), available at: <https://www.regulations.gov/document?D=CFPB-2017-0005-0071>.

389. Mikella Hurly and Julius Adebayo, *Credit Scoring in the Era of Big Data*, 18 Yale J. L. & Tech. 148 (2016) (table 1).

390. See Office of Research, Bureau of Consumer Financial Protection, *Data Point: Credit Invisibles* (May 2015), at 12, available at: [http://files.consumerfinance.gov/f/201505\\_cfpb\\_data-point-credit-invisibles.pdf](http://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf) ("Credit Invisibles Report").

391. Julapa Jagtiani and Catharine Lemieux, *Fintech Lending: Financial Inclusion, Risk Pricing, and Alternative Information*, Federal Reserve Bank of Philadelphia working paper (July 6, 2017), at 9-12, available at: <https://www.philadelphiafed.org/-/media/research-and-data/publications/working-papers/2017/wp17-17.pdf>.



month over month on their credit cards or paying in full, can also improve credit risk analysis. At the same time, some groups have raised the concern that expanding the use of certain data (e.g., rent, utility, telecom payments) for persons that already have a FICO score could result in reduced credit availability.<sup>392</sup> The use of alternative credit data can provide consumers an on-ramp into the financial services landscape. For example, FICO recently launched another credit score product designed to provide credit applicants a “second chance” score, to be used where the applicant has no traditional FICO score. The new score provides a means to assess consumers with thin credit reports who could not be scored without additional information. FICO found that using its “second chance” score, more than a third of such applicants had FICO scores above 620. Moreover, for applicants with scores above 620 and that access credit, more than two-thirds reported FICO scores of 660 or higher two years later.<sup>393</sup>

Several firms that are actively deploying these approaches in consumer and small business lending report significant improvements in loss rates, which suggests some improvements in modeling approaches. For example, firms anecdotally report: (1) double-digit improvements in approval rates and declines in loss rates from using machine learning techniques on existing available data sources for lenders (that is, their own data, but with improved analysis); and (2) that some of the nontraditional data sources provide predictive value that is comparable to the traditional credit-data, which can indicate either strong proxy relationships with traditional credit-data or other important information not available to existing credit data sets. It should be noted, however, that the timeframe of these favorable results is limited and does not reflect performance through a credit cycle.

The Bureau has also highlighted the potential benefits in these approaches to data and modeling. The Bureau launched a no-action letter program as part of its Project Catalyst, launched in November 2012, to facilitate consumer-friendly innovations. Specifically, the Bureau was looking to explore how “alternative data” and the use of emerging technologies like machine learning, could improve credit decisions.<sup>394</sup>

### Consumer Protections and Compliance

Firms looking to use alternative data and more advanced algorithms must navigate compliance with several areas of consumer protection law, including: (1) the Fair Credit Reporting Act (FCRA) of 1970, which is designed to make sure that credit reporting agencies that sell data for certain decision-making purposes maintain accurate data, provide consumers access to and the ability to correct their data, and that such data is used only for permissible activities; (2) fair lending laws, including the Equal Credit Opportunity Act and the Fair Housing Act, which are

---

392. Letter from National Consumer Law Center et al., *Comments in Response to Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process*, Docket No. CFPB-2017-0005 (May 19, 2017), at 3-4, available at: <https://www.regulations.gov/document?D=CFPB-2017-0005-0097>.

393. Letter from Fair Isaac Corporation, *Request for Information Regarding the Use of Alternative Data and Modeling Techniques in the Credit Process – Docket No. CFPB-2017-0005* (May 19, 2017), at 9, available at: <https://www.regulations.gov/document?D=CFPB-2017-0005-0080>.

394. Bureau of Consumer Financial Protection, CFPB Announces First No-Action Letter to Upstart Network (Sept. 14, 2017), available at: <https://www.consumerfinance.gov/about-us/newsroom/cfpb-announces-first-no-action-letter-upstart-network/>.

designed to prohibit discrimination on the basis of various protected categories; (3) the Federal Trade Commission (FTC) Act, which prohibits unfair or deceptive acts or practices (UDAP) in or affecting commerce; and (4) the Bureau's authority with respect to unfair, deceptive or abusive acts and practices (UDAAP).

The FCRA requires that consumers be provided adverse action notices if they are denied credit or charged more as the result of their consumer report information. This requirement, among other factors, may represent challenges for market participants that are seeking to innovate by incorporating additional data sources into the credit underwriting process.

New models and data may also unintentionally run the risk of producing results that arguably risk violating fair-lending laws if they result in a “disparate impact” on a protected class<sup>395</sup> or because the FTC or the Bureau might find the use of such models and data to be a violation of UDAP or UDAAP, respectively.

### Model Validation and Reliability

Existing regulatory guidance on credit models<sup>396</sup> may need to be tailored to incorporate issues raised by alternative data or machine learning based models. As an example, applying traditionally accepted practices of model validation and back-testing may be challenging when models are constantly “learning” and producing potentially new results on a continual basis.

The data available today significantly exceeds the data available during past credit cycles. Machine learning based models that require significant amounts of data would generally suffer from the absence of past credit-cycle data to “train” the model.

### Data Quality and Privacy

Alternative data sources may not be as reliable as traditional sources. Banks active in consumer lending, for example, report that vendors of “alternative data” may not always know the source of their own data, which would present material compliance risks if such data were to be used for

395. Carol Evans, Board of Governors of the Federal Reserve System, *Keeping Fintech Fair: Thinking about Fair Lending and UDAP Risks*, Consumer Compliance Outlook (2017), available at: <https://consumercomplianceoutlook.org/assets/2017/second-issue/ccoi22017.pdf?la=en>.

396. See Board of Governors of the Federal Reserve System, Guidance on Model Risk Management, SR Letter 11-7 (Apr. 4, 2011), available at: <https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm>; Office of the Comptroller of the Currency, Credit Scoring Models, OCC Bulletin 1997-24 (May 20, 1997), available at: <https://www.occ.treas.gov/news-issuances/bulletins/1997/bulletin-1997-24.html>; Office of the Comptroller of the Currency, Sound Practices for Model Risk Management, OCC Bulletin 2011-12 (Apr. 4, 2011), available at: <https://www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-12.html>; Federal Deposit Insurance Corporation, Supervisory Insights – Model Governance (last updated Dec. 5, 2005, available at: [https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin05/article01\\_model\\_governance.html](https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin05/article01_model_governance.html); Federal Deposit Insurance Corporation, Supervisory Insights – Fair Lending Implications of Credit Scoring Systems (last updated Apr. 11, 2013), available at: [https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum05/article03\\_fair\\_lending.html](https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum05/article03_fair_lending.html).

eligibility and credit decisions.<sup>397</sup> The prevalence of errors from such data is not currently known, though even traditional credit bureau information may have meaningful rates of errors.<sup>398</sup>

### *Recommendations*

Treasury recognizes that these new credit models and data sources have the potential to meaningfully expand access to credit and the quality of financial services. Treasury therefore recommends that federal and state financial regulators further enable the testing of these newer credit models and data sources by both banks and nonbank financial companies.

Regulators, through interagency coordination wherever possible, should tailor regulation and guidance to enable the increased use of these models and data sources by reducing uncertainties. In particular, regulators should provide regulatory clarity for the use of new data and modeling approaches that are generally recognized as providing predictive value consistent with applicable law for use in credit decisions.

Regulators should in general be willing to recognize and value innovation in credit modelling approaches. Such approaches can create more robust risk management environments and improve both the cost and access to credit. Regulators should enable prudent experimentation with the aim of working through various issues raised, which may in turn require new approaches to supervision and oversight.

Given that consumers without credit scores tend to make regular monthly payments to telecom, utility, or rental companies and may benefit from the reporting of these fields, Treasury supports continued industry efforts to capture this type of additional consumer credit data through regular reporting to the consumer credit bureaus. Similarly, Treasury supports efforts to report monthly credit card payment amounts to the consumer credit bureaus to provide an additional level of granularity into consumer credit utilization.

## **Credit Bureaus**

### **Overview**

The consumer credit bureaus are essential to the functioning of consumer credit markets in the United States. Credit bureaus have not only become a vital resource for financial market participants such as lenders and servicers, but are also increasingly relied upon by property management companies and employers. Credit bureaus collect, store, and analyze consumer financial data including repayment history, outstanding debt, and other factors to produce a profile of a consumer's credit history. Today, about 189 million American consumers have credit reports with

---

397. Letter from Consumer Bankers Association, *Response of the Consumer Bankers Association to the Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process* (Docket No. CFPB-2017-0005) (May 19, 2017), at 9, available at: <https://www.regulations.gov/document?D=CFPB-2017-0005-0073>.

398. See, e.g., Bureau of Consumer Financial Protection, *Supervisory Highlights Consumer Reporting Special Edition* (Winter 2017), available at: [https://files.consumerfinance.gov/f/documents/201703\\_cfpb\\_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf](https://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf).

sufficient information for the calculation of a credit score.<sup>399</sup> Credit bureaus also maintain files on another 19 million Americans who are considered “unscorable” due to insufficient information.<sup>400</sup> In total, nearly 210 million Americans rely on the three major consumer credit bureaus to accurately reflect their credit histories so that this history can be used by credit scorers and financial institutions to model credit risk, determine eligibility for credit, and establish the price of that credit. These entities collect significant amounts of personal and financial data about consumers, and, as a result, have a statutory requirement to protect consumer information in their possession.

### Regulatory Treatment

Credit bureaus are subject to federal and state regulation for consumer protection purposes. At the federal level, credit bureaus are subject to the FCRA, which governs how credit bureaus collect information regarding consumers, use the information, and share the information with third parties.<sup>401</sup> In 2012, the Bureau, using its “larger participants” authority, began supervising the largest credit bureaus for compliance with federal consumer financial protection laws.<sup>402</sup> Prior to 2012, credit bureaus were not routinely supervised at the federal level.

Credit bureaus must safeguard personal financial information and are subject to statutory data security standards. The FTC has actively used its authority to enforce data security provisions under Section 5 of the FTC Act<sup>403</sup> and pursuant to the FTC’s “Safeguards Rule,”<sup>404</sup> which the FTC implemented under authority granted to it by section 501(b) of the Gramm-Leach-Bliley Act (GLBA).<sup>405</sup> While GLBA granted FTC rulemaking and enforcement authority regarding the security and confidentiality of customer information, GLBA did not grant FTC authority to conduct supervision of credit bureaus for compliance with GLBA data security standards and privacy requirements. A similar limitation exists with respect to the Bureau. Dodd-Frank granted the Bureau supervisory authority with respect to certain requirements of GLBA, including provisions regarding consumer privacy,<sup>406</sup> but did not grant authority with respect to section 501 of GLBA,

399. Credit Invisibles Report.

400. *Id.*

401. The FTC website provides a summary of consumer rights under the FCRA, available at <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

402. In its final rule [12 C.F.R. part 1090], the Bureau defined the consumer reporting market to include companies that collect, analyze, maintain, or provide consumer report or other account information used in a decision by another person for offering of any consumer financial product or service. At the time, the Bureau’s larger participants rulemaking for credit reporting covered nearly 30 companies accounting for 94% of annual receipts in the market. See *Defining Larger Participants in Certain Consumer Financial Product and Service Markets* (Feb. 8, 2012) [77 Fed. Reg. 9592 (Feb. 17, 2012)].

403. 15 U.S.C. § 45(a); see also Federal Trade Commission, *Enforcing Privacy Promises*, available at <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises> (last accessed June 27, 2018) (listing press releases for FTC enforcement actions relating to privacy).

404. 16 C.F.R. Part 314; see also *Standards for Safeguarding Customer Information* (May 22, 2002) [67 Fed. Reg. 36484 (May 23, 2002)].

405. In addition to enforcement actions to stop practices that are harmful to consumers, the FTC engages with industry participants through reports and educational tools and also conducts policy and legislative work.

406. See Bureau of Consumer Financial Protection, *Privacy of Consumer Financial Information - Gramm-Leach-Bliley Act (GLBA) Examination Procedures* (Oct. 2016), at 1, available at: [https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/102016\\_cfbp\\_GLBAExamManualUpdate.pdf](https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/102016_cfbp_GLBAExamManualUpdate.pdf).

which requires regulators to establish standards for the protection of nonpublic personal information.<sup>407</sup> As a result, neither the FTC nor the Bureau supervises credit bureaus for compliance with these GLBA section 501 data security requirements.

## **Issues and Recommendations**

### **Data Security – Supervision and Enforcement**

In July 2017, Equifax noticed suspicious activity on the portal they provide consumers for dispute resolution and engaged a cybersecurity firm to investigate the suspicious activity.<sup>408</sup> The firm found that consumers' personal information was disclosed to unauthorized parties from May 13 to July 30, 2017.<sup>409</sup> In total, almost 150 million consumers' names, social security numbers, dates of birth, addresses, gender, phone numbers, driver's license numbers, and email addresses were breached.<sup>410</sup> Hundreds of thousands of consumers' credit or debit card information and documents provided to Equifax by 182,000 customers related to dispute resolutions were breached.<sup>411</sup> This incident has highlighted the need for greater supervision of the consumer credit bureaus, especially relating to the protection of nonpublic personal information.

The FTC has deep expertise on privacy and data security for nonbank financial companies. The FTC exercises enforcement authority under GLBA with respect to some types of nonbank financial companies, including credit bureaus.<sup>412</sup> However, as noted earlier, credit bureaus are not subject to routine supervision by either the FTC or the Bureau with respect to the requirements implemented under section 501 of the GLBA for the protection of nonpublic personal information. Given the sensitive nature of the information credit bureaus collect, the bureaus have a heightened duty to protect the information they collect.

### *Recommendations*

The FTC should retain its rulemaking and enforcement authority for nonbank financial companies under the GLBA. Additionally, Treasury recommends that the relevant agencies use appropriate authorities to coordinate regulatory actions to protect consumer data held by credit reporting agencies and that Congress continue to assess whether further authority is needed in this area.

### **Credit Education and Counseling**

In 1996, Congress passed the Credit Repair Organizations Act (CROA) to help protect consumers against unfair or deceptive advertising and business practices by credit repair organizations. In

---

407. Dodd-Frank § 1002(12)(J).

408. Equifax Inc., *Press Release – Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes* (Sept. 15, 2017), available at: <https://www.equifaxsecurity2017.com/2017/09/15/equifax-releases-details-cybersecurity-incident-announces-personnel-changes/>.

409. *Id.*

410. Equifax Inc., *Form 8-K Current Report* (May 4, 2018), available at: <https://otp.tools.investis.com/clients/us/equifax/SEC/sec-show.aspx?Type=html&FilingId=12735591&CIK=0000033185&Index=10000>.

411. *Id.*

412. In recent years, the Bureau has also undertaken enforcement actions in the area of data security, pursuant to its unfair, deceptive or abusive acts or practices (UDAAP) authority. At present, detailed guidance for compliance with UDAAP, akin to the FTC's Safeguards Rule, is not available.

CROA's passage, Congress found that credit repair companies were creating economic hardships for some consumers who had engaged their services and that consumers should be provided with information to help make an informed decision about the purchase of credit repair services. CROA defines a credit repair organization as "any person who uses any instrumentality of interstate commerce or the mails to sell, provide, or perform (or represent that such person can or will sell, provide, or perform) any service, in return for the payment of money or other valuable consideration, for the express or implied purpose of (i) improving any consumer's credit record, credit history, or credit rating; or (ii) providing advice or assistance to any consumer with regard to any activity or service described in clause (i)," with certain exceptions.<sup>413</sup> Under CROA, any entity deemed to be a credit repair organization is subject to requirements regarding how it may engage with a consumer and actions it must take before accepting payment for services. The FTC and private plaintiffs may bring actions for violations of CROA under a strict liability theory.

Credit repair organizations claim to help consumers improve their credit report and credit score, often by indicating they can assist in removing negative, unfair, or inaccurate credit information from consumer credit reports, with some companies falsely claiming that their years of expertise or relationship with the consumer credit bureaus will result in a more favorable outcome than if the consumer pursued removing inaccurate information on their own. Generally, these credit repair services are offered at a significant cost to the consumer. It is important to note that under existing law, consumers can receive a free credit report from each of the three national credit bureaus on an annual basis and can work directly with each of the credit bureaus to dispute any inaccurate information found in their credit report. Regardless of whether a consumer engages with the credit bureau or a credit repair company, accurate, negative credit information cannot be removed from the consumer's credit report.

Recently, credit bureaus, including the three largest bureaus, have expanded their offerings of credit and financial education services directly to consumers. These services generally do not involve specific action taken by the credit bureau to repair or change a credit report or score, but instead provide advice and education on how to address behavior or issues that influence consumers' credit profiles.

In *Stout v. Freescore, LLC*, the U.S. Court of Appeals for the Ninth Circuit held that Freescore, an online provider of credit scores, reports, and consumer credit information, was a "credit repair organization" under CROA.<sup>414</sup> The court reasoned that, in order to fall within the definition of "credit repair organization" under CROA, a person need not actually provide a service aimed at improving a consumer's credit record, history, or rating, as long as it represents that it can or will provide such a service. Consequently, since Freescore "affirmatively represents that its services can or will improve, or help to improve, a consumer's credit record, history, or rating," the court held that it fell within CROA's definition of a credit repair organization.<sup>415</sup> The decision in *Stout v. Freescore* troubled credit bureaus and credit scorers offering credit counseling services because those services aim to help consumers prospectively improve their credit scores, potentially exposing these firms to legal liability under CROA. The court's interpretation of CROA's scope creates a risk

413. 15 U.S.C. § 1679a.

414. *Stout v. Freescore, L.L.C.*, 743 F.3d 680, 681-85 (9th Cir. 2014).

415. *Id.* at 685-86.



that these companies, which have valuable insight to provide consumers, will limit their credit counseling offerings.

While the credit bureaus and credit scoring companies can and do offer limited consumer credit counseling services, CROA inhibits innovation by unduly restricting legitimate product offerings. For example, CROA requires a three-day waiting period from the time a consumer signs up for credit counseling services with a credit repair organization to the time the consumer receives the service, and prohibits credit repair organizations from collecting payment for the performance of any service until the entirety of that service is completed. Further, CROA includes strict liability and private right of action provisions that have discouraged legitimate entities like consumer credit bureaus and credit scorers from providing greater credit counseling offerings due to concerns about potential liability under CROA.

Innovation and modernization of credit education and counseling are important developments to ensure consumers become sophisticated and responsible borrowers. While the proper application of CROA provides valuable consumer protections, CROA's expansive definition of "credit repair organization" has unnecessarily restricted entities with significant expertise in consumer credit (such as credit bureaus and credit scorers) from offering consumer credit education and counseling products.

### *Recommendations*

Treasury recommends that Congress amend CROA to exclude the national credit bureaus and national credit scorers (i.e., credit scoring companies utilized by financial institutions when making credit decisions) from the definition of "credit repair organization" in CROA.

### **InsurTech**

As the broader financial services sector invests heavily in technology, digitally enabled advances across the insurance industry have come to be known as "InsurTech." InsurTech is a broad term used to describe new technologies with the potential to bring innovation to the insurance sector and these advances may impact regulatory practices for insurance markets.<sup>416</sup> Industry stakeholders — including existing or "traditional" insurers, startups, intermediaries, regulators, and consumers — are all exploring how technological advancements can be leveraged to increase efficiency, offer better-tailored products to consumers, increase consumer choice, and provide more effective and efficient regulation. Technological innovation reportedly has now overtaken insurance regulation as the issue about which property and casualty insurer senior executives are most concerned.<sup>417</sup>

416. Organization for Economic Co-operation Development, *Technology and Innovation in the Insurance Sector* (2017), available at: <https://www.oecd.org/finance/Technology-and-innovation-in-the-insurance-sector.pdf>. Treasury, through the Federal Insurance Office, highlighted a number of examples where InsurTech is changing the business of insurance in its 2017 Annual Report, available at: [https://www.treasury.gov/initiatives/fio/reports-and-notice/2017\\_FIO\\_Annual\\_Report.pdf](https://www.treasury.gov/initiatives/fio/reports-and-notice/2017_FIO_Annual_Report.pdf).

417. See, e.g., KPMG, *A New World of Opportunity: The Insurance Innovation Imperative* (Oct. 2015), at 7, available at: <https://assets.kpmg.com/content/dam/kpmg/pdf/2016/01/the-insurance-innovation-imperative.pdf>.

Recent InsurTech developments have affected a wide variety of operations, from back-office operations — including data collection techniques and pricing algorithms — to digital platforms, claims-handling processes, and product offerings. Technological tools now used by insurance stakeholders include the Internet of Things, telematics, big data, robo-advisors, machine learning/artificial intelligence (AI), and blockchain. Business models and product offerings have also evolved to include peer-to-peer (P2P), usage-based, and on-demand insurance.

InsurTech startup funding is substantial, with \$2.3 billion invested in 2017 alone.<sup>418</sup> Traditional insurers have helped drive this growth by investing in InsurTech startups, and many have established business units devoted exclusively to strategic investment in InsurTech ventures, the exploration of their own InsurTech initiatives, and/or partnerships with InsurTech “hubs” that bring together entrepreneurs, investors, and industry experts.<sup>419</sup> Entrepreneurs and investors from outside of the insurance industry have also taken note of the potential to use InsurTech to make the insurance supply-chain more efficient. InsurTech thus continues to attract considerable interest for both its potential to complement existing processes and its potential to disrupt.

Stakeholders have also observed that the United States’ regulatory environment could limit innovation in the U.S. insurance sector, which could inhibit economic growth. Factors that potentially could restrict insurance innovation include: (1) high regulatory barriers to entry; (2) little flexibility for regulators to accommodate new products or technologies; (3) inconsistent laws and regulations (or the possibility of inconsistent application of laws and regulations) across the 50 states; and (4) lengthy product approval processes. As a result, in some cases, insurers and startups prefer the regulatory practices of foreign jurisdictions, such as the United Kingdom or Singapore, over the United States when testing or introducing a new product or practice.

In response to InsurTech developments, insurance regulators are examining technological innovation and its potential regulatory impact. In the United States, state insurance regulators and the National Association of Insurance Commissioners (NAIC) have taken preliminary steps to better understand emerging technologies and their regulation.<sup>420</sup> The NAIC, for example, has formed an Innovation and Technology Task Force, which will, among other things, “[p]rovide a forum for the discussion of innovation and technology developments in the insurance sector, including the collection and use of data by insurers and state insurance regulators — as well as new products, services and distribution platforms — in order to educate

418. See, e.g., Deloitte, *Fintech by the Numbers: Incumbents, Startups, Investors Adapt to Maturing Ecosystem* (2017), available at: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-dcfs-fintech-by-the-numbers-web.pdf>; Willis Towers Watson, *Quarterly InsurTech Briefing Q4 2017* (Jan. 2018), available at: <https://www.willistowerswatson.com/-/media/WTW/PDF/Insights/2018/01/quarterly-insurtech-briefing-q4-2017.pdf>.

419. See, e.g., Oliver Suess, *InsurTech Startups Attract Growing List of Traditional Insurer Partners*, *Ins. J.* (Nov. 28, 2016), available at: <https://www.insurancejournal.com/news/international/2016/11/28/433226.htm>; Sam Boyer, *Traditional Insurance City Set to Become Disrupting Insurance City*, *Insurance Business America* (Dec. 13, 2017), available at: <https://www.insurancebusinessmag.com/us/news/technology/traditional-insurance-city-set-to-become-disrupting-insurance-city-87629.aspx>.

420. State regulation of the insurance industry is coordinated through the NAIC, a voluntary organization whose membership consists of the chief insurance regulatory officials of the 50 states, the District of Columbia, and the five U.S. territories.



state insurance regulators on how these developments impact consumer protection, privacy, insurer and producer oversight, marketplace dynamics and the state-based insurance regulatory framework.”<sup>421</sup> The International Association of Insurance Supervisors (IAIS)<sup>422</sup> has also taken an interest in innovation and recently published a report titled “Fintech Developments in the Insurance Industry.”<sup>423</sup>

Lawmakers, policymakers, and regulators should also take coordinated steps to encourage the development of innovative insurance products and practices in the United States. Domestically, this includes consideration of improving product speed to market, creating increased regulatory flexibility, and harmonizing inconsistent laws and regulations. Treasury’s Federal Insurance Office, which provides insurance expertise in the federal government, should work closely with state insurance regulators, the NAIC, and federal agencies on InsurTech issues.

## Payments

### Overview of the U.S. Payments System

The United States is the leader in facilitating consumer and business payment transactions. In 2016, interbank payments systems in the United States handled over \$1 quadrillion in transaction value, with payment systems involving nonbanks handling nearly \$190 trillion of that transaction value.<sup>424</sup> Payments are essential to commerce and the payments infrastructure that has been built over decades empowers consumer choice in payments. This system has proven, over time, to be stable, secure, and effective.

In the United States, four primary core payment systems transfer value between financial institutions: credit card networks, debit card networks, automated clearing house (ACH) transfers, and wire transfer services. In addition to these core components, nonbank payment processors, payment service providers, money transmitters, and others help drive payment speed, security, efficiency and global penetration for businesses and consumers alike.

Recently, new technologies, especially in commerce, have changed the way that people live, consume, and pay for goods and services. New technological abilities have led to higher consumer expectations as to the speed and convenience of systems such as payments. Financial systems have

421. See [http://www.naic.org/cmtc\\_ex\\_itff.htm](http://www.naic.org/cmtc_ex_itff.htm).

422. Established in 1994, the IAIS is the international standard-setting body responsible for developing and assisting in the implementation of principles, standards, and other supporting material for the supervision of the insurance sector. The IAIS’s objectives are as follows: to promote effective and globally consistent supervision of the insurance industry; to develop and maintain fair, safe, and stable insurance markets; and to contribute to global financial stability. IAIS members include insurance supervisors and regulators from more than 200 jurisdictions in approximately 140 countries.

423. International Association of Insurance Supervisors, *FinTech Developments in the Insurance Industry* (Feb. 21, 2017), available at: <https://www.iaisweb.org/file/65440/report-on-fintech-developments-in-the-insurance-industry>.

424. Bank for International Settlements Committee on Payments and Market Infrastructures, *Statistics on Payment, Clearing and Settlement Systems in the CPMI Countries* (Dec. 2017), at 406 and 408, available at: <https://www.bis.org/cpmi/publ/d172.pdf>.

and will continue to evolve to meet market demand, and payments is an area where innovation and disruption by nonbank and technology firms has been increasingly visible. Over the past few years, many firms have either launched a payments solution, or have publicly expressed interest in entering the payments ecosystem. Firms see a need and a demand for services that are faster, more convenient, and more integrated. As such, the breadth of available options coupled with the competition in payments has led to increased functionality, innovative solutions, and newer ways to ease transactions in order to promote economic activity and growth.

However, barriers to entry and innovation do exist in payments. First, a business case must be made before a firm even begins to build and implement a payment solution — scale of consumer adoption, ubiquity of acceptance, and security of the mechanism, among other challenges — must be taken into account for any new and innovative payment scheme to be successful.

Second, the payments system in the United States is operationally complex — while the payments landscape continues to undergo rapid innovation, there has been very little relative change to the back-end processes that actually move value throughout the financial system. Innovation in payments has largely been happening on the front-end, consumer-facing side of a transaction. The user experience, products, and innovative solutions that have been introduced in recent years with the advent of mobile technology, in essence, layer on top of the existing core payment systems.

Third, regulation of payments is fragmented; further, the core payment systems exist to move money between financial institutions and their customer accounts and as such, only regulated financial institutions have direct access to the infrastructure. To ensure the security of the payments system, those firms that directly connect to it must be safe and sound institutions that are adequately supervised; financial institutions as direct participants, therefore, are subject to prudential bank regulation and supervision. Firms that layer on top of this bank-centric system and provide consumer-facing solutions are regulated in a variety of ways, and governance of payments is as fragmented as the payment systems themselves. Payments firms are generally overseen through the banking agencies' third-party oversight guidance, through state money transmitter statutes, and/or by private payment network association operating rules and contracts. This fragmented approach to payments governance has perhaps in some ways entrenched legacy systems and slowed down innovations in areas like faster payments, but on the other hand, such a system has allowed for innovations over a wide range of niches that allow for multiple solutions to emerge and be tested by a wider audience. This can ensure innovation with fewer risks to payment safety.

Innovation has progressed through solutions built on top of the legacy payments infrastructure. There are benefits and challenges in employing such an approach; while the infrastructure, legal, and regulatory hurdles are very complex, this method has also allowed for more expediency than a built-from-scratch system and has allowed private firms to innovate on their own without extensive government mandates. See *Appendix C* for additional background on the U.S. payments systems.

### **Money Transmitters**

Money transmitters are generally nonbank firms that transfer funds or value between individuals. These firms are important because they allow for payments to be made through a variety of channels and can be offered by various nonbank firms. In most cases, a nonbank that is moving

monetary value, whether it be by remittance (domestic or international), stored value/prepaid cards, check cashing, or person-to-person payments, will be licensed as a money transmitter.

### Licensing and Supervision

Money transmitter licensing is governed primarily by state law. Differences in state statutes mean that there is no unified definition of a money transmitter; as a result, states have different variations that could bring in a number of firms that do not necessarily engage in the traditional form of funds transfer. If a firm engages in money transmission, or even if it may potentially fall under the definition of a money transmitter in a certain state, then it must apply for a money transmitter license in that state, in many cases without even having a physical presence in the state. The effect is that for any firm with a nationwide footprint, a license in every state is necessary. Licensing requirements vary by state, but generally include requirements to submit credit reports, business plans, and financial statements; and a requirement to maintain a surety bond to cover losses that might occur. States have engaged in several efforts to streamline the licensing process, but overall adoption of these initiatives has been mixed. (Further discussion of state licensing of money transmitters is addressed in the previous chapter on Aligning the Regulatory Framework to Promote Innovation.)

Money transmitters are considered money services businesses (MSBs) and are therefore subject to the requirements of the Bank Secrecy Act. They must register at the federal level with FinCEN. Banks, foreign banks, or firms that are registered with the U.S. Securities and Exchange Commission (SEC) or U.S. Commodity Futures Trading Commission (CFTC) are not considered MSBs and do not have to register as such.

Money transmitters are supervised and examined by each state where they hold a license. For money transmitters with nationwide state licenses, this means duplicative examinations by a number of different state regulators, and has emerged as a common theme for reform among firms. The most recent data available from state regulators shows that over half of all consolidated money transmitter firms operate and have licenses in multiple states.<sup>425</sup>

State regulators note that while states have different frequency of exams, most money transmitters are examined annually, either by individual states and/or through joint exams organized among several states. States examine for safety and soundness as well as compliance with both state law and BSA/AML requirements.<sup>426</sup> Firms have raised concerns regarding the frequency and quantity of examinations and the sometimes-differing standards and idiosyncratic requirements from state to state.

### Regulation E Remittance Rule Disclosures

For money transmitters that provide international remittances, a particular regulatory inefficiency has emerged after financial reform. Section 1073 of Dodd-Frank requires disclosures to be provided

425. Conference of State Bank Supervisors and Money Transmitters Regulators Association, *The State of State Money Service Businesses Regulation and Supervision* (May 2010), at 6, available at: <https://www.csbs.org/state-state-money-service-businesses-regulation-and-supervision>.

426. *Id.* at 9-10.

to senders of remittance transfers.<sup>427</sup> The Bureau implemented section 1073 through amendments to Regulation E to require that:

- Companies give disclosures to consumers before the consumers pay for the transfer. These disclosures must include: the exchange rate, fees and taxes collected, fees charged by agents and intermediaries, the amount of money delivered not including fees and taxes charged to the recipient, and a disclaimer that other fees may apply.
- Companies also provide a post-transaction receipt that repeats all the information from the first disclosure, plus dates of payment availability, and error resolution and cancellation rights notices.
- Companies generally give customers 30 minutes to cancel a transfer in exchange for a full refund.<sup>428</sup>

The rule applies to any electronic transfer of funds from a U.S.-based customer to a person in a foreign country; this includes both money transmitters and banking organizations and applies even if done through a wire transfer or ACH. There is, however, a de minimis exemption for transfers of \$15 or less and companies that performed 100 or fewer remittance transfers in the current and previous calendar year.<sup>429</sup> Firms have noted concerns with the lack of flexibility in the disclosure rules. For example, electronic disclosures, like an email or mobile disclosure, may only be given if the transaction is done electronically. For in-person transactions, paper receipts must be provided.

#### *Recommendations*

Treasury supports the Bureau's ongoing efforts to reassess Regulation E. Treasury recommends that the Bureau provide more flexibility regarding the issuance of Regulation E disclosures and raise the current 100 transfer per annum threshold for applicability of the de minimis exemption.

### **Fintech and Payments**

Technology has advanced the payments market, increased competition, and increased innovation as new payment services have been introduced and further layered upon the existing payments system. Many new firms and technologies are now competing for a greater share of consumer transactions and the corresponding data. Thus far, few dominant players have yet emerged, and fintech payments solutions have largely remained confined to niche uses within the market.

### **Person-to-Person (P2P) Payments**

P2P payments that move money directly between bank accounts have been relatively slow to develop in the United States, in large part due to challenges within the existing payments infrastructure. Two core payment systems used to transfer funds between bank accounts — wire transfers and ACH — each have challenges for P2P. For example, wire transfers are far more expensive than ACH. On the other hand, ACH does not transfer in real time like wire transfers. Both methods require that the receiver provide the sender with their bank account information — routing and account numbers

427. 12 U.S.C. § 5601.

428. 12 C.F.R. §§ 1005.30-1005.36.

429. *Id.* § 1005.30.

— which may be cumbersome to find and may raise security concerns. More recently, technology and innovation have provided a way for a competitive market for P2P payments to emerge.

Like many other innovations in the payments system, these new P2P technologies layer on top of the existing payment systems. These new products are filling a demand for better account-to-account transfer mechanisms and consumer experience, and are beginning to build scale. According to a consumer payments survey, P2P payments are gaining ground, but mostly among young consumers. The survey found that the breakdown of P2P payment adopters fell largely along lines of age demographics, as people under the age of 35 were far more likely to already use or be ready to adopt P2P payment platforms than consumers over the age of 55.<sup>430</sup> However, there is room for growth, as only 29% of those surveyed have completed a P2P payment, with slightly less than half of the under-35 demographic having already used such a service. Among respondents who had not used a P2P payment service in 2017, more than half of those between 18 and 55 said that they were likely or somewhat likely to use such a service in the future. Security concerns are more likely to hold back older users from using P2P payments than other types of concerns.<sup>431</sup>

Innovative solutions to these problems have begun to emerge in the market and additional innovation in this space is to be expected. While multiple options exist in the market, two well-known examples are discussed.

### Bank Account-to-Bank Account Transfers

A consortium of some of the largest U.S. banks<sup>432</sup> has been working on a mechanism to transfer funds quickly and directly between bank accounts. The system works by leveraging the debit card infrastructure to move money, and generally functions through the online and mobile banking portals of each member bank. Previously, account-to-account transfers have needed to use either the wire transfer or ACH networks to complete the transaction. But now, the new transactions are cleared and posted in near real time and settlement occurs bilaterally between the applicable banks at the end of the day via ACH; in essence, the new network serves as a special standardized messaging system between banks for specific account-to-account transfers.

### Nonbank P2P Transfers

A number of MSBs have also emerged in the P2P space. These nonbank firms usually have obtained money transmitter licenses in every state, and only allow users to transfer money to other users of the same service. These sorts of services work by first using the balance that is held in a user's account; if the account does not have enough funds, an ACH transfer from a bank account or funding with a debit card or a credit card, can be used as a funding option.<sup>433</sup>

430. Total System Services, Inc., *2017 TSYS U.S. Consumer Payment Study* (Mar. 27, 2017), at 13-14, available at: [https://www.tsys.com/Assets/TSYS/downloads/rs\\_2017-us-consumer-payment-study.pdf](https://www.tsys.com/Assets/TSYS/downloads/rs_2017-us-consumer-payment-study.pdf) ("TSYS Payment Study").

431. *Id.*

432. Bank of America, BB&T, Capital One, JPMorgan Chase, PNC Bank, U.S. Bank, and Wells Fargo Bank. See Early Warning Services, LLC, *Early Warning Corporate Overview* (2017), available at: <https://www.earlywarning.com/pdf/early-warning-corporate-overview.pdf>.

433. See, e.g., PayPal, Inc., *Venmo User Agreement* (last updated Dec. 18, 2017), available at: <https://venmo.com/legal/us-user-agreement>.

### Digital Wallets

Digital and mobile wallets have increased in popularity and have continued to evolve within the last few years. Researchers at the Federal Reserve Bank of Boston have categorized mobile wallets into four distinct models: (1) near field communication (NFC) wallets; (2) cloud-based, card-on-file wallets; (3) cloud-based, card-on-file card network wallets; and (4) merchant or financial institution QR code-based wallets.<sup>434</sup> Each of these methods uses tokenization to secure payment information.

- NFC wallets are contactless payment mechanisms. Payments are made when a smart-phone is held near a payment terminal, and authentication takes place (fingerprint or PIN number) before the information is sent from the phone to the terminal. NFC wallets have a number of common features, although the hardware and software vary. NFC wallets can only accept eligible and wallet-accepted credit and debit cards, are available for use where a retailer has an NFC-enabled payment terminal, and can only be used with the corresponding smartphone operating system.<sup>435</sup>
- Cloud-based, card-on-file wallets are primarily used for online e-commerce payments. These services allow a consumer to utilize multiple funding methods — credit/debit/pre-paid cards, ACH, and so on — for input into the mobile wallet. The consumer may then check out at various merchants online using the funding method of their choice within the wallet. Generally, any payment card may be input – there is not a need for the issuing bank to provide for eligibility. Merchants utilize APIs to enable payment using these services.<sup>436</sup>
- Cloud based, card-on-file card network wallets function similar to the card-on-file systems previously noted, removing the need for merchants to store and collect payment data. The card networks work with merchants to allow for the digital wallets to be enabled on their own website or mobile app.<sup>437</sup>
- QR code-based wallets use QR codes as a way to complete payment, with payment information that is stored in the app. These services, however, can only be used in their own environments. For bank-based wallets, a QR code provided by the app must be scanned by the cashier, and can only be used in conjunction with the financial institution's products. A store-based payment app requires the consumer to scan the QR code provided by the store's payment terminal to complete the payment.<sup>438</sup>

Like P2P payments, digital wallets are also seeing increased adoption among younger consumers, albeit very gradually. Age is a significant factor in the likelihood that a particular consumer has loaded or plans to load card information into a digital wallet. As for funding choice, consumers are

434. Susan M. Pandey and Marianne Crowe, Federal Reserve Bank of Boston, *Adapting to Mobile Wallets: The Consumer Experience* (revised June 16, 2017), available at: <https://www.bostonfed.org/publications/payment-strategies/choosing-a-mobile-wallet-the-consumer-perspective.aspx>.

435. *Id.* at 5.

436. *Id.* at 13.

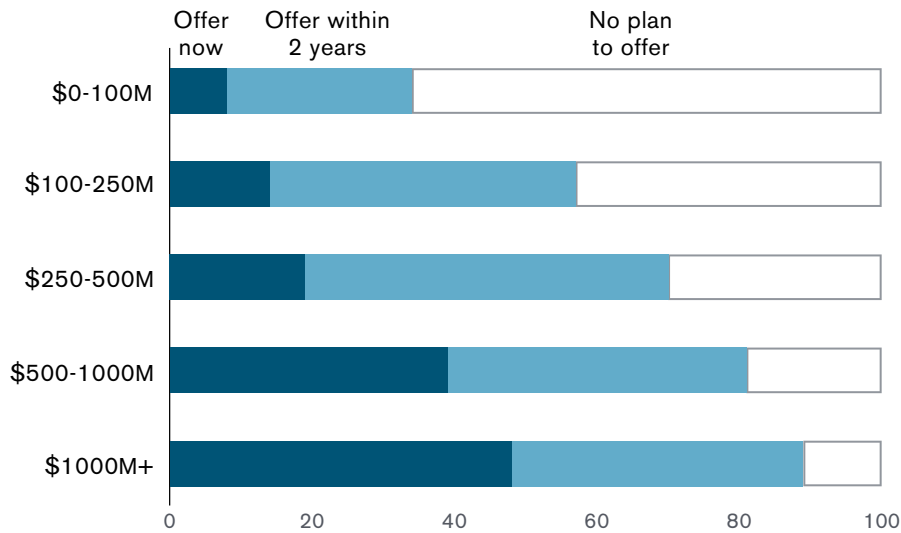
437. *Id.* at 16.

438. *Id.* at 18-20.

more likely to load a credit card into a digital wallet than a debit card, and far more likely to use a credit card to make an online payment.<sup>439</sup>

For mobile wallet usage (especially NFC wallets) to increase, the cards that are issued by banks must be eligible for enrollment. In 2017, the Federal Reserve Bank of Boston released a survey that asked banks from across the United States about their plans for mobile payments, among other things. The survey found that a relatively small percentage of banks offered mobile wallet services, and those that did were predominantly larger banks.

Figure 23: U.S. Financial Institutions Mobile Payment Services Plan (percent of respondents by asset size)



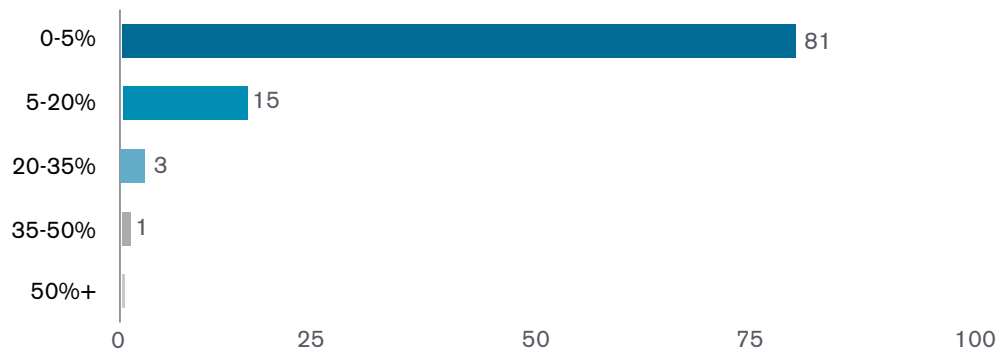
Source: Marianne Crowe et al., *Mobile Banking and Payment Practices of U.S. Financial Institutions 2016 Mobile Financial Services Survey Results from FIs in Seven Federal Reserve Districts*, Federal Reserve Bank of Boston (Dec. 2017), at 50.

439. TSYS Payment Study, at 13-14.



Also, as shown in **Figure 24** below, the survey found that at banks that offer mobile payment services and track customer usage data, a small percentage of customers (vertical axis) account for a large proportion of mobile wallet usage (horizontal axis).<sup>440</sup>

Figure 24: Customer Enrollment in Mobile Payment Services (percent of respondents that track data)



Source: Marianne Crowe et al., *Mobile Banking and Payment Practices of U.S. Financial Institutions 2016 Mobile Financial Services Survey Results from FIs in Seven Federal Reserve Districts*, Federal Reserve Bank of Boston (Dec. 2017), at 60.

Despite the fragmented regulatory framework and layered nature of the overall system, payments have been an area of high innovation and competition, which thus far has been beneficial to consumers and the market. This competition has led to a number of private actors emerging that are capable of providing innovative services in new and different ways. Given the structure of the payments system in general, a wait-and-see approach to innovative payments may be most beneficial. The next steps in payments will likely center around the pursuit of more speed and security in payments.

### Payments Modernization

Technology continues to evolve and transform the way that consumers in the United States and abroad do business. The increase in technological capacity and delivery systems has sped up the nature of even routine transactions. Today, one can shop, compare, transact, and receive delivery faster than ever before — and the underlying technology will continue to advance in order to make this process even quicker and more efficient. However, as noncash transactions have increased, the back-end payments system underlying these transactions remains largely the same. As innovation allows for faster transactions, consumers are going to demand payments systems that likewise function with more speed.

440. Marianne Crowe, Elisa Tavilla, and Breffni McGuire, *Mobile Banking and Payment Practices of U.S. Financial Institutions: 2016 Mobile Financial Services Survey Results from FIs in Seven Federal Reserve Districts* (Dec. 2017), at 60, available at: <https://www.bostonfed.org/publications/mobile-banking-and-payment-surveys/mobile-banking-and-payment-practices-of-us-financial-institutions.aspx>.



Recognizing this, the Federal Reserve set out to lead a discussion on how best to modernize the U.S. payments system. The process started with the Federal Reserve releasing a consultation paper<sup>441</sup> for public comment in 2013. Following the comment period, the Federal Reserve issued a strategy document<sup>442</sup> that outlined desired outcomes and next steps for improving the payments system. In order to advance solutions for the five desired outcomes of speed, security, efficiency, ease of international payments, and collaboration, the Federal Reserve set up two task forces: one for faster payments and one for secure payments. While the Federal Reserve served as the leader and convener of these task forces, they were inclusive of a wide variety of stakeholders and perspectives so that they would result in collective agreement on a path forward.

### **Faster Payments Task Force**

The Faster Payments Task Force was initially convened in May 2015 with the charge of identifying and evaluating approaches for implementing safe and ubiquitous faster payments capabilities. The task force consisted of over 300 stakeholders, and was initially given a deadline of 2016 for completing this work. Their final report was released in two parts in 2017: part one<sup>443</sup> discussed the task force's approach, and part two<sup>444</sup> outlined the task force's recommendations. The task force asked industry participants to submit proposals for faster payments solutions that firms had under consideration. The goal was not to select proposals as winners, but merely to identify ideas for solutions that private-sector participants were envisioning.

### **Industry Efforts on Faster Payments**

#### **The Clearing House's Real-Time Payments (RTP) System**

In November 2017, The Clearing House's (TCH) RTP system — one of the private-sector, faster payments solutions proposed to the task force — went live as an entirely new payment system. Though RTP is open to all U.S. depository institutions, it currently connects six U.S. banks, and TCH has partnered with servicing firm FIS in order to expand the reach of RTP past TCH's membership base. RTP allows participants to send credit (push) payments through the system at any time with clearance, settlement, and availability/posting to the receiver in real time. RTP does not include a consumer-facing payment application; it is the back-end plumbing that moves payments between banks resulting from the banks' own customer-facing applications and services. One of the key components of RTP is the secure messaging system that allows banks to communicate with

441. Federal Reserve Banks, *Payment System Improvement – Public Consultation Paper* (Sept. 10, 2013), available at: [https://fedpaymentsimprovement.org/wp-content/uploads/2013/09/Payment\\_System\\_Improvement-Public\\_Consultation\\_Paper.pdf](https://fedpaymentsimprovement.org/wp-content/uploads/2013/09/Payment_System_Improvement-Public_Consultation_Paper.pdf).

442. Federal Reserve System, *Strategies for Improving the U.S. Payment System* (Jan. 26, 2015), available at: <https://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf>.

443. Faster Payments Task Force, *The U.S. Path to Faster Payments Final Report Part One: The Faster Payments Task Force Approach* (Jan. 2017), available at: <https://fasterpaymentstaskforce.org/wp-content/uploads/faster-payments-final-report-part1.pdf>.

444. Faster Payments Task Force, *The U.S. Path to Faster Payments Final Report Part Two: A Call to Action* (July 2017), available at: <https://fasterpaymentstaskforce.org/wp-content/uploads/faster-payments-task-force-final-report-part-two.pdf>.

payment messages. The messages are flexible, compliant with global messaging standards,<sup>445</sup> and allow for immediate confirmation.

TCH is the rule writer for the RTP system.<sup>446</sup> System participants must be depository institutions with branches or offices located in the United States. While nonbank firms cannot be direct participants in RTP, TCH does have a process for allowing third-party processors to be used for transmitting and receiving messages through the system on behalf of their banking clients. Currently, payment values through the system are capped at \$25,000 per transaction.

Banks are required to prefund a Federal Reserve account and participants must have Federal Reserve clearing accounts to use RTP (or have a relationship with a correspondent bank that can act as a funding agent). TCH uses a single pooled account at the Federal Reserve which is jointly owned by all participating banks (and/or funding agents), with TCH acting as the sole custodian. While all the banks have an ownership stake in the account, only TCH can approve or push money out to a bank. The account is pre-funded by the banks via Fedwire payment. The size of each bank's prefunding obligation is determined by TCH rules, and while it is envisioned that most banks will prefund once per day, provisions allow for multiple rounds of prefunding or top-up funding throughout the day.

### Same Day ACH<sup>447</sup>

Over the past several years, the rule-writing organization for all ACH networks, NACHA, and the ACH operators have been working to bring more speed to ACH payments by introducing a same-day ACH service. In 2017, its first full year of availability, same-day ACH payments amounted to 75.1 million separate transactions with an aggregate value of \$87.1 billion.<sup>448</sup>

Same-day ACH was implemented in three phases. The first phase (September 2016)<sup>449</sup> set up two new daily payment submission windows: a morning submission deadline at 10:30 a.m. ET, with settlement occurring at 1 p.m.; and an afternoon submission deadline at 2:45 p.m. ET, with settlement occurring at 5 p.m. The first phase was limited to credit (push) transactions, and mandated that every receiving financial institution be able to accept same-day ACH transfers and make the funds available to customers at the end of its processing day. The second phase (September 2017)<sup>450</sup>

445. Specifically, the messages are compliant with ISO 20022, which is a universal financial industry messaging scheme that enables financial systems around the world to communicate through a common messaging protocol.

446. The Clearing House, *Real-Time Payments Operating Rules* (Oct. 30, 2017), available at: <https://www.theclearinghouse.org/payment-systems/-/media/6de51d50713841539e7b38b91fe262d1.ashx>; The Clearing House, *Real-Time Payments Participation Rules* (Oct. 30, 2017), available at: <https://www.theclearinghouse.org/payment-systems/-/media/d0314d2612ab4619b3c09745b54cf96f.ashx>.

447. See **Appendix C** for more background on the ACH system.

448. NACHA, *Same Day ACH Volume 2017* (Jan. 11, 2018), available at: <https://web.nacha.org/resource/same-day-ach/same-day-ach-volume-2017>.

449. NACHA, *Same Day ACH: Moving Payments Faster (Phase 1)* (Sept. 23, 2016), available at: <https://www.nacha.org/rules/same-day-ach-moving-payments-faster>.

450. NACHA, *Same Day ACH: Moving Payments Faster (Phase 2)* (Sept. 15, 2017), available at: <https://www.nacha.org/rules/same-day-ach-moving-payments-faster-phase-2>.

allowed debit (pull) entries to be originated. The third and final phase (March 2018)<sup>451</sup> mandated that all same-day ACH funds be made available to customers by 5 p.m. local time for each receiving financial institution. Currently, international transactions and single transfers exceeding \$25,000 are not eligible for same-day ACH.

Although the same-day ACH project has been completed, NACHA continues its focus on increasing the speed of payments. In early 2018, NACHA asked for member comment on a proposed new rule that would: (1) add a third same-day ACH submission window with a deadline at 5:15 p.m. ET and settlement occurring at 6:30 p.m.; (2) mandate 1 p.m. local time funds availability for the first ACH settlement window; and (3) increase the eligible transaction cap to \$100,000.

## Challenges for Faster Payments in the United States

### Adoption and Acceptance

In any payment system, one of the key challenges is the level of consumer adoption of the system. If a payment system does not have broad adoption by consumers, then merchants have less incentive to expend resources to accept it. Likewise, consumers are less likely to use a payment method if it is not widely accepted. One factor that can mitigate this problem is if there is interoperability between systems, and providers can at least receive payments on behalf of customers. Without a mandate, either from the government or a large share of private sector operators, change can be much slower. For example, same-day ACH had a very low adoption level until NACHA amended its rules to require receipt.<sup>452</sup> Similarly, it was the private credit card networks that initiated the liability shift for EMV cards over the last few years. U.S. government entities have opted not to create mandates, instead preferring a collective approach.<sup>453</sup>

### Use Cases

Another challenge to faster payments is the lack of clear business and use cases for faster payments, aside from emergency payments. As a part of its payments improvement work, the Federal Reserve commissioned consultants to study the question of use cases. First, the consultants noted that among countries that have established faster payments, the decision was more strategic than based on use cases and that premium pricing was likely to affect adoption, among other factors.<sup>454</sup> When discussing business cases, the consultants found that they were net neutral or even net negative given the conservative assumptions used, but that business cases could be net positive if the time horizon were expanded.<sup>455</sup> They did note however, that latent demand could be a challenge in the analysis — that demand could emerge in the market after the new

451. NACHA, *Same Day ACH: Moving Payments Faster (Phase 3)* (Mar. 16, 2018), available at: <https://www.nacha.org/rules/same-day-ach-moving-payments-faster-phase-3>.

452. Faster Payments Task Force Final Report Part Two, at 17-18.

453. Federal Reserve System, *Strategies for Improving the U.S. Payment System: Federal Reserve Next Steps in the Payments Improvement Journey* (Sept. 6, 2017), available at: <https://fedpaymentsimprovement.org/wp-content/uploads/next-step-payments-journey.pdf>.

454. Federal Reserve System, *Strategies for Improving the U.S. Payment System* (Jan. 26, 2015), at 37-38, available at: <https://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf> ("Federal Reserve 2015 Strategies").

455. *Id.* at 43-44.

technology and infrastructure is introduced, similar to the U.K.'s experience where payments technology allowed for a shift to a “just-in-time” product delivery model that lessened the need for excess small business working capital.<sup>456</sup>

### Cost

Today, faster payments services are more expensive to use. Taking the ACH system as an example, next-day batched ACH through the Federal Reserve's FedACH system costs \$0.0035 per transaction (although there is tiered pricing, and discounts are available for higher volumes),<sup>457</sup> whereas the same-day ACH service costs \$0.052 per transaction.<sup>458</sup> This difference in cost is why the majority of ACH payments made by Treasury, for example, through FedACH may not be suitable for same-day servicing.

### Settlement

Post-transaction settlement refers to the payment of obligations between parties. This can be done in one of two ways — between private banks or through a country's central bank, with the latter seen as less risky. When it comes to faster payments, the United States, unlike some other jurisdictions, does not currently have a 24x7x365 real-time settlement system. Real-time settlement can reduce credit risk that institutions otherwise have to take once payments are cleared and posted to the receiver's account in real time.

The Federal Reserve Banks own and operate the National Settlement Service (NSS), which provides multilateral settlement for private-sector clearing arrangements, including private ACH networks. Unlike Fedwire, which settles immediately upon payment under a Real-Time Gross Settlement framework, the NSS is a deferred net settlement system, which means that payments are accumulated and netted throughout the day (or period if more frequently than daily), until net settlement occurs.<sup>459</sup> The NSS is open for use Monday-Friday from 7:30 a.m.-5:30 p.m., ET.<sup>460</sup>

In the Federal Reserve's payments strategy document, they note that the NSS expanded its daily opening times by a half hour at open and close during 2015, and that the Fed would look into weekend and 24x7x365 service in the future.<sup>461</sup> To date, available hours have not been expanded further.

The European Central Bank is developing an instant payments settlement system that is scheduled to go live in November 2018. The TARGET Instant Payment Settlement service will be available 24x7x365.<sup>462</sup>

456. *Id.* at 44-45.

457. FedACH, *Services 2018 Fee Schedule*, accessible at: <https://www.frbervices.org/resources/fees/ach-2018.html>.

458. NACHA, 2016, *Same Day ACH: FAQ*, at 3, accessible at: [https://web.nacha.org/system/files/resource/2017-08/Same-Day-ACH-FAQ-2016\\_0.pdf](https://web.nacha.org/system/files/resource/2017-08/Same-Day-ACH-FAQ-2016_0.pdf).

459. Bank for International Settlements Committee on Payment and Settlement Systems, *Principles for Financial Market Infrastructures* (Apr. 2012), at 149-150, accessible at: <https://www.bis.org/cpmi/publ/d101a.pdf>.

460. Board of Governors of the Federal Reserve System, *National Settlement Service* (last updated Jan. 15, 2015), available at: [https://www.federalreserve.gov/paymentsystems/natl\\_about.htm](https://www.federalreserve.gov/paymentsystems/natl_about.htm).

461. Federal Reserve 2015 Strategies, at 50-52.

462. European Central Bank, *The New TARGET Instant Payment Settlement (TIPS) Service* (June 2017), available at: [https://www.ecb.europa.eu/paym/intro/news/articles\\_2017/html/201706\\_article\\_tips.en.html](https://www.ecb.europa.eu/paym/intro/news/articles_2017/html/201706_article_tips.en.html).

*Recommendations*

Treasury agrees with the approach taken by the Faster Payments Task Force and notes that collective action and agreement can be a very powerful tool in creating a faster payments system that works for all stakeholders. However, now that the foundational work has been completed, Treasury recommends that the Federal Reserve set public goals and corresponding deadlines consistent with the overall conclusions of the Faster Payments Task Force's final report.

Treasury recommends that the Federal Reserve move quickly to facilitate a faster retail payments system, such as through the development of a real-time settlement service, that would also allow for more efficient and ubiquitous access to innovative payment capabilities. In particular, smaller financial institutions, like community banks and credit unions, should also have the ability to access the most-innovative technologies and payment services.

While Treasury believes that a payment system led by the private sector has the potential to be at the forefront of innovation and allow for the most advanced payments system in the world, back-end Federal Reserve payment services must also be appropriately enhanced to enable innovations. Treasury agrees with the Federal Reserve's policy criteria for introducing a new payment service – namely, that the Federal Reserve must: (1) expect to achieve full cost recovery in the long run; (2) expect the service to provide a clear public benefit, including improving the effectiveness of markets, reducing the risk in payments, or improving efficiency of the payments system; and (3) conclude that the service should be one that other providers alone cannot expect to provide with reasonable effectiveness, scope, and equity.<sup>463</sup>

### **Faster Payments Abroad**

Many jurisdictions around the world have embarked on initiatives to increase the speed of payments. In many cases, the progress towards faster payments abroad has outpaced progress in the United States. As of mid-year 2017, it is estimated that there were 25 countries that had some sort of live faster payments system. Features of these faster payment systems vary, but most systems are operational 24/7 and post transactions to accounts in real time, near real time, or within a few minutes.<sup>464</sup> At the same time, it is estimated that there were 10 additional countries that had faster payments systems under development, including the United States.<sup>465</sup>

### **The United Kingdom's Transition to Faster Payments**

One such system, the U.K. Faster Payments Scheme, is worth looking at in more detail as its transition could provide an interesting comparison to the current U.S. payments system. The U.K. Faster Payments Service (FPS) was created as an entirely new infrastructure on a directive

463. Board of Governors of the Federal Reserve System, *Federal Reserve in the Payments System*, Policy Statement (1990), available at: [https://www.federalreserve.gov/paymentsystems/pfs\\_frpaysys.htm](https://www.federalreserve.gov/paymentsystems/pfs_frpaysys.htm).

464. FIS, *Flavors of Fast: A Trip Around the World of Immediate Payments* (2017), at 29-55.

465. *Id.* at 66-71. This estimate was made prior to TCH's RTP system going live, although RTP is still currently limited to a small number of member banks.

from the government, and went live in 2008.<sup>466</sup> Prior to the implementation of FPS, the U.K. had a payment rail network that was very similar to the current U.S. system. The U.K. large value Real-Time Gross Settlement system, CHAPS, is very similar to Fedwire and CHIPS. The U.K. batched electronic payment transfer network, Bacs, is very similar to the U.S. ACH networks.<sup>467</sup>

The process to build and implement FPS took about three years, from directive to an operational system.<sup>468</sup> The United Kingdom first considered options to speed up account to account payments through systems that were already operational. While they considered speeding up Bacs to same-day service, or promoting more usage of CHAPS for lower value payments, problems of ultimate speed and cost to the consumer, respectively, pushed them to choose the path of creating a brand new infrastructure.<sup>469</sup> The FPS system authorizes and clears transactions in real time, but settlement is still deferred and done through the Bank of England's three daily settlement cycles, as was done prior to FPS. The most recent annual data from FPS shows that the service is growing the fastest of any form of electronic payment in the United Kingdom, having logged 16% growth between 2016 and 2017.<sup>470</sup>

One notable difference between the U.K. FPS and a potential U.S. faster payments system is the ability for widespread adoption. Since the U.K. banking system is more concentrated than the U.S. banking system, a U.S. system would need to be reachable by a larger number of banking institutions to benefit all consumers, and the cost to operate the system would have to be borne by a greater number of institutions which could lead to higher costs of implementation and maintenance.<sup>471</sup> While the United Kingdom provides an example for implementation of a faster payments network, many of these issues may have different outcomes in a U.S. system.

### Cross Border Faster Payments

Most payments systems work within the borders of a single country and transfer units of a single currency. However, there are systems that are in development and beginning to come online that will allow for faster transfer of funds across borders and currencies. One example is the SWIFT GPI enhanced messaging system, which went live in January 2017. SWIFT currently has over 150 banks worldwide that are committed to the service, and 45 banks that are live. The SWIFT GPI systems allows for faster crediting of funds (50% credited within 30 minutes), unaltered remittance information, complete directories of members, and tracking of payments through the entire process.<sup>472</sup>

466. Claire Greene et al., *Costs and Benefits of Building Faster Payments Systems: The U.K. Experience and Implications for the United States*, Federal Reserve Bank of Boston Current Policy Perspectives No. 14-5 (Feb. 24, 2015), at 2, available at: <https://www.bostonfed.org/publications/current-policy-perspectives/2014/costs-and-benefits-of-building-faster-payment-systems-the-uk-experience-and-implications-for-the-united-states.aspx>.

467. *Id.* at 10-11.

468. *Id.* at 28.

469. *Id.* at 30-31.

470. For additional statistics for FPS growth and volumes, see <http://www.fasterpayments.org.uk/statistics>.

471. Greene et al., at 44-46.

472. See SWIFT, *SWIFT gpi: Cross-Border Payments, Transformed* (Mar. 2018), available at: <https://www.swift.com/resource/swift-gpi-brochure>.



### **Secure Payments Task Force**

The Secure Payments Task Force was initially convened in June 2016 and focused on three priorities: (1) identifying payment security priorities; (2) advising the Federal Reserve on payment security; and (3) coordinating with the Faster Payments Task Force.<sup>473</sup> The group included stakeholders from both government and the private sector. The Federal Reserve acted as a facilitator and convener. The Secure Payments Task Force issued its final deliverable in March 2018 — an educational report on the payment lifecycle and security profiles of various payment methods including legal and regulatory references for each category of payment, and a short, high-level list of challenges and improvement opportunity within each payment bucket.<sup>474</sup> After issuing the report, the task force disbanded.

In March 2018, the Federal Reserve announced a 4-6 month study to measure and assess payments fraud and its costs, which is expected to provide insights into the vulnerability points within payment security.<sup>475</sup> The Federal Reserve also plans to establish collaborative industry workgroups on topics yet to be discussed. Other efforts to enhance payment security, such as EMV migration, have been accomplished through private sector channels.

### *Recommendations*

Treasury recognizes the utility of a working group that is focused on the continued high level of security in the U.S. payments system. To this end, Treasury looks forward to specific next steps and actionable deadlines for continued work from members of the Secure Payments Task Force and similar groups. The Federal Reserve should work as the convener, coordinator, and driver of the work product produced by members that worked on the Secure Payments Task Force, which could include work streams identified by the Faster Payments Task Force as areas for future work. Specifically, the Federal Reserve should engage stakeholders to identify payment systems resiliency as new payment systems come online, and to help counsel the Federal Reserve as it works to potentially develop its own operating faster payments system. The Federal Reserve should continue to engage stakeholders to promote and develop mechanisms to improve information sharing within the payments ecosystem, and especially between members of the improved payments task forces. Treasury recommends that continued work in the area of payment security include an actionable plan for future work, and ensure that solutions, especially in security, do not include specific tech mandates.

473. Federal Reserve System, *Strategies for Improving the U.S. Payment System: Federal Reserve Next Steps in the Payments Improvement Journey* (Sept. 6, 2017), at 7, available at: <https://www.federalreserve.gov/newsevents/pressreleases/files/other20170906a1.pdf>.

474. Secure Payments Task Force, *Payment Lifecycles and Security Profiles* (Mar. 2018), available at: <https://securepaymentstaskforce.org/wp-content/uploads/sptf-profiles-all.pdf>.

475. Board of Governors of the Federal Reserve System, *Press Release - Federal Reserve to Study Payments Fraud and Security Vulnerabilities* (Mar. 29, 2018), available at: <https://www.federalreserve.gov/newsevents/pressreleases/other20180329a.htm>.

## Wealth Management and Digital Financial Planning

### Overview

One of the Core Principles outlined in Executive Order 13772 is to “empower Americans to make independent financial decisions and informed choices in the marketplace, save for retirement, and build individual wealth.” Despite efforts at improving financial literacy, including through the Financial Literacy and Education Commission chaired by the Secretary of the Treasury,<sup>476</sup> many Americans struggle with making financial decisions that have a profound effect on their own well-being and the well-being of their dependents. Too often, individuals make financial decisions that are sub-optimal or based on immediate gratification rather than their long-term financial welfare.<sup>477</sup>

For decades, wealthier Americans have hired advisors to develop, implement, and monitor financial plans. Financial planning can involve a broad range of services, including recommendations for budgeting and goal setting, spending oversight, debt management, asset allocation for investment portfolios, selection of insurance products, and tax and estate planning; however, there is no universal definition as to what should be included in a financial plan.<sup>478</sup> There are also no legal requirements regarding the qualifications to be a financial planner. Some financial advisors may describe themselves as financial planners, but only recommend investments in a narrow range of products.<sup>479</sup>

In the past, the costs of retaining a financial planner may not have made economic sense for Americans with modest means. This lack of financial planning advice can often make it more difficult for these Americans to achieve sufficient wealth accumulation to sustain their livelihoods in retirement. To the extent that Americans do not adequately plan and save for their financial needs, additional stresses can be placed on the taxpayer-supported safety net. Disparities in access to financial expertise can lead to increased wealth inequality in the United States.

### Trends in Retirement Savings

The benefits provided by Social Security were never intended to be the sole source for retirement income needs.<sup>480</sup> While Americans are responsible for covering the remainder of their retirement needs, a significant number are inadequately prepared.<sup>481</sup>

476. See generally <https://www.treasury.gov/resource-center/financial-education/Pages/commission-index.aspx>.

477. See Justine S. Hastings and Olivia S. Mitchell, *How Financial Literacy and Impatience Shape Retirement Wealth and Investment Behaviors*, NBER Working Paper (Jan. 2011), available at: <http://www.nber.org/papers/w16740.pdf>.

478. See U.S. Government Accountability Office, *Consumer Finance: Regulatory Coverage Generally Exists for Financial Planners, but Consumer Protection Issues Remain* (Jan. 2011), at 1, available at: <https://www.gao.gov/new.items/d11235.pdf>.

479. Office of Investor Education and Advocacy, U.S. Securities and Exchange Commission, *Investment Advisers: What You Need to Know Before Choosing One* (Aug. 7, 2012), available at: <https://www.sec.gov/reportspubs/investor-publications/investorpubsinadvadershtm.html>.

480. Social Security Administration, *Understanding the Benefits* (2018), at 1, available at: <https://www.ssa.gov/pubs/EN-05-10024.pdf>.

481. YiLi Chien and Paul Morris, Federal Reserve Bank of St. Louis, *Many Americans Still Lack Retirement Savings*, Regional Economist (1st Qtr. 2018), available at: <https://www.stlouisfed.org/publications/regional-economist/first-quarter-2018/many-americans-still-lack-retirement-savings?print=true#1>.



Recent trends since the 1980s have given American workers more individual responsibility and control in retirement planning. During this period, companies shifted their worker retirement arrangements from defined benefits plans to defined contribution plans, such as 401(k) plans.<sup>482</sup> Defined contribution plans may be potentially better suited to an environment in which workers frequently change jobs,<sup>483</sup> while giving individuals greater responsibility for prudent investment of their retirement savings.

With respect to defined contribution and other self-directed retirement plans, individuals must decide when to start saving, how much to invest, which investments to select for an asset allocation that matches their risk tolerances, and what to do when transitioning between employers. Individuals may be ill-equipped to make these complex decisions, which can have significant consequences for their financial security in retirement.<sup>484</sup> According to one survey of individuals who had self-directed retirement savings, 53% were either not comfortable or were “only slightly comfortable making these decisions.”<sup>485</sup> For 59% of workers, the survey found that it was their lack of interest or capacity for saving in a 401(k) plan that limited their participation, rather than their employer not providing a plan to invest in.<sup>486</sup>

Although providing 401(k) plan participants with advice would help them manage their accounts, a recent industry survey found that only a minority of plan sponsors were offering investment advice to plan participants.<sup>487</sup> In 2016, GAO reported that plan sponsors might be reluctant to provide this investment advice due to the costs and concerns of potential legal liability.<sup>488</sup>

## Digital Tools

Digital financial planning brings the possibility of expanded access to advice for a larger number of Americans. Although personal finance software has been available since the early 1990s, these digital tools have become more sophisticated when combined with data aggregation. Through the use of data analytics, machine learning, and other computing advances, the costs of providing digital financial planning have declined significantly. Compared to human financial planners, digital financial planning services are often available to individuals with minimal balances.<sup>489</sup>

482. GAO Fintech Report, at 9.

483. Employee Benefits Research Institute, *Employee Tenure Trends, 1983-2016* (Sept. 17, 2017), at 3, available at: [https://www.ebri.org/pdf/notespdf/EBRI\\_Notes\\_v38no9\\_Tenure.20Sept17.pdf](https://www.ebri.org/pdf/notespdf/EBRI_Notes_v38no9_Tenure.20Sept17.pdf) (indicating that employee tenure data from the U.S. Census Bureau shows that the notion of a worker staying with the same employer for most of his or her career has never existed for most works and will continue not to exist).

484. U.S. Government Accountability Office, *The Nation's Retirement System: A Comprehensive Re-evaluation is Needed to Better Promote Future Retirement Security* (Oct. 2017), at 22, available at: <https://www.gao.gov/assets/690/687797.pdf>.

485. Board of Governors of the Federal Reserve System, *Report on the Economic Well-Being of U.S. Households in 2016* (May 2017), at 59, available at: <https://www.federalreserve.gov/publications/files/2016-report-economic-well-being-us-households-201705.pdf>.

486. *Id.* at 60.

487. Plan Sponsor Council of America, *60th Annual Survey of Profit Sharing and 401(k) Plans* (Feb. 2018) (finding that about one-third of plan sponsor respondents offer investment advice to participants).

488. U.S. Government Accountability Office, *401(k) Plans: DOL Could Take Steps to Improve Retirement Income Options for Plan Participants* (Aug. 2016), at 47, available at: <https://www.gao.gov/assets/680/678924.pdf>.

489. GAO Fintech Report, at 13-14.

Investment assets managed by digital advisers are projected to grow from \$100 billion in 2017 to \$385 billion by 2021.<sup>490</sup>

More importantly, digital financial planning is available to younger individuals who are entering the work force, a stage at which their wealth is typically quite small. Establishing a pattern of saving and investing during the early period of an individual's career can significantly increase the probability of long-term success in accumulating wealth and building retirement savings.<sup>491</sup>

Digital financial planning is currently offered directly to consumers via the Internet, and some services require little, if any, interaction with a human advisor. Other methods for providing digital financial advice may emerge in the future, such as through the use of chatbots.<sup>492</sup> These technological developments have resulted in certain market participants seeking to significantly undercut the pricing of human financial planners in an effort to attract clients and their assets.

At the same time, digital tools have altered the way traditional financial planners provide services to their clients. Data aggregators, for example, reduce the need of financial planners to engage in the menial task of compiling information from multiple client accounts, thereby freeing up time for more value-added activities.<sup>493</sup> For financial planners that are registered as brokers or investment advisers, data aggregation can be used to provide a more complete picture of a client's financial situation for purposes of suitability assessments or providing advice under a fiduciary standard.<sup>494</sup> Firms that employ human financial planners have reported that digital tools also improved the consistency of advice provided to clients.

Another model for providing financial planning services has also emerged. Referred to as the "hybrid" model, this model utilizes an internet or mobile-based interface for primary interaction with clients but also allows for contact with a human financial planner. Typically, fintech financial planning entities provide access to a human financial planner for an additional fee or with a higher-level service package.

Digital financial planning offers a wide range of services, some of which are more comprehensive than others. This is similar to how traditional firms market financial planning services, but may

490. Liz Skinner, *5 Robo-Advisers with the Most Client Assets*, Investment News (June 6, 2017), available at: <http://www.investmentnews.com/article/20170606/FREE/170539987/5-robo-advisers-with-the-most-client-assets> (citing a report from Cerulli Associates).

491. Employee Benefits Security Administration, U.S. Department of Labor, *New Employee Savings Tips – Time Is on Your Side*, available at: <https://www.dol.gov/sites/default/files/ebsa/about-ebsa/our-activities/resource-center/publications/new-employee-savings-tips-time-is-on-your-side.pdf> (last accessed July 10, 2018).

492. See, e.g., Sharon Adarlo, *Will Small Clients be Claimed by Chatbots?*, Financial Planning (Apr. 18, 2018), available at: <https://www.financial-planning.com/news/whats-the-word-on-chatbots-in-wealth-management?brief=00000153-6773-d15a-abd7-ef445d10000>.

493. See, e.g., Heidrick & Struggles, *Future of Digital Financial Advice* (Dec. 2016), at 19-20, available at: <https://centerforfinancialplanning.org/wp-content/uploads/2016/12/Future-of-Digital-Financial-Advice.pdf> (summarizing the work of the Certified Financial Planner Board of Standards Digital Advice Working Group).

494. Lowell Putnam, Quovo, *FINRA Standards Depend on Account Aggregation, Despite Alert's Caution*, blog post (Apr. 13, 2018), available at: <https://www.quovo.com/fintech-blog/the-ecosystem/finra-standards-depend-on-account-aggregation-despite-alerts-caution/>.

only offer limited advice.<sup>495</sup> Digital financial planning is offered by fintech applications, banks and brokerage firms, and technology companies. They often use the services of a data aggregator to centralize information about a consumer's accounts from multiple financial institutions.

The scope and nature of digital financial planning continue to evolve.<sup>496</sup> Digital financial planning services offer the ability to aggregate all accounts in one location and to produce balance sheet type information, such as net worth and investment portfolio summaries. Other services include budgeting, goal setting, and bill payment functions. Some tools compare a consumer's expenses and savings to peer groups in order to change the consumer's behavior, while others analyze spending patterns based on financial transaction data. Using computer algorithms, the service will make recommendations, such as to reduce expenses in particular areas or to consider re-financing outstanding debt. Some services automatically send funds to investment accounts, such as by rounding up spending transactions or diverting anticipated savings.

Digital financial planning can offer advice with respect to securities, loan products, or insurance products. Computer algorithms can provide advice that recommends an asset allocation and portfolio investments based on the consumer's responses to questions regarding risk tolerance, time horizons, and other factors. Some services provide exposure to recommended asset classes through investment vehicles like low-cost, exchange-traded funds. Investment portfolios may be automatically rebalanced to remain within recommended allocations and receive advice on tax loss harvesting strategies.

Some digital financial planning services directly charge consumers, through either a fixed-fee or a percentage of assets under management. Other programs offer a limited set of services for free and allow the consumer to "buy up" for additional services. Some services do not impose any fee directly on the consumer, but instead have relationships with financial partners that pay a fee for inclusion in the range of products that the service may recommend.

### **Issues and Recommendations**

Financial planning has not been directly regulated by the federal or state governments through licensing or registration requirements.<sup>497</sup> Instead, regulatory oversight is triggered either by engaging in certain activities as part of offering financial planning services or by offering these services by an individual who is regulated under another regime.

495. Financial Planning Coalition, *Consumers Are Confused and Harmed: The Case for Regulation of Financial Planners*, White Paper (Oct. 2014), at 16-19, available at: <http://financialplanningcoalition.com/wp-content/uploads/2014/06/Financial-Planning-Coalition-Regulatory-Standards-White-Paper-Final.pdf> ("FPC White Paper").

496. Cf. Michael Kitces, *The Six Levels of Account Aggregation #FinTech and PFM Portals for Financial Advisors*, blog post (Oct. 9, 2017), available at: <https://www.kitces.com/blog/six-levels-account-aggregation-pfm-fintech-solutions-accounts-advice-automation/>.

497. Some states have adopted laws regulating the conduct of financial planners, but they do not require licensing or registration as a financial planner. The definition of a financial planner under state law can vary. For example, Nevada's law applies only to persons offering advice for compensation "upon the investment of money or upon provision for income to be needed in the future" but Minnesota's law applies to any person "engaged in the business of financial planning." See Nev. Rev. Stat. § 628A; Minn. Stat. § 45.026. Both the Minnesota and Nevada laws impose a fiduciary duty upon financial planners, but, for example, Connecticut only requires disclosure of whether a financial planner has a fiduciary duty. See Conn. Pub. Act No. 17-120 (July 5, 2017).

Many financial planners provide investment advice and are therefore regulated by the SEC or state securities regulators.<sup>498</sup> Securities regulators have responded to the recent rise in digital investment advice by providing guidance related to compliance obligations under existing laws and regulations.<sup>499</sup> Securities regulators also have antifraud authority for nonsecurities advice that stems from the advisory relationship.<sup>500</sup>

Financial planning services provided by agents in connection with the sale of insurance products are regulated by state insurance regulators. Financial planners providing advice to plan participants in 401(k) plans are also subject to the obligations and prohibitions under Employee Retirement Income Security Act of 1974 and DOL rules. Although the Bureau has the authority to regulate consumer financial products or services, including financial advisory services (other than services relating to securities provided by a person regulated by the SEC or a state securities regulator, and who is acting in a regulated capacity) provided to consumers for individual financial matters or relating to proprietary financial products or services,<sup>501</sup> the Bureau generally does not have authority over accountants, tax preparers, and attorneys.<sup>502</sup>

Financial planning activities conducted by banks and its employees are subject to supervision by bank regulators and the Bureau. Accountants and attorneys offer financial planning services that are subject to oversight by state boards of accountancy and state bars, which may include regulation for conflicts of interest.

Under the current regulatory structure, financial planners could be subject to regulation by multiple regulators at the federal and state levels, with each regulator responsible for the specific activities falling within that regulator's purview. Treasury has concerns as to whether the current regulatory structure is efficient and appropriately rationalized. For example, a number of digital financial planning tools do not provide advice on 401(k) accounts, and some participants in outreach discussions indicated that regulatory compliance concerns were a factor in such decisions. Given that 401(k) account balances may account for a significant portion of an individual's investment portfolio, the lack of advice on such accounts will not advance Americans' ability to save for retirement and accumulate wealth.

498. Applicability of the Investment Advisers Act to Financial Planners, Pension Consultants, and Other Persons Who Provide Investment Advisory Services as a Component of Other Financial Services (Oct. 8, 1987) [52 Fed. Reg. 38400 (Oct. 16, 1987)].

499. See Division of Investment Management, U.S. Securities and Exchange Commission, *IM Guidance Update 2017-12: Robo-Advisers* (Feb. 2017), available at: <https://www.sec.gov/investment/im-guidance-2017-02.pdf>; Financial Industry Regulatory Authority, *Report on Digital Investment Advice* (Mar. 2016), available at: <https://www.finra.org/sites/default/files/digital-investment-advice-report.pdf>.

500. Under the antifraud provisions of the Investment Advisers Act, there is no requirement that fraudulent behavior by an investment adviser be in connection with the purchase or sale of securities. See 15 U.S.C. § 80b-6(1) and (2).

501. 12 U.S.C. §§ 5481(15)(A)(viii) and 5491(a). A financial product or service does not include activities relating to the writing of insurance. See 12 U.S.C. § 5481(15)(C).

502. 12 U.S.C. § 5517.

*Recommendations*

Numerous approaches could be undertaken to rationalize the regulatory framework for financial planning. For instance, one could focus regulatory responsibility exclusively within a single federal regulator, either new or existing. Another could be to create a self-regulatory organization (SRO) that would be subject to oversight by one or more federal regulators. The SRO could be responsible for promulgating rules, conducting inspections, and undertaking enforcement, as there are currently no widely applicable regulatory standards for those offering, or claiming to offer, financial planning advice that include competency standards and standards of conduct.<sup>503</sup> Alternatively, the SRO could only promulgate rules, and rely on a regulator to carry out examination and enforcement.

Treasury believes that appropriate protection for clients of financial planners, digital and otherwise, can be achieved without imposing either a fragmented regulatory structure or creating new regulatory entities. Treasury has concerns that the current regulatory structure discourages the provision of integrated investment advice for assets held in retirement and nonretirement accounts. A patchwork of regulatory authority makes it more costly for financial planners — costs that will be passed on to consumers in the form of higher costs or reduced services. The fragmented regulatory structure also potentially presents unnecessary barriers to the development of digital financial planning services.

Treasury recommends that an appropriate existing regulator of a financial planner, whether federal or state, be tasked as the primary regulator with oversight of that financial planner and other regulators should exercise regulatory and enforcement deference to the primary regulator. To the extent that the financial planner is providing investment advice, the relevant regulator will likely be the SEC or a state securities regulator.

---

503. FPC White Paper, at 12-15.

# **Enabling the Policy Environment**



# Agile and Effective Regulation for a 21st Century Economy

## Introduction

While the financial services industry has been a frequent adopter of new technology, the current scale and pace of technological change has left many regulators re-examining their regulatory frameworks for shortcomings from a perspective of both regulatory efficiency and effectiveness.

The United States has historically led the world in innovation in financial services. Innovation has played a factor in making the U.S. capital markets the largest, deepest, and most vibrant in the world and has been of critical importance in supporting the U.S. economy. But the United States cannot take its leading position in innovation for granted. As the rest of the world takes measures to improve its ability to create, develop, and deploy innovative new products and services in the financial sector, the United States risks losing out by failing to provide appropriate regulatory clarity and assurances, and remove unnecessary barriers to innovation.

The drive to develop new technologies is relentless, expanding to more actors with lower barriers of entry, and moving at accelerating speed. New technologies include advanced computing, “big data” analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology — the very technologies that ensure we will be able to fight and win the wars of the future.

*The Honorable James N. Mattis,  
Secretary of Defense<sup>504</sup>*

## Regulatory Sandboxes

Competitive and free markets help foster economic growth. New ideas can facilitate market efficiency, spurring improvements to services and products. Not all innovations will succeed; some might even cause harm. Regulation should address and potentially mitigate negative externalities. A regulatory environment with largely binary outcomes — either approval or disapproval — may lack appropriate flexibility for dealing with innovations and often results in extensive delays, after which the innovation has become obsolete.

The regulatory environment should instead be flexible so that firms can experiment without the threat of enforcement actions that would imperil the existence of a firm. Innovating is an iterative process, and regulator feedback can play a helpful role while upholding safeguards and standards.

---

504. Secretary Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States of America*, available at: <https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.



Treasury recognizes that U.S. regulators already employ a number of methods in support of innovation and encourages them to build on their efforts. Some examples include:

- Outreach efforts conducted throughout the United States to meet with innovators
- Creation of an agency innovation office so that innovators have a central point of contact
- Issuance of guidance, exemptive orders, or no-action letters, which may have conditions or be time-limited, to permit experimentation in the marketplace
- Agency-wide working groups that span multiple divisions and offices to address new technology trends
- Publication of white papers, speeches, and other materials discussing innovations and technology
- Engagement with foreign regulators on new developments, including cross-border collaboration agreements

During outreach discussions with Treasury, however, many stakeholders expressed frustration with the sheer number of agencies at the federal and state levels that need to be consulted when bringing a new product or service to market. Frequently, firms find that it is not even clear which agencies — or which units within those agencies — need to be engaged. The result is that innovators, particularly smaller firms, face significant and unnecessary burdens in terms of time, money, and opportunity costs.

The fragmented nature of the U.S. financial regulatory system undercuts efforts by regulators to support innovation. For example, a no-action letter or exemptive relief from one agency may be of limited use without assurance that other agencies with jurisdiction will provide comparable relief. Fragmentation also raises the likelihood of inconsistency among regulators. To be effective, a coordinated effort is needed to obtain appropriate relief across the marketplace.

New technologies, like predictive data analytics, artificial intelligence, and blockchain or distributed ledger technology, are examples of promising innovations that could be used by financial services firms. They are also technologies for which regulatory treatment may be uncertain, if for no other reason than that innovative technology requires time to mature. From the perspective of regulators, these technologies may pose unknown benefits and risks. In such situations, it would be beneficial for regulators to permit meaningful experimentation in the real world, subject to appropriate limitations.

### *Recommendations*

Treasury recommends that federal and state financial regulators establish a unified solution that coordinates and expedites regulatory relief under applicable laws and regulations to permit meaningful experimentation for innovative products, services, and processes. Such efforts would form, in essence, a “regulatory sandbox” that can enhance and promote innovation. The solution should be based on the following principles:

- Promote the adoption and growth of innovation and technological transformation in financial services
- Provide equal access to companies in various stages of the business lifecycle (e.g., start-ups and incumbents)



- Delineate clear and public processes and procedures, including a process by which firms enter and exit
- Provide targeted relief across multiple regulatory frameworks
- Offer the ability to achieve international regulatory cooperation or appropriate deference where applicable
- Maintain financial integrity, consumer protections, and investor protections commensurate with the scope of the project
- Increase the timeliness of regulator feedback offered throughout the product or service development lifecycle

Treasury will work with federal and state financial regulators to design such a solution in a timely manner. The alternative of establishing a formal sandbox overseen by a single regulator would require preemption of a firm's other regulators, and in some cases may even subject a firm to a new regulator that is unfamiliar with its operations; it is also very unclear who that single regulator would be. If financial regulators are unable to address these objectives, however, Treasury recommends that Congress consider legislation to provide for a single process consistent with the principles set forth above, including preemption of state laws if necessary.

The parameters of any regulatory sandbox should be designed with the participation of the private sector and contain appropriate metrics for testing, including sample size and development periods appropriate to these endeavors, to ensure the effectiveness of product and service development.

### International Efforts in Financial Technology

The ongoing attempt to balance innovation and regulation has spawned new regulatory initiatives, public-private partnerships, and investment schemes across both developed and emerging economies. In an effort to drive innovation, domestic investment, and effective new regulatory approaches, financial authorities abroad have endeavored to establish various “innovation facilitators.” In a recent survey by the Financial Stability Board and Basel Committee on Banking Supervision, authorities provided information about their respective domestic approaches toward innovation facilitators in three distinct categories: innovation hubs, accelerators, and regulatory sandboxes.<sup>505</sup> Innovation hubs such as LabCFTC provide access points to regulators for fintech firms, which has the dual benefit of providing firms more regulatory clarity and facilitating information sharing with regulators. Accelerators, such as the various grants and schemes in Singapore's Startup SG ecosystem, offer firms incentives to innovate and start businesses. Regulatory sandboxes like Hong Kong's Fintech Supervisory Sandbox provide an environment for firms to conduct pilot trials of financial innovations under lower regulatory burdens than might traditionally be required for the same service provided in a different way, while offering the authorities insights and feedback on new approaches.

505. Basel Committee on Banking Supervision, *Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors* (Feb. 2018), available at: <https://www.bis.org/bcbs/publ/d431.pdf>.

## Sandbox Case Studies

### Monetary Authority of Singapore

The Monetary Authority of Singapore (MAS) has introduced a regulatory sandbox — a policy framework that relaxes specific legal and regulatory requirements for a fixed time period for fintech and financial institutions experimenting with innovative products and services. Firms apply for entry into the sandbox, and if approved, MAS will determine what specific regulations it is prepared to relax for participating firms. In its guidelines for the regulatory sandbox, MAS notes that the sandbox is not meant to help firms circumvent legal and regulatory requirements, but is instead meant to help encourage efficiency and manage risks in the financial sector.<sup>506</sup> The sandbox may not be appropriate, for instance, if the proposed innovation is similar to a service already being offered in Singapore or if the applicant has not demonstrated an adequate level of due diligence. The guidelines are also clear that the financial service should have a clear plan to deploy in Singapore or be able to provide some benefit for Singapore's market and consumers. If a firm is successful in its experimentation, then upon exiting the sandbox, it must fully comply with Singapore's legal and regulatory requirements. The MAS sandbox accepts applications at any time and, if needed, MAS will permit firms to extend their time in the sandbox on a case-by-case basis.

### United Kingdom Financial Conduct Authority

The U.K. Financial Conduct Authority (FCA) launched a regulatory sandbox in June 2016 as part of the FCA's Project Innovate, an initiative started in 2014 to encourage innovation with an explicit mandate to promote competition in U.K. financial services.<sup>507</sup> The FCA selects firms in cohorts regardless of a firm's size or maturity, and allows these firms to test within the sandbox on a small scale while providing a degree of regulatory clarity and guidance. Firms in the sandbox are assigned a dedicated case officer and may be provided with targeted regulatory assistance, such as waivers or no-action letters, to facilitate a customized regulatory environment for each test. Before testing in the sandbox, however, firms must meet authorization requirements relevant for the proposed activity and must meet sufficient, bespoke safeguards to mitigate consumer harm. Upon transitioning out of the sandbox, firms are required to submit a final report highlighting the outcomes of the test. The FCA has also indicated an interest in establishing a global sandbox, where firms could potentially participate and conduct tests spanning more than one jurisdiction.

## Agile Regulation

The pace of technological development and its applications to financial services have increased dramatically. It is critical that financial regulators stay abreast of developments and establish mechanisms for adopting appropriate regulation and guidance accordingly without stifling innovations

506. Monetary Authority of Singapore, *Fintech Regulatory Sandbox Guidelines* (Nov. 2016), available at: <http://www.mas.gov.sg/~media/Smart%20Financial%20Centre/Sandbox/FinTech%20Regulatory%20Sandbox%20Guidelines%2019Feb2018.pdf>.

507. Financial Conduct Authority, *Regulatory Sandbox Lessons Learned Report* (Oct. 2017), available at: <https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf>.

that require time to mature. Regulators must be more agile than in the past in order to successfully uphold their missions without creating unnecessary barriers to innovation. This requires principles- and performance-based regulation that enables the private sector to adopt innovative, technology-based compliance solutions.

In addition, regulators need to understand technology on the same timeline as business. To do this, financial regulators need to engage with the private sector to test and understand new technologies and innovations as they arise. Agile regulation requires regulators to acquire and understand existing and emerging technologies, to engage with developers and first-movers, and to hire and retain staff with the appropriate technical expertise. To this end, Treasury believes that regulators should increase efforts to proactively engage in collaborative dialogue with the private sector as innovations arise. Regulators should be looking to facilitate U.S. strengths in technology and work toward the common goals of fostering markets and promoting growth through responsible innovation.

### **Procurement**

As new technologies are introduced in the financial services sector, financial regulators require the ability to work interactively with them in order to understand them, determine potential regulatory or operational implications, and evaluate them for potential use by the regulator itself. Regulators' hands, however, are frequently tied when it comes to obtaining such technology. Although innovators and other participants are often willing to provide the technology or proofs of concept to the regulator to help improve their understanding, statutory and regulatory requirements can either expressly prohibit, or effectively prohibit, the acquisition of the technology as either a gift or a purchase.

Under principles of federal appropriations law, federal agencies may not augment their appropriations from outside sources absent specific statutory authority.<sup>508</sup> Whether an agency may accept goods and services often depends on whether the agency has statutory authority to accept gifts. Because of the longstanding principle against augmenting appropriations, federal agencies may not accept for their own use gifts of money or other property in the absence of specific statutory authority.<sup>509</sup> Thus, even though many fintech companies are willing to provide regulators with new technology at no cost in order to demonstrate viability or to help expedite the regulatory process, federal regulators may be precluded from accepting such offers.

If a federal financial regulator wants to purchase a particular technology and has appropriated funds, federal acquisition regulations can make it difficult to do so in a timely enough manner to justify the purchase. For example, procurement regulations generally require an agency to first establish a defined need for the acquisition, describe the requirements to satisfy the agency need, and then either engage in sealed bidding or competitive negotiation, which can take many months. In outreach meetings with Treasury, some regulators indicated that it can be difficult to identify a specific agency need or describe exact requirements for a potential technological solution requiring incubation, and that, even if they could, the time to complete the acquisition would

508. U.S. Government Accountability Office, *Principles of Federal Appropriations Law, Volume II* (3rd ed. Feb 2006), at 6-162, available at: <https://www.gao.gov/assets/210/202819.pdf>.

509. *Id.* at 6-222.

be too lengthy to be effective. The nature of innovative new technologies — not yet widespread, often without direct substitutes, and materially advancing in technology in matters of weeks not months — does not fit the traditional competitive bidding and procurement processes set out by federal acquisition regulations. Even the process a firm must undergo to be considered an eligible bidder for a government contract often dissuades firms from entering the bidder pool, particularly younger companies with less resources and newer technologies that are bound to change before the process is completed. These challenges significantly limit some financial regulators' ability to better understand, test, and procure new technologies, potentially constraining the effectiveness and efficiency of federal regulation.

Federal acquisition law establishes “other transaction authority,” which allows select government agencies to develop agreements that do not need to adhere to a standard format or include terms and conditions required in traditional approaches to acquisition.<sup>510</sup> Other transaction authority has been authorized for the U.S. Department of Defense (DOD), U.S. Department of Energy, U.S. Department of Health and Human Services, U.S. Department of Homeland Security (DHS), U.S. Department of Transportation, National Aeronautics and Space Administration, Federal Aviation Administration, Transportation Security Administration, Domestic Nuclear Detection Office, Advanced Research Projects Agency-Energy, and certain programs at the National Institutes of Health. Other transaction authority can be granted on a permanent or temporary basis.

Other transaction authority has been used by these agencies to facilitate critical understanding and application of new technology by the government. DOD launched the Defense Innovation Unit (Experimental) (DIUx) in order to accelerate the development, procurement, and integration of commercially derived disruptive capabilities.<sup>511</sup> As DIUx has noted, the state of innovation is “dramatically different from past decades when key technologies were developed in government labs,” with many new technological developments originating from the commercial sector.<sup>512</sup> Since June 2016, DIUx has initiated 61 prototype projects with an average time of only 90 days from first contact to contract award.<sup>513</sup> Similarly, using other transaction authority, DHS established its Next Generation Cyber Infrastructure Apex program (“Cyber Apex”), which seeks out solutions to fill cybersecurity gaps and protection of critical systems and networks.<sup>514</sup> Cyber Apex is working with a consortium, which includes private companies in the financial services sector, to test existing marketplace solutions, while simultaneously working with a DHS innovation program in Silicon Valley in search of early-stage solutions.<sup>515</sup>

510. U.S. Government Accountability Office, *Federal Acquisitions: Use of “Other Transaction” Agreements Limited and Mostly for Research and Development* (Jan. 2016), available at: <https://www.gao.gov/assets/680/674534.pdf>.

511. Defense Innovation Unit (Experimental), U.S. Department of Defense, *Commercial Solutions Opening (CSO)*, at 1, available at: <https://www.diu.mil/download/datasets/736/DIUx-Commercial-Solutions-Opening-White-Paper.pdf> (last accessed June 29, 2018).

512. Defense Innovation Unit (Experimental), U.S. Department of Defense, *Annual Report 2017*, at 2, available at: <https://www.diu.mil/download/datasets/1774/DIUx%20Annual%20Report%202017.pdf>.

513. *Id.* at 4.

514. Cyber Security Division, U.S. Department of Homeland Security, *Technology Guide 2018*, at 6, available at: <https://www.hsdl.org/?view&did=808790>.

515. *Id.*

*Recommendations*

Treasury recommends that Congress enact legislation authorizing financial regulators to use other transaction authority for research and development and proof-of-concept technology projects. Regulators should use this authority to engage with the private sector to better understand new technologies and innovations and their implications for market participants, and to carry out their regulatory responsibilities more effectively and efficiently. Using the expertise of the private sector in developing regulatory tools will generally produce more optimal solutions than restricting input to be entirely in-house.

**Regtech**

In the aftermath of the financial crisis, financial services companies have incurred increased compliance costs in an environment of enhanced regulatory scrutiny. This dynamic has led to the rise of firms specifically focused on delivering products and services that assist regulated entities in meeting compliance requirements. These firms have been labeled by some as “regtech” companies.

Regtech within financial services has grown rapidly as advances in technology have made it possible to deliver automated solutions for compliance tasks that are otherwise performed manually. Estimates suggest there are some 80-250 firms currently operating that primarily serve the financial services industry’s compliance and regulatory needs. The range of services is broad and includes activities such as customer identification/verification and transaction monitoring for Bank Secrecy Act anti-money laundering/countering the financing of terrorism; antifraud surveillance; risk assessment and management; market conduct services; origination processes; and regulatory requirement monitoring.<sup>516</sup>

Financial services companies may benefit from partnering with regtech firms that have proprietary technologies or processes such companies may not be able to build in-house, particularly smaller entities, such as community banks, that may not have the financial resources to develop internally the technologies necessary to achieve marginal reductions in risk and compliance costs. One report on regtech firms estimates that “governance, risk and compliance (GRC) costs account for 15% to 20% of the total ‘run the bank’ cost base of most major banks. GRC demand drives roughly 40% of costs for ‘change the bank’ projects under way.”<sup>517</sup>

Regulators at both the federal and state levels can have a significant impact on the regtech industry through not only the compliance requirements they set, but also the means by which examination for compliance is executed. Some emerging regtech solutions aim to facilitate more efficient communication between regulated financial institutions and regulators by providing APIs or distributed ledger technology-based channels to share information, such

516. See Bain and Company, *Banking Regtechs to the Rescue?* (2016), available at: [http://www.bain.com/Images/BAIN\\_BRIEF\\_Banking\\_Regtechs\\_to\\_the\\_Rescue.pdf](http://www.bain.com/Images/BAIN_BRIEF_Banking_Regtechs_to_the_Rescue.pdf); and PricewaterhouseCoopers, *Regtech in Financial Services* (2018), available at: <https://www.pwc.com/us/en/industries/financial-services/research-institute/top-issues/regtech.html>.

517. See Bain and Company, at 3.

as suspicious transaction reports and supporting information, or other mandatory reports, with central banks and regulators, and by providing digital channels for further inquiries and responses.

Treasury encourages regulators to appropriately tailor regulations to ensure innovative technology companies providing tools to regulated financial services companies can continue to drive technological efficiencies and cost reductions. Additionally, Treasury encourages regulators to seek out and explore innovative partnerships with financial services companies and regtech firms alike to better understand new technologies that have the potential to improve the execution of their own regulatory responsibilities more effectively and efficiently.

## **Engagement**

Beyond experimentation, broad regulatory engagement with financial services companies on multiple levels is essential. Treasury commends the efforts by financial regulators to create labs, working groups, innovation offices, and other channels for industry participants to engage directly with regulators. These discussions provide regulators with visibility into technology developments and provide an opportunity to receive real-time feedback from regulators on their ideas. Additionally, they encourage an ongoing dialogue, lessening the likelihood that financial services firms are operating based on erroneous information or misinterpretation of regulations.

However, a number of reasons have been provided for why some in the private sector may be reluctant to communicate openly with regulators. A few participants in Treasury outreach meetings raised concerns that conversations with regulators could be used as a reason to initiate an enforcement investigation.<sup>518</sup> Participants argued that if regulators are not in a position during engagement sessions to provide either assurances or helpful advice on how innovations can comply with the rules, then there is little for the market participant to gain from a one-way engagement and significant risk of being delayed and losing the chance to be the first to market. Some firms faulted financial regulators for having an “enforcement first” perspective, not being timely in providing useful guidance, and not having a sufficient appreciation of how delay and regulatory uncertainty can result in a new product or service being overtaken by a competitor.

## **Recommendations**

Treasury recommends that financial regulators pursue robust engagement efforts with industry and establish clear points of contact for industry and consumer outreach. The outcome of engagement should be to create an environment where growth can occur with appropriate protections while reducing compliance costs. Both regulators and the private sector must recognize that they have a symbiotic relationship that is needed to support the U.S. economy and maintain global competitiveness.

Treasury recommends that financial regulators increase their efforts to bridge the gap between regulators and start-ups, including efforts to engage in different parts of the country rather than

518. On the other hand, Treasury acknowledges that some firms may have had reason to believe that their activities might be subject to regulation and chose not to bring their activities to the attention of regulators. See, e.g., Peter Van Valkenburgh, Coin Center, *Framework for Securities Regulation of Cryptocurrencies* (Jan. 2016), available at: <https://coincenter.org/wp-content/uploads/2016/01/SECFramework2.5.pdf> (noting that some cryptocurrencies may “functionally resemble securities” when sold to investors).



requiring entities to come to Washington, D.C. Unlike incumbent financial institutions with well-established government relations offices, start-ups may be less familiar with how to engage with federal regulators but equally critical for regulators to engage with. While start-ups must comply with existing laws and regulations, regulators should seek to understand the business models of these entities that may be subject to their authorities. Further, Treasury recommends that financial regulators periodically review existing regulations as innovations occur and new technology is developed and determine whether their regulations fulfill their original purpose in the least costly manner.

Treasury recommends that financial regulators engage at both the domestic and international levels, as financial technology in many cases is borderless. Treasury encourages international initiatives by financial regulators to increase their knowledge of fintech developments in other nations, such as the recent agreement between the CFTC and the U.K. Financial Conduct Authority.<sup>519</sup>

### **Education**

More efforts need to be taken to close the knowledge gap, both between private industry and regulators, and among and within financial regulators themselves. In outreach meetings with Treasury, many industry participants from both the financial services industry and the technology industry indicated that regulators and examiners often lack basic knowledge about the technologies employed by firms. Participants also indicated that technical sophistication often varied among regulators, adding to difficulties in navigating an already fragmented regulatory system.

Treasury acknowledges that it is challenging for the U.S. government to attract and retain talented human capital, as it lacks the ability to compete for such talent with incentives such as higher salaries and equity compensation. While the attraction of highly qualified technical personnel to the private sector may disadvantage the government, it is surely a benefit for U.S. firms leading the world in innovation.

Because innovation in technology occurs at such a rapid pace, Treasury recognizes that it may be impractical for individuals to leave the private sector temporarily and commit to public service for an extended period of time without being at significant risk of not being able to re-enter the technology sector at a competitive level. Thus, the nature of the technology industry creates a structural close hold on its workforce. Despite these differences, Treasury believes that a number of steps can be taken to improve the technology-savviness of the regulatory workforce.

Currently, some universities have programs that bring policymakers and the technology industry together through practical simulations and experiential learning, requiring each to walk in the shoes of the other. These activities, for instance when applied to topics like cybersecurity, help policymakers to understand and appreciate the demands of managing a corporation and a firm's duties that may cause the firm to take various actions in response to regulatory guidance. These types of experiential learning opportunities are critical to bridging the knowledge gap between regulators and the entities they regulate.

---

519. U.S. Commodity Futures Trading Commission, *Press Release No. 7698-18* (Feb. 19, 2018), available at: <https://www.cftc.gov/PressRoom/PressReleases/pr7698-18>.

Another approach to bridging this gap is to bring experts into a regulatory agency on temporary assignment. Some agencies, like the SEC, already have existing professional fellowship programs in which outside industry veterans join the agency on a non-permanent basis and are subject to extensive requirements to manage any conflicts of interest that arise from their temporary hiatus from the private sector. Regulators benefit from exposure to the fellow's knowledge, and the fellow benefits from exposure to the regulator's mission and operations. The experience and understanding of regulatory processes acquired during these fellowships is then shared by the participating fellows upon returning to industry.

Since 2012, the U.S. Government has recruited Presidential Innovation Fellows to leverage outside industry expertise to work with the government. The Presidential Innovation Fellows serve for a 12-month program, which can be extended for up to a total of four years. To date, none of the financial regulators have participated in the program. Recently, the OCC considered creating new positions for Innovation Fellows as part of its efforts to better understand innovation. Treasury encourages financial regulators to consider establishing similar fellowship opportunities that would focus on financial technology, recognizing the likely shorter duration required to make such a fellowship successful in attracting the right talent.

### Critical Infrastructure

The transformational technologies and service offerings examined by this report in key areas of financial services have generated even further innovation leading to the re-architecting of current technologies, applications, networks, and back-office infrastructures. Cybersecurity, resilience, and operational risk considerations are inseparable from any examination of these technologies. Particularly when applied to financial services, these developments directly impact the nation's critical infrastructure.

Increased reliance on emerging technologies yields benefits as well as new risks, requiring developers to build for security, resiliency, and agility from the start, not as afterthoughts. Treasury recommends that financial regulators thoroughly consider cybersecurity and other operational risks as new technologies are implemented, firms become increasingly interconnected, and consumer data are shared among a growing number of firms, including third parties. The task of ensuring that the country's critical infrastructure — systems, networks, functions, and data — remain available and reliable is increasingly complex as risks may reside throughout the supply chain, not solely with the owner or operator. Furthermore, the supply chain includes a mix of firms, operating under a range of cybersecurity risk profiles — some may lack common baseline cybersecurity protections and standards, and others, even regulated firms subject to cybersecurity regulations, suffer from differing interpretations and implementations of regulatory guidance. A firm with a more mature cybersecurity posture may additionally be exposed to cybersecurity risks because its vendors or suppliers have not developed a similarly robust cybersecurity posture.



The Banking Report provided two recommendations regarding cybersecurity that Treasury continues to endorse: (1) developing a common lexicon, and (2) harmonizing regulations.<sup>520</sup> In addition to the work taking place within the Financial and Banking Information Infrastructure Committee (FBIIC) to implement those recommendations, the FBIIC agencies should neither stifle innovation, nor mandate specific technology solutions; the FBIIC agencies should remain technology neutral. Treasury additionally recommends that the FBIIC consider establishing a technology working group charged with better understanding the technologies that firms are increasingly relying upon, and staying well-informed regarding innovation taking place within the sector.

Policy approaches to protect the nation's critical infrastructure cannot focus solely on regulation and the financial regulators. Treasury will continue to partner with federal agencies to better understand supply chain and third-party risks, and work directly with financial services firms, and across the critical infrastructure community, to address these challenges.

Treasury also encourages the sector to migrate away from the historical focus on threat, and balance that with a focus on vulnerability identification and remediation. Broadly speaking, the financial services industry works very hard now to identify threats that exploit vulnerabilities to create risk. Reducing vulnerabilities is as important, if not more so, as reducing risk. When a vulnerability is found and closed, no one can exploit it. Alternatively, finding one threat (such as a criminal enterprise) and shutting it down will still leave the vulnerability available in a system for exploitation by other threats.

To this end, Treasury commits to leading a multiyear program with the financial services industry to identify, properly protect, and remediate vulnerabilities. Finally, Treasury supports the industry's continued efforts to promote and support the adoption of the National Institute of Standards and Technology Cybersecurity Framework to reduce risks to the nation's financial critical infrastructure.

## International Approaches and Considerations

### Overview

Across the world, many economies are shifting toward enabling more open and faster banking services by enabling greater competition from nonbanks like fintechs and technology companies. Primarily, open banking has entailed enabling greater access to financial data or payment clearing and settlement systems that were previously maintained by or provided to banks and unavailable to nonbanks. Often, this enhanced access is provided through APIs. These efforts are largely in the preliminary stages of being implemented but are expected to significantly shape how financial services are delivered in these economies.

520. The Banking Report, at 31.

- **India:** India introduced the Unified Payments Interface (UPI) in August 2016, which allows for open API interfaces for real-time payments.<sup>521</sup> The UPI, combined with other policy efforts to minimize the use of cash, promote digital identity, and leverage mobile devices, has created an environment where many new payment players are expected to emerge.
- **Europe and the United Kingdom:** The Revised Payment Services Directive (PSD2) and the United Kingdom's Open Banking initiative were intended to encourage greater competition within these jurisdictions' banking systems by allowing nonbank firms to connect to banking payments and data systems through licensing regimes tailored for these activities.<sup>522</sup>
- **Australia:** Australia commissioned an open banking study, with the final report published in late 2017.<sup>523</sup> The government is now consulting on a final decision and implementation.
- **Hong Kong:** Hong Kong is embarking on an initiative to launch a “new era of smart banking.” This initiative was announced in September 2017,<sup>524</sup> and includes areas of focus such as faster payments, fintech sandboxes, and open-banking APIs. To implement the API aspect of the strategy, the Hong Kong Monetary Authority published an open API framework in July 2018.<sup>525</sup>
- **Singapore:** The Monetary Authority of Singapore has taken a more organic approach to open banking. While the idea is being encouraged by the government, Singapore believes that open banking will ultimately be more successful if it is led by the industry and not done through government mandates.<sup>526</sup> Financial services companies have been working toward APIs as the Association of Banks in Singapore released a voluntary API playbook for banks in 2016.<sup>527</sup>

521. National Payments Corporation of India, *Press Release – NPCI's Unified Payments Interface (UPI) Set to Go Live* (Aug. 25, 2016), available at: <https://www.npci.org.in/sites/default/files/NPCIsUnifiedPaymentsInterface%28UPI%29settogoliveAugust252018.pdf>.

522. Competition and Markets Authority, *Retail Banking Market Investigation: Final Report* (Aug. 9, 2016), at 441-461, available at: <https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf>; Directive (EU) 2015/2366 of the European Parliament and of the Council (Nov. 25, 2015), available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN> (preamble).

523. The Treasury (Australia), *Review into Open Banking: Give Customers Choice, Convenience and Confidence* (Dec. 2017), available at: [https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-\\_For-web-1.pdf](https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf).

524. Hong Kong Monetary Authority, *Press Release – A New Era of Smart Banking*, Press Release (Sept. 29, 2017), available at: <http://www.hkma.gov.hk/eng/key-information/press-releases/2017/20170929-3.shtml>.

525. Hong Kong Monetary Authority, *Press Release – Open API Framework for the Banking Sector and the Launch of Open API on HKMA's Website*, Press Release (July 18, 2018), available at: <http://www.hkma.gov.hk/eng/key-information/press-releases/2018/20180718-5.shtml>.

526. Chanyaporn Chanjaroen and Haslinda Amin, *Singapore Favors 'Organic' Policy in Move Toward Open Banking*, Bloomberg (Apr. 11, 2018), available at: <https://www.bloomberg.com/news/articles/2018-04-12/singapore-favors-organic-policy-in-move-toward-open-banking>.

527. The Association of Banks in Singapore, *Media Release – The Association of Banks in Singapore Issues Finance-as-a-Service: API Playbook*, Media Release (Nov. 16, 2016), available at: [https://abs.org.sg/docs/library/mediarelease\\_20161116.pdf](https://abs.org.sg/docs/library/mediarelease_20161116.pdf).

Within banking systems, there are also significant efforts to modernize and increase core capabilities, such as in the area of payments. Many jurisdictions around the world have embarked on initiatives to increase the speed of wholesale payments through implementation of real-time payment systems. As of mid-year 2017, it was estimated that there were 25 countries (primarily large advanced economies) that had some type of live faster-payments system.<sup>528</sup>

Impacting the provision of credit, nonbank digital lenders have emerged in many jurisdictions that deploy automated lending platforms, provide rapid credit decisions, and are funded through investment capital or peer-to-peer financing.<sup>529</sup> Some of the most sizable activity and fastest growth has occurred in U.S., Chinese, and U.K. markets. The U.S. market has grown rapidly to about \$35 billion in 2016, or roughly three times 2014 levels. The U.K. market, while materially smaller, has also roughly tripled since 2014 to £4.6 billion. Meanwhile, the Chinese market has grown to \$246 billion in 2016, up by a factor of 10 from \$24.3 billion in 2014.<sup>530</sup> Common across these markets is an emphasis on providing credit to consumer and small business segments.

## Data Regulation

The expanded access to financial and nonfinancial data enabled by movement toward more open banking across multiple jurisdictions has raised critical issues with respect to protecting the confidentiality of consumers' financial and personal data. Multiple jurisdictions have adopted laws to address some of these growing concerns with respect to their personal data. For example, Europe recently introduced its General Data Protection Regulation (GDPR), which attempts to create a fundamental right to privacy that includes the right for people to have their data deleted and transferred, among other provisions. The GDPR, however, has raised a number of questions about implementation for companies, regardless of their country of domicile, that hold the personal data of E.U. and U.K. citizens.<sup>531</sup> Uncertainties in the implementation of GDPR may also create unnecessary barriers to trade and damage cross-border regulatory cooperation due to this lack of regulatory clarity. Some other examples of efforts to add personal data protection regulations

528. FIS, *Flavors of Fast: A Trip Around the World of Immediate Payments* (4<sup>th</sup> ed. June 2017), at 29-55, available at: <https://www.fisglobal.com/flavors-of-fast-2017>.

529. See, e.g., World Economic Forum, *The Future of FinTech: A Paradigm Shift in Small Business Finance* (Oct. 2015), available at: [http://www3.weforum.org/docs/IFP/2015/FS/GAC15\\_The\\_Future\\_of\\_FinTech\\_Paradigm\\_Shift\\_Small\\_Business\\_Finance\\_report\\_2015.pdf](http://www3.weforum.org/docs/IFP/2015/FS/GAC15_The_Future_of_FinTech_Paradigm_Shift_Small_Business_Finance_report_2015.pdf) (discussing small business lending via marketplace lenders).

530. Tania Ziegler et al., *The 2017 Americas Alternative Finance Industry Report*, University of Cambridge Judge Business School Centre for Alternative Finance (May 2017), available at: [https://www.jbs.cam.ac.uk/fileadmin/user\\_upload/research/centres/alternative-finance/downloads/2017-06-americas-alternative-finance-industry-report.pdf](https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-06-americas-alternative-finance-industry-report.pdf) (U.S. market); Kieran Garvey et al., *Cultivating Growth: The 2nd Asia Pacific Region Alternative Finance Industry Report*, University of Cambridge Judge Business School Centre for Alternative Finance (Sept. 2017), available at: [https://www.jbs.cam.ac.uk/fileadmin/user\\_upload/research/centres/alternative-finance/downloads/2017-12-cultivating-growth.pdf](https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-12-cultivating-growth.pdf) (Chinese market); Bryan Zhang et al., *Entrenching Innovation: The 4th UK Alternative Finance Industry Report*, University of Cambridge Judge Business School Centre for Alternative Finance (Dec. 2017), available at: [https://www.jbs.cam.ac.uk/fileadmin/user\\_upload/research/centres/alternative-finance/downloads/2017-12-21-ccaf-entrenching-innov.pdf](https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-12-21-ccaf-entrenching-innov.pdf) (U.K. market).

531. See, e.g., Secretary Wilbur Ross, *E.U. Data Privacy Laws are Likely to Create Barriers to Trade*, Financial Times (May 30, 2018).

include Hong Kong's Personal Data Ordinance on Privacy in 2012,<sup>532</sup> Australia's Consumer Data Right,<sup>533</sup> and Singapore's Personal Data Protection Act.<sup>534</sup>

## Business Models

Nonbanks and technology-focused companies have played active roles in developing payments and credit-scoring systems to improve the access to and functionality of financial services, and to reduce costs. While access to payment clearing and settlement services is generally limited to depositary institutions in the United States, some countries have provided mechanisms that allow nonbanks to access those services. Notable examples include China and regions of Africa, where the payments market is heavily reliant on nonbank-operated chat or mobile phone text message systems.

In China, authorities have allowed nonbank fintechs to access payment systems to clear and settle retail payment transactions. Large nonbank firms, like Ant Financial (Alipay) and Tencent (WeChat) have established dominant positions in the Chinese mobile payments market, with 54.3% and 38.2% shares of the market, respectively, in 2017.<sup>535</sup> The mobile wallets and payments mechanisms allow consumers to make payments while shopping online or through a messaging app, and provide access to other financial services offered within the ecosystem of the company that owns the mobile wallet.<sup>536</sup>

M-PESA, which began in Kenya, is another example of a nonbank payments company that operates outside a bank-centric payments ecosystem. It is operated by a telecommunications company and allows customers to make and receive payments using a mobile phone, without the need for a bank account. As of year-end 2016, M-PESA was live in 10 countries, had 29.5 million active customers, and processed about 6 billion transactions.<sup>537</sup>

Given the success of these nonbank models in some jurisdictions, it is not surprising that many analysts are estimating that a significant share of financial institutions' volumes and profits around

532. Privacy Commissioner for Personal Data (Hong Kong), *The Ordinance at a Glance*, available at: [https://www.pcpd.org.hk/english/data\\_privacy\\_law/ordinance\\_at\\_a\\_Glance/ordinance.html](https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html) (last accessed June 29, 2018).

533. As announced on November 26, 2017, the Consumer Data Right (CDR) is intended as an economy-wide right, to be applied sector-by-sector on the designation of the Australian Treasurer. The Treasurer will be leading the development of the CDR, with the design of the broader CDR informed by the government's response to the recommendations of its open banking review. See The Treasury (Australia), *Consumer Data Right – Fact Sheet*, available at: <http://static.treasury.gov.au/uploads/sites/1/2018/02/180208-CDR-Fact-Sheet-1.pdf> (last accessed June 29, 2018).

534. Personal Data Protection Commission (Singapore), *Legislation and Guidelines Overview*, available at: <https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview> (last accessed June 29, 2018).

535. Don Weinland, *Tencent Closes in on Alipay Crown*, Financial Times (Apr. 3, 2018).

536. Mancy Sun et al., Goldman Sachs Equity Research, *The Rise of China Fintech* (Aug. 7, 2017); Wei Wang and David Dollar, Brookings Institution, *What's Happening with China's FinTech Industry* (Feb. 2018), available at: <https://www.brookings.edu/blog/order-from-chaos/2018/02/08/whats-happening-with-chinas-fintech-industry/>.

537. Vodafone Group Plc., *Press Release – Vodafone Marks 10 Years of the World's Leading Mobile Money Service, M-Pesa* (Feb. 21, 2017), available at: <http://www.vodafone.com/content/index/media/vodafone-group-releases/2017/m-pesa-10.html#>.

the world are at risk of disruption from technology-driven business models.<sup>538</sup> In particular, technology firms are expected to take advantage of new open-banking paradigms, such as Europe's PSD2 or India's UPI, for instance, by using messaging platforms to access the country's real-time payment system.

## New Technologies

In this changing international landscape, the intersection of technological advancement, data privacy, and industrial policy has put pressure on globally active firms. As they confront technological innovation, some foreign governments have attempted to restrict access to U.S. firms by, for example, requiring data to be stored and processed locally, putting caps on foreign ownership, forcing joint ventures, and enforcing discriminatory licensing requirements. These restrictions have a range of commercial consequences for those firms and may conflict with regulatory objectives, both in the United States and abroad.

Interest in crypto-assets from a range of financial authorities has increased substantially over the past year, as evidenced in the March 2018 G20 Finance Ministers and Central Bank Governors Communiqué. For the first time, the G20 explicitly addressed crypto-assets, and assigned the Financial Stability Board (FSB) “in consultation with other standard-setting bodies, including the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions, and Financial Action Task Force (FATF) to report in July 2018 on their work on crypto-assets.” The resulting report sets out the metrics that the FSB will use to monitor crypto-asset markets as part of its ongoing assessment of vulnerabilities in the financial system.<sup>539</sup> The G20 authorities are cognizant of the inherent risks these new assets currently pose for investor protection and anti-money laundering and illicit finance regimes.

### March 2018 G20 Communiqué

We acknowledge that technological innovation, including that underlying crypto-assets, has the potential to improve the efficiency and inclusiveness of the financial system and the economy more broadly. Crypto-assets do, however, raise issues with respect to consumer and investor protection, market integrity, tax evasion, money laundering and terrorist financing. Crypto-assets lack the key attributes of sovereign currencies. At some point they could have financial stability implications. We commit to implement the FATF standards as they apply to crypto-assets, look forward to the FATF review of those standards, and call on the FATF to advance global implementation. We call on international standard-setting bodies to continue their monitoring of crypto-assets and their risks, according to their mandates, and assess multilateral responses as needed.

Source: Communiqué of the G20 Finance Ministers & Central Bank Governors, Buenos Aires, Argentina (March 19-20, 2018).

538. Miklós Dietz et al., McKinsey & Company, *Remaking the Bank for an Ecosystem World* (Oct. 2017), available at: <https://www.mckinsey.com/industries/financial-services/our-insights/remaking-the-bank-for-an-ecosystem-world> (estimating that 65% of bank profits are under threat from nonbank players, like large technology platform companies); Aaron Fine and Rick Chavez, Oliver Wyman, *The Customer Value Gap: Re-Calculating the Route* (2018), available at: <http://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/January/state-of-the-financial-industry-2018-web.pdf>.

539. Financial Stability Board, *Crypto-Assets: Report to the G20 on Work by the FSB and Standard-Setting Bodies* (July 16, 2018), available at: <http://www.fsb.org/wp-content/uploads/P160718-1.pdf>.



Related to these issues, but separate from the focus on crypto-assets, is continuing international interest in the underlying technology. The financial services industry is already developing applications for distributed ledger technology (DLT), including in commodities trading and securities settlement, property registries, and secure, trusted identity products and services, among other use-cases. Some central banks have contemplated the potential for central bank-backed digital currencies, or a tokenized form of a fiat currency that utilizes DLT, asserting that they could potentially help reduce fees, processing times, and operational risk for market participants. Whether such potential benefits could materialize is still highly uncertain. Some central bankers are also considering how to use DLT to conduct interbank payments or employ DLT as a basis for other financial infrastructure, including through Project Ubin at the Monetary Authority of Singapore and Project Jasper at the Bank of Canada. Private consortiums are also experimenting with permissioned distributed ledgers, which operate by allowing only a known set of participants to validate transactions.

### **International Engagement**

The United States engages with international counterparts on a bilateral and multilateral basis to advance U.S. interests abroad. Given the cross-border implications of financial technology, international bodies have established various groups focused on financial innovation. Financial authorities from the United States participate in international forums such as G20, the FSB, and International Monetary Fund to identify and manage global challenges, mitigate financial stability risks, and strengthen the external environment for U.S. growth. Additionally, U.S. authorities monitor developments and gather information to inform U.S. regulatory and supervisory approaches and priorities.

The United States strives to advance a coordinated policy approach at relevant international forums and standard-setting bodies. As financial technologies evolve, the emerging regulatory issues stemming from financial innovation often mean that U.S. authorities are in the process of developing a domestic regulatory approach at the same time that international organizations and standard-setting bodies are determining an international agenda. It is important that the United States remain engaged in these international discussions to ensure that any outcomes are consistent with domestic priorities.

International organizations have ramped up work on financial innovation in response to members' demand. However, U.S. authorities should guard against international standards being prematurely adopted before domestic policy is sufficiently advanced. International forums offer important opportunities for U.S. regulatory authorities to share experiences and gather information about the implications of financial innovation for policy objectives such as financial stability, investor protection, and illicit finance regimes. Financial innovations can pose fresh questions and challenges for regulatory authorities, and there is a tension between taking time to develop competency and experience relevant to a new technology and adopting a regulatory framework for that technology in a timely manner. For this reason, international regulatory approaches and standards should be developed in coordination with market participants to ensure the regulatory regime is appropriately calibrated.

Given the nature of innovations in financial technology, cybersecurity is of critical importance, and the United States remains committed to building cyber resilience in the financial sector domestically

and internationally. Internationally, the United States is engaging with foreign counterparts on cybersecurity in the financial sector through several key multilateral and bilateral partnerships. At the G-7, Treasury co-chairs the Cybersecurity Expert Group (CEG) with the Bank of England. The CEG discusses approaches to financial sector cybersecurity, with the objective of fostering common understandings and collaboration on areas of interest. The G-7, through the CEG, continues to work toward building cyber resilience internationally in the financial services sector.

**Figure 25** illustrates the various initiatives related to financial innovation underway in a number of prominent international bodies. Treasury continues to engage closely with other U.S. agencies, including those representing the United States at the Committee on Payments and Market Infrastructures, the International Organization of Securities Commissions, FATF, and other international bodies, to maintain a unified message — namely that we support responsible innovation in the marketplace, while maintaining the integrity and accessibility of the financial system. It is important that we stay vigilant to the international discussions on financial innovation, particularly any which may result in the potential development of standards or best practices, to ensure that any outcomes are balanced and consistent with the U.S. approach.

### *Recommendations*

Treasury should continue to leverage international bodies to support our domestic agenda, with domestic financial and regulatory priorities guiding the positions we take in international forums. Treasury will work to ensure actions taken by international organizations align with U.S. national interests and the domestic priorities of U.S. regulatory authorities. Treasury believes in avoiding regulatory fragmentation where possible, and promoting international approaches that facilitate cross-border capital and investment flows. It would be premature, however, to develop international regulatory standards for many applications of financial technology currently under discussion. In these cases, Treasury recommends continued participation by relevant experts in international forums and standard-setting bodies to share experiences regarding respective regulatory approaches and to benefit from lessons learned. Market participants require regulatory clarity to operate, but that clarity must start from domestic authorities determining the right approach within their own jurisdictions.

Treasury and U.S. financial regulators should engage with the private sector with respect to ongoing work programs at international bodies to ensure regulatory approaches are appropriately calibrated. Discussions on financial innovation occurring in international organizations sometimes do not include relevant experts. Additionally, central banks, ministries of finance, and capital markets regulators must continue building relevant in-house expertise regarding financial innovations such as cloud services, APIs, and artificial intelligence.

Finally, Treasury and U.S. financial regulators should proactively engage with international organizations to ensure that they are adhering to their core mandates. Standard-setting bodies should closely align their work and recommendations with the core competencies of each institution, including when they are addressing issues related to applications of financial technology.

Figure 25: International Interagency Fintech Collaboration Efforts

Group Name		
Participating agencies	Mission / Goals	Correlation to Fintech
The Bank for International Settlements, Committee on Payments and Markets Infrastructure and Committee on the Global Financial System		
Federal Reserve (committee chair) and the Federal Reserve Bank of New York represent the United States. Other members include other central banks.	Identify and assess potential sources of stress in global financial markets, further the understanding of the structural underpinnings of financial markets, and promote improvements to the functioning and stability of these markets.	Fintech Payments and Lending. From 2014 to February 2017, the Committee on Payments and Markets Infrastructure has published papers on a variety of fintech payments topics including DLT in payments, virtual currencies, faster payments, and nonbanks in retail payments papers.
Basel Committee on Banking Supervision's Task Force on Financial Technology (TFFT)		
OCC co-chairs, and FDIC and Federal Reserve also represent the United States. Other participants include central banks and authorities with formal responsibility for the supervision of banking business.	TFFT assesses the risks and supervisory challenges associated with innovation and technological changes affecting banking.	General Fintech. TFFT's work is currently focused on the effect that fintech has on banks and banks' business models, and the implications this has for supervision.
Financial Action Task Force (FATF) Fintech & Regtech Forums		
Treasury (lead), Federal Reserve and OCC represent the United States. Other members include agencies from other jurisdictions and two regional organizations, and associate members include other international and regional organizations.	Conduct industry outreach and provide a platform for a constructive dialogue and support innovation in financial services while addressing the regulatory and supervisory challenges posed by emerging technologies.	General Fintech. In 2017, FATF held three fintech-related events on fintech, regtech, and AML/ countering the financing of terrorism (CFT) covering topics including: relevance of emerging fintech trends to financial institutions; AML/ CFT standards in fintech; how different jurisdictions approach the regulation and supervision of fintech; fintech's effect on AML/CFT-related information availability and exchange; and risk management and mitigation for fintech.



Group Name		
Participating agencies	Mission / Goals	Correlation to Fintech
<b>Financial Stability Board Financial Innovation Network</b>		
Treasury, FRB, SEC, OCC, FDIC, FRBNY, and the Office of Financial Research represent the United States. Other members include central banks and authorities with formal responsibility for the supervision of banking business.	The Financial Stability Board promotes international financial stability by coordinating national financial authorities and international standard-setting bodies as they work toward developing financial sector policies. The Financial Innovation Network is responsible for understanding emerging trends in financial services and the potential effect on financial stability.	General Fintech. In 2017, published white papers and a report on the financial stability implications of fintech credit (in collaboration with the Committee on the Global Financial System), the use of artificial intelligence (AI) and machine learning in financial services, and fintech supervisory and regulatory issues that merit authorities' attention.
<b>International Credit Union Regulators Network (ICURN)</b>		
NCUA represents the United States. Other members include national and other supervisors of credit unions and financial cooperatives.	ICURN provides training to supervisors of credit unions and financial cooperatives on a variety of topics.	General Fintech. ICURN's July 2017 conference included a panel on understanding fintech and regulation. Discussion covered sectors including payments, lending, digital wealth management, and DLT.
<b>International Organization of Securities Commissions (IOSCO), Committee on Emerging Risks</b>		
SEC and CFTC represent the United States. Other members include national and provincial securities regulators.	IOSCO brings together the world's securities regulators and works with the G20 and the Financial Stability Board (FSB) on the global regulatory reform agenda. The Committee on Emerging Risks provides a platform for securities regulators and economists to discuss emerging risks and market developments and to develop and assess tools to assist regulators in reviewing the regulatory environment and identifying, monitoring, and managing systemic risk.	General Fintech. In February 2017, the Committee on Emerging Risks published a research report on fintech, which included sections on fintech lending, digital investment advice, DLT, fintech in emerging markets, and other regulatory considerations. IOSCO also established an Initial Coin Offering Consultation Network, through which members can discuss their experiences and concerns regarding token sales, and has issued related statements to members and the public.

Source: U.S. Government Accountability Office, *Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight* (March 2018).

# **Appendix A**

## **Participants in the Executive Order Engagement Process**



# Participants in the Executive Order Engagement Process

## GOVERNMENT AND INTERNATIONAL

### U.S. Federal and State

Appraisal Subcommittee of the Federal Financial Institutions Examination Council	Financial Crimes Enforcement Network
Arizona Attorney General's Office	Financial Industry Regulatory Authority
Board of Governors of the Federal Reserve System	Government National Mortgage Association (Ginnie Mae)
Bureau of Consumer Financial Protection	National Association of Consumer Credit Administrators
Bureau of the Fiscal Service – U.S. Department of the Treasury	National Credit Union Administration
Conference of State Bank Supervisors	North American Securities Administrators Association
Defense Innovation Unit Experimental (DIUx)	Office of the Comptroller of the Currency
Federal Communications Commission	U.S. Department of Homeland Security
Federal Deposit Insurance Corporation	U.S. Department of Housing and Urban Development
Federal Housing Administration	U.S. Commodity Futures Trading Commission
Federal Housing Finance Agency	U.S. Securities and Exchange Commission
Federal Trade Commission	

Non-United States

Bank of Canada	International Monetary Fund
Dutch National Bank	Monetary Authority of Singapore
European Commission	U.K. Financial Conduct Authority

**EXPERTS AND ADVOCATES**

Americans for Financial Reform	Mercatus Center at George Mason University
Autonomous NEXT	National Community Reinvestment Coalition
Bandman Advisors	National Consumer Law Center
CB Insights	Paul Hastings LLP
Center for Financial Services Innovation	Thomas W. Miller Jr., Mississippi State University College of Business
Center for Responsible Lending	U.S. Public Interest Research Group
David Yermack, New York University Stern School of Business	Urban Institute
Davis Polk & Wardwell LLP	Willkie Farr & Gallagher LLP
Delta Strategy Group	World Economic Forum
Marco Santori, Blockchain.com	
Michael Kitces, CFP	

**TRADE ASSOCIATIONS**

American Bankers Association	American Institute of Certified Public Accountants
American Financial Services Association	American Land Title Association

## Appendix A • Participants in the Executive Order Engagement Process

American Transaction Processors Coalition	MarketPlace Lending Association
CFA Institute	Money Service Business Association
Community Financial Services Association of America	Mortgage Bankers Association
Consumer Bankers Association	National Association of Auto Dealers
Consumer Financial Data Rights	National Association of Personal Financial Advisors
Electronic Transactions Association	National Association of Realtors
Financial Innovation Now	National Money Transmitters Association
Financial Planning Association	Network Branded Prepaid Card Association
Financial Services Centers of America	Online Lenders Alliance
Financial Services Information Sharing and Analysis Center	Real Estate Valuation Advocacy Association
Financial Services Roundtable	Receivables Management Association
Futures Industry Association	Securities Industry and Financial Markets Association
Global Financial Markets Association	Small Business Finance Association
Independent Community Bankers of America	Structured Finance Industry Group
International Swaps and Derivatives Association	The Appraisal Foundation
Investment Adviser Association	The Data Coalition
Investment Company Institute	U.S. Chamber of Commerce

FIRMS	
Ace Cash Express	BNP Paribas
Advance America	Capital One
Affirm	Charles Schwab & Co.
Ally	Chase Mortgage Servicing
Amazon	Citigroup
American Education Services/ PHEAA	CLS Bank
American Express	Coinbase
American Honda Finance Corporation	CommonBond
Andreessen Horowitz	Compass Point Research and Trading
Apple Pay	ConsenSys
Avant	CoreLogic
Bank of America	Credit Karma
Bayview Loan Servicing	Credit Suisse
BBVA	Cross River Bank
Better Mortgage	Depository Trust and Clearing Corporation
Betterment	DRW Venture Capital
Black Knight, Inc.	DV01
BlackRock/FutureAdvisor	E*TRADE
Blend	Early Warning
Bloom	Ellie Mae
Bloq	Encore Capital

## Appendix A • Participants in the Executive Order Engagement Process

Envestnet   Yodlee	Keefe, Bruyette & Woods
Experian North America	Lightspeed Venture Partners
Facebook	LeadsMarket
Fair Isaac Corporation (FICO)	LedgerX
Fannie Mae	Legal & General Investment Management America
Fay Servicing	Lend360
Fidelity Investments	Lending Club
Financial Engines	LoanCare
First Data	LoanDepot
FIS	Mastercard
Folio Investing	Microsoft Azure
Freddie Mac	Mid America Mortgage
FT Partners	MOHELA
Funding Circle	MoneyGram
Goldman Sachs	Moneytree
Google	Moody's
Great Lakes	Morgan Stanley
Intercontinental Exchange	Morningstar
Intercontinental Exchange/ MERSCORP	Mortgage Investors Group
Intuit	Mr. Cooper
Invesco	NASDAQ
JPMorgan Chase	Navient
Kabbage	Nelnet

## Appendix A • Participants in the Executive Order Engagement Process

NextCapital Group	TD Ameritrade
NOIC/Concord	The Clearing House Payments Company
Ocwen Financial	Toyota Financial Services
One Main Financial	TransUnion
Orchard Platform	Tricadia Capital
PayPal	TSYS
PeerIQ	Two Sigma Investments
PennyMac Financial Services	U.S. Bancorp
Plaid	United Income
PNC Financial	Upstart
Primary Residential Mortgage	Vanguard
Prosper	Veritec Solutions
Quicken Loans	Veros
R3	Viamerica
Ripple	Visa
S&P Global	Wealthfront
Select Portfolio Servicing	WebBank
Sequoia Capital	Wells Fargo Mortgage Servicing
Silicon Valley Bank	Western Asset Management
SoFi	Western Union
Square	WorldPay (Vantiv)
Stripe	ZestFinance
T. Rowe Price	



# **Appendix B**

## **Table of Recommendations**



# Table of Recommendations

## Embracing Digitization, Data, and Technology

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Digitization			
Telephone Consumer Protection Act (TCPA) and Fair Debt Collection Practices Act (FDCPA)			
Treasury recommends that the FCC continue its efforts to address the issue of unwanted calls through the creation of a reassigned numbers database. Treasury recommends that the FCC create a safe harbor for calls to reassigned numbers that provides callers a sufficient opportunity to learn the number has been reassigned.		FCC	F, G
Treasury recommends that the FCC provide clear guidance on reasonable methods for consumers to revoke consent under the TCPA. Congress should consider statutory changes to the TCPA to mitigate unwanted calls to consumers and provide for a revocation standard similar to that provided under the FDCPA.	Congress	FCC	A, F
Treasury recommends that the Bureau promulgate regulations under the FDCPA to codify that reasonable digital communications, especially when they reflect a consumer’s preferred method, are appropriate for use in debt collection.		Bureau	A, F
Consumer Financial Data			
Consumer Access to Financial Account and Transaction Data			
Treasury recommends that the Bureau affirm that for purposes of Section 1033, third parties properly authorized by consumers, including data aggregators and consumer fintech application providers, fall within the definition of “consumer” under Section 1002(4) of Dodd-Frank for the purpose of obtaining access to financial account and transaction data.		Bureau	A, F
Treasury recommends that regulators such as the SEC, Financial Industry Regulatory Authority, DOL, and state insurance regulators recognize the benefits of consumer access to financial account and transaction data in electronic form and consider what measures, if any, may be needed to facilitate such access for entities under their jurisdiction. However, Treasury recommends against further legislative action to expand the scope of Section 1033 at this time.	Congress	SEC, FINRA, DOL, State Insurance Regulators	A
Treasury recommends that the Bureau work with the private sector to develop best practices on disclosures and terms and conditions regarding consumers’ use of products and services powered by consumer financial account and transaction data provided by data aggregators and financial services companies. If necessary, the Bureau should consider issuing principles-based disclosure rules pursuant to its authority under Section 1032 of Dodd-Frank.		Bureau	A, F

## Appendix B • Table of Recommendations

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Treasury believes that consumers should have the ability to revoke their prior authorization that permits data aggregators and fintech applications to access their financial account and transaction data. Data aggregators and fintech applications should provide adequate means for consumers to readily revoke the prior authorization. If necessary, banking regulators and the SEC should consider issuing rules that require financial services companies to comply with a consumer request to limit, suspend, or terminate access to the consumer's financial account and transaction data by data aggregators and fintech applications.		FRB, FDIC, OCC, SEC	A, F
Treasury sees a need to remove legal and regulatory uncertainties currently holding back financial services companies and data aggregators from establishing data sharing agreements that effectively move firms away from screen-scraping to more secure and efficient methods of data access. Treasury believes that the U.S. market would be best served by a solution developed by the private sector, with appropriate involvement of federal and state financial regulators. A potential solution should address data sharing, security, and liability. Any solution should explore efforts to mitigate implementation costs for community banks and smaller financial services companies with more limited resources to invest in technology.		FRB, FDIC, OCC, SEC, FINRA, State Regulators	A
Treasury recommends that any potential solution discussed in the prior recommendation also address resolution of liability for data access. If necessary, Congress and financial regulators should evaluate whether federal standards are appropriate to address these issues.	Congress	FRB, FDIC, OCC, SEC, FINRA, State Regulators	A, F
Treasury recommends that any potential solution discussed in the prior recommendation address the standardization of data elements as part of improving consumers' access to their data. Any solution should draw upon existing efforts that have made progress on this issue to date. If necessary, Congress and financial regulators should evaluate whether federal standards are appropriate to address these issues.	Congress	FRB, FDIC, OCC, SEC, FINRA, State Regulators	A, F

## Appendix B • Table of Recommendations

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Treasury recommends that the banking regulators remove ambiguity stemming from the third-party guidance that discourages banks from moving to more secure methods of data access such as APIs.		FRB, FDIC, OCC, Bureau	A, F
To the extent that any additional regulation of data aggregation is necessary, Treasury recommends that it occur at the federal level by regulators that have significant experience in data security and privacy, and that will have, through legislation if necessary, broad jurisdiction to ensure equivalent treatment in the nonfinancial sector.	Congress		F, G
<b>Data Security and Breach Notification</b>			
Treasury recommends that Congress enact a federal data security and breach notification law to protect consumer financial data and notify consumers of a breach in a timely manner. Such a law should be based on the following principles: protect consumer financial data; ensure technology-neutral and scalable standards based on the size of an entity and type of activity in which the entity engages; recognize existing federal data security requirements for financial institutions; and employ uniform national standards that preempt state laws.	Congress		F, G
<b>Digital Legal Identity</b>			
Treasury recommends that financial regulators work with Treasury to enhance public-private partnerships to identify ways government can eliminate unintended or unnecessary regulatory and other barriers and facilitate the adoption of trustworthy digital legal identity products and services in the financial services sector. Treasury also recognizes that the development of digital legal identity products and services in the financial services sector should be implemented in a manner that is compatible with solutions developed across other sectors of the U.S. economy and government.		Treasury, FinCEN, FRB, FDIC, OCC, SEC, State Regulators	F
Treasury supports the efforts of OMB to fully implement the long-delayed U.S. government federated digital identity system. Treasury recommends policies that would restore a public-private partnership model to create an interoperable digital identity infrastructure and identity solutions that comply with NIST guidelines and would reinvigorate the role of U.S. government-certified private sector identity providers, promoting consumer choice and supporting a competitive digital identity marketplace.		OMB, GSA, Commerce	F

## Appendix B • Table of Recommendations

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
The Potential of Scale			
Cloud Technologies and Financial Services			
Treasury recommends that federal financial regulators modernize their requirements and guidance (e.g., vendor oversight) to better provide for appropriate adoption of new technologies such as cloud computing, with the aim of reducing unnecessary barriers to the prudent and informed migration of activities to the cloud. Specific actions U.S. regulators should take include: formally recognizing independent U.S. audit and security standards that sufficiently meet regulatory expectations; addressing outdated record keeping rules like SEC Rule 17a-4; clarifying how audit requirements may be met; setting clear and appropriately tailored chain outsourcing expectations; and providing staff examiners appropriate training to implement agency policy on cloud services.		FRB, FDIC, OCC, SEC, CFTC, SROs	D, F
Treasury recommends that a cloud and financial services working group be established among financial regulators so that cloud policies can benefit from deep and sustained understanding by regulatory authorities. Financial regulators should support potential policies by engaging key industry stakeholders, including providers, users, and others impacted by cloud services. U.S. financial regulators should seek to promote the use of cloud technology within the existing U.S. regulatory framework to help financial services companies reduce the risks of noncompliance as well as the costs associated with meeting multiple and sometimes conflicting regulations. Regulators should be wary of imposing data localization requirements and should instead seek other supervisory or appropriate technological solutions to potential data security, privacy, availability, and access issues.		Treasury, FRB, FDIC, OCC, SEC, CFTC, SROs	D, F
Big Data, Machine Learning, and Artificial Intelligence in Financial Services			
Regulators should not impose unnecessary burdens or obstacles to the use of AI and machine learning and should provide greater regulatory clarity that would enable further testing and responsible deployment of these technologies by regulated financial services companies as the technologies develop.		Federal and State Financial Regulators	D, F
Treasury recommends that financial regulators engage with the Select Committee on Artificial Intelligence, in addition to pursuing other strategic interagency AI efforts. Engagement in such efforts should emphasize use-cases and applications in the financial services industry, including removing regulatory barriers to deployment of AI-powered technologies.		Federal Financial Regulators	D, F

## Aligning the Regulatory Framework to Promote Innovation

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Modernizing Regulatory Frameworks for National Activities			
Improving the Clarity and Efficiency of Our Regulatory Frameworks			
Treasury supports state regulators' efforts to build a more unified licensing regime and supervisory process across the states. Such efforts might include adoption of a passporting regime for licensure. However, critical to this effort are much more accelerated actions by state legislatures and regulators to effectively reduce unnecessary inconsistencies across state laws and regulations to achieve much greater levels of harmonization. Treasury recommends that if states are unable to achieve meaningful harmonization across their licensing and supervisory regimes within three years, Congress should act to encourage greater uniformity in rules governing lending and money transmission to be adopted, supervised, and enforced by state regulators.	Congress	State Regulators	A, D, F
Treasury recommends that the OCC move forward with prudent and carefully considered applications for special purpose national bank charters. OCC special purpose national banks should not be permitted to accept FDIC-insured deposits, to reduce risks to taxpayers. The OCC should consider whether it is appropriate to apply financial inclusion requirements to special purpose national banks. The Federal Reserve should assess whether OCC special purpose national banks should receive access to federal payment services.		FRB, OCC	A, B, D, F

## Appendix B • Table of Recommendations

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
<p>Federal banking regulators should, in coordination, review current third-party guidance through a notice and comment process. U.S. banking regulators should further harmonize their guidance with a greater emphasis on (1) improving the current tailoring and scope of application of guidance upon third-party vendors to improve the efficiency of oversight and (2) enabling innovations in a safe and prudent manner. Such a review should specifically consider how to:</p> <ul style="list-style-type: none"> <li>• Further develop the framework to regulate bank partnerships with fintech lenders to apply strong and tailored regulatory oversight while also supporting efforts by banks, particularly smaller community banks, to partner with fintechs.</li> <li>• Provide greater clarity around the vendor oversight requirements for cloud service providers, including clarifying how third-party guidance should apply to a third-party's sub-contractors, like cloud service providers (i.e., fourth party vendors).</li> <li>• Support more secure methods for consumers to access their financial data, such as through API agreements between banks and data aggregators.</li> <li>• Identify common tools banks can leverage as part of due diligence efforts, such as robust independent audits, recognized certifications, and collaboration among institutions in an effort to enhance efficiencies and reduce costs.</li> <li>• Maintain ongoing efforts with other federal and state regulators to identify opportunities for harmonization as appropriate.</li> </ul> <p>Looking ahead and recognizing the dynamic nature of financial technology developments, the banking regulators should be prepared to flexibly adapt their third-party risk relationships framework to emerging technology developments in financial services. Moreover, banking regulators should consider how to make examiners' application of interagency guidance on third-party relationships more consistent across and within the agencies.</p>		FRB, FDIC, OCC	A, D, F, G
<p>Treasury recommends that the Federal Reserve consider how to reassess the definition of BHC control to provide firms a simpler and more transparent standard to facilitate innovation-related investments. This recommendation is consistent with public comments by Federal Reserve officials who have called for reassessing this issue. In addition, the banking regulators should interpret banking organizations' permitted scope of activities in a harmonized manner as permitted by law wherever possible and in a manner that recognizes the positive impact that changes in technology and data can have in the delivery of financial services.</p>		FRB, FDIC, OCC	A, D, F, G

## Updating Activity-Specific Regulations

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Lending and Servicing			
Marketplace Lending			
Treasury recommends that Congress codify the “valid when made” doctrine to preserve the functioning of U.S. credit markets and the long-standing ability of banks and other financial institutions, including marketplace lenders, to buy and sell validly made loans without the risk of coming into conflict with state interest rate limits. Additionally, the federal banking regulators should use their available authorities to address challenges posed by <i>Madden</i> .	Congress	FRB, FDIC, OCC	A, F
Treasury recommends that Congress codify that the existence of a service or economic relationship between a bank and a third party (including financial technology companies) does not affect the role of the bank as the true lender of loans it makes. Further, federal banking regulators should also reaffirm (through additional clarification of applicable compliance and risk-management requirements, for example) that the bank remains the true lender under such partnership arrangements.	Congress	FRB, FDIC, OCC	A, F
Treasury recognizes the role of state laws and oversight in protecting consumers, but such state regulation should not occur in a manner that hinders bank partnership models already operating in a safe and sound manner with appropriate consumer protections. Treasury recommends that states revise credit services laws to exclude businesses that solicit, market, or originate loans on behalf of a federal depository institution pursuant to a partnership agreement.		States	A, F
Mortgage Lending and Servicing			
Treasury recommends that Ginnie Mae pursue acceptance of eNotes and supports the measures outlined in its <i>Ginnie Mae 2020</i> roadmap to more broadly develop its digital capabilities.		HUD / Ginnie Mae	A, F
Treasury recommends Congress appropriate for FHA the funding it has requested for technology upgrades in the President’s Fiscal Year 2019 Budget – a portion of which FHA would use to improve the digitization of loan files. In addition, FHA, VA, and USDA should explore the development of shared technology platforms, including for certain origination and servicing activities.	Congress	HUD / FHA, VA / USDA	A, F
Treasury recommends the FHLBs explore ways to address their concerns regarding eNotes with the goal of accepting eNotes on collateral pledged to secure advances.		FHLBs	A, F
Treasury recommends that Congress revisit Title XI FIRREA appraisal requirements to update them for developments that have occurred in the market during the past thirty years. An updated appraisal statute should account for the development of automated and hybrid appraisal practices and sanction their use where the characteristics of the transaction and market conditions indicate it is prudent to do so.	Congress		A, F



## Appendix B • Table of Recommendations

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Treasury recommends FHA and other government loan programs develop enhanced automated appraisal capabilities to improve origination quality and mitigate the credit risk of overvaluation. These programs may also wish to consider providing targeted appraisal waivers where a high degree of property standardization and information about credit risk exists to support automated valuation, and where the overall risks of the mortgage transaction make such a waiver appropriate. Treasury supports legislative action where statutory changes are required to authorize granting limited appraisal waivers for government programs.	Congress	HUD / FHA, VA, USDA	A, F
Treasury further recommends that government loan programs explore opportunities to leverage industry-leading technology capabilities to reduce costs to taxpayers and accelerate adoption of new technology in the government-insured sector.		HUD / FHA, VA, USDA	A, F
Treasury recommends that states yet to authorize electronic and remote online notarization pursue legislation to explicitly permit the application of this technology and the interstate recognition of remotely notarized documents. Treasury recommends states align laws and regulations to further standardize notarization practices.		States	A, F
Treasury recommends Congress consider legislation to provide a minimum uniform standard for electronic and remote online notarizations.	Congress		A, F
Treasury recommends that recording jurisdictions yet to recognize and accept electronic records implement the necessary technology updates to process and record these documents and to pursue digitization of existing property records.		States	A, F
<p>To address the perception associated with the use of the FCA on mortgage loans insured by the federal government, Treasury recommends that HUD establish more transparent standards in determining which program requirements and violations it considers to be material to assist DOJ in determining which knowing defects to pursue. In doing so, Treasury recommends that:</p> <ul style="list-style-type: none"> <li>FHA clarify the remedies and liabilities lenders and servicers face, which could include, where appropriate, remedies such as indemnification and/or premium adjustments. Remedies should be correlated to the Defect Taxonomy.</li> <li>FHA should continue to review and refine its lender and loan certifications and its loan review system, including the Defect Taxonomy. Lenders that make errors deemed immaterial to loan approval should receive safe harbor from a denial of claim and forfeiture of premiums. Lenders should receive a similar safe harbor for material violations that are cured based on remedies prescribed by FHA absent patterns which indicate a systemic issue.</li> <li>HUD, in determining the appropriate remedies for violations of its program requirements, should consider the systemic nature of the problem, involvement or knowledge of the lender's senior management, overall quality of the originations of a specific lender, and whether or to what extent the loan defect may have impacted the incidence or severity of the loan default.</li> </ul>		HUD / FHA	F

## Appendix B • Table of Recommendations

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Treasury recommends that DOJ ensure that materiality for purposes of the FCA is linked to the standards in place at the agency administering the program to which the claim has been filed, and that DOJ and HUD work together to clarify the process by which mutual agreement is reached on the resolution of claims. Where a relator pursues <i>qui tam</i> action against a lender for a nonmaterial error or omission, DOJ, in consultation with HUD and FHA, should exercise its statutory authority to seek dismissal.		DOJ, HUD	F
Treasury recommends Congress consider appropriate remedial legislation if the recommended administrative actions are unsuccessful at achieving the desired result of increasing lender and servicer participation in federal mortgage programs.	Congress		F
Treasury recommends that federally supported mortgage programs explore standardizing the most effective features of a successful loss mitigation program across the federal footprint. Such standardization should broadly align a loss mitigation approach that facilitates effective and efficient loan modifications when in the financial interest of the borrower and investor, promotes transparency, reduces costs, and mitigates the impact of defaults on housing valuations during downturns.		FHFA / GSEs, HUD / FHA, VA, USDA	F
Treasury recommends HUD continue to review FHA servicing practices with the intention to increase certainty and reduce needlessly costly and burdensome regulatory requirements, while fulfilling FHA's statutory obligation to the Mutual Mortgage Insurance Fund (MMIF). In particular, Treasury recommends that FHA consider administrative changes to how penalties are assessed across FHA's multi-part foreclosure timeline to allow for greater flexibility for servicers to miss intermediate deadlines while adhering to the broader resolution timeline, as well as to better align with federal loss mitigation requirements now in place through the Bureau.		HUD / FHA	A, F
Treasury recommends FHA explore changes to its property conveyance framework to reduce costs and increase efficiencies by addressing the frequent and costly delays associated with the current process. As an additional measure, Treasury recommends that FHA continue to make appropriate use of, and consider expanding, programs which reduce the need for foreclosed properties to be conveyed to HUD, such as Note Sales and FHA's Claim Without Conveyance of Title.		HUD / FHA	A, F
Treasury recommends that states pursue the establishment of a model foreclosure law, or make any modifications they deem appropriate to an existing law, and amend their foreclosure statutes based on that model law.		States	A, F
Treasury recommends federally supported housing programs, including those administered by FHA, USDA, and VA, and the GSEs, explore imposing guaranty fee and insurance fee surcharges to account for added costs in states where foreclosure timelines significantly exceed the national average.		FHFA / GSEs, HUD / FHA, VA, USDA	A, F

## Appendix B • Table of Recommendations

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Treasury recommends that Ginnie Mae collaborate with FHFA, the GSEs, and the Conference of State Bank Supervisors to expand and align standard, detailed reporting requirements on nonbank counterparty financial health, including terms and covenants associated with funding structures, to provide confidence that taxpayers are protected during a period of severe market stress.		HUD / Ginnie Mae, FHFA / GSEs, CSBS	B
Treasury supports Ginnie Mae's consideration of enhancing its counterparty risk mitigation approach, including through the imposition of stress testing requirements that can provide information on the financial health of servicer counterparties across an economic cycle.		HUD / Ginnie Mae	B
Treasury recommends Ginnie Mae have sufficient flexibility to charge guaranty fees appropriate to cover additional risk arising from changes in the overall market or at the program level.	Congress		B
Treasury recommends a comprehensive assessment of Ginnie Mae's current staffing and contracting policies, including the costs and benefits of alternative pay and/or contracting structures. Ginnie Mae would be better equipped to manage its program and monitor counterparty risk if it were able to more readily attract personnel with requisite expertise by paying salaries comparable to those at other financial agencies with premium pay authority. Additionally, being able to adopt similar contracting procedures as other agencies that are outside of federal acquisition statutes and regulations would enable Ginnie Mae to more effectively monitor and respond to changing market conditions and needs. However, any change to Ginnie Mae's personnel or contracting policies should be informed by a comprehensive assessment of current challenges. The potential benefits of alternative pay and/or contracting structures should be weighed against the additional federal costs that would be incurred.	Congress	HUD / Ginnie Mae	B
<b>Student Lenders and Servicers</b>			
Education should establish guidance on minimum standards specifying how servicers should handle decisions with significant financial implications (e.g., payment application across loans, prioritizing repayment plans, and use of deferment and forbearance options), minimum contact requirements, standard monthly statements, and timeframes for completing certain activities (e.g., processing forms or correcting specific account issues). Treasury applauds the required use of Education branding on servicing materials in the new Direct Loan servicing procurement to reduce borrower confusion.		ED	F
In Education's new Direct Loan Servicing contract, Education should require student loan servicers to make greater use of emails and provide guidance to servicers on how to use email appropriately to balance privacy and security concerns with the need for effective and timely communication. All emails sent to federal student loan borrowers should provide enough information for borrowers to easily discern whether action must be taken on their account.		ED	A, F

## Appendix B • Table of Recommendations

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Education should contract with providers of secure e-signature software and cloud technology for use by federal student loan servicers on all forms.		ED	F
Education's Office of Federal Student Aid should include in its management team individuals with significant expertise in managing large consumer loan portfolios.		ED	B, F
Education should take steps to address existing data quality issues to better monitor and manage portfolio performance. Education should increase transparency by publishing greater portfolio performance data, servicer performance data, and cost estimation analysis on its website to give stakeholders greater insight into Education's management of the taxpayer investment in higher education.		ED	B, F
Treasury supports legislative efforts to implement a risk-sharing program for institutions participating in the federal student loan program based on the amount of principal repaid following five years of payments. Schools whose students have systematically low loan repayment rates should be required to repay small amounts of federal dollars in order to protect taxpayers' growing investment in the federal student loan program. Congress should consider how to address schools with systematically low repayment rates but large populations of disadvantaged students.	Congress	ED	F
<b>Short-Term, Small-Dollar Installment Lending</b>			
Treasury recognizes and supports the broad authority of states that have established comprehensive product restrictions and licensing requirements on nonbank short-term, small-dollar installment lenders and their products. As a result, Treasury believes additional federal regulation is unnecessary and recommends the Bureau rescind its Payday Rule.		Bureau	F, G
Treasury recommends the federal and state financial regulators take steps to encourage sustainable and responsible short-term, small-dollar installment lending by banks. Specifically, Treasury recommends that the FDIC reconsider its guidance on direct deposit advance services and issue new guidance similar to the OCC's core lending principles for short-term, small-dollar installment lending.		FRB, FDIC, OCC, Bureau, State Financial Regulators	A, D, F
<b>Debt Collection</b>			
Treasury recommends the Bureau establish minimum effective federal standards governing the collection of debt by third-party debt collectors. Specifically, these standards should address the information that is transferred with a debt for purposes of debt collection or in a sale of the debt. Further, the Bureau should determine whether the existing FDCPA standards for validation letters to consumers should be expanded to help the consumer assess whether the debt is owed and determine an appropriate response to collection attempts. Treasury does not support broad expansion of the FDCPA to first-party debt collectors absent further Congressional consideration of such action.		Bureau	F, G

## Appendix B • Table of Recommendations

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
IRS Income Verification			
It is important that IRS update its income verification system to leverage a modern, technology-driven interface that protects taxpayer information and enables automated and secure data sharing with lenders or designated third parties. Treasury recommends Congress fund IRS modernization, which would include upgrades that will support more efficient income verification.	Congress	Treasury	D, F, G
New Credit Models and Data			
Treasury recognizes that these new credit models and data sources have the potential to meaningfully expand access to credit and the quality of financial services. Treasury, therefore, recommends that federal and state financial regulators further enable the testing of these newer credit models and data sources by both banks and nonbank financial companies.		Federal and State Financial Regulators	A, D
Regulators, through interagency coordination wherever possible, should tailor regulation and guidance to enable the increased use of these models and data sources by reducing uncertainties. In particular, regulators should provide regulatory clarity for the use of new data and modeling approaches that are generally recognized as providing predictive value consistent with applicable law for use in credit decisions.		Federal and State Financial Regulators	D, F, G
Regulators should in general be willing to recognize and value innovation in credit modelling approaches. Regulators should enable prudent experimentation with the aim of working through various issues raised, which may in turn require new approaches to supervision and oversight.		Federal and State Financial Regulators	D, F, G
Credit Bureaus			
The FTC should retain its rulemaking and enforcement authority for nonbank financial companies under the GLBA. Additionally, Treasury recommends that the relevant agencies use appropriate authorities to coordinate regulatory actions to protect consumer data held by credit reporting agencies and that Congress continue to assess whether further authority is needed in this area.	Congress	FTC, Bureau	F, G
Treasury recommends that Congress amend CROA to exclude the national credit bureaus and national credit scorers (i.e., credit scoring companies utilized by financial institutions when making credit decisions) from the definition of “credit repair organization” in CROA.	Congress		F, G
InsurTech			
Lawmakers, policymakers, and regulators should take coordinated steps to encourage the development of innovative insurance products and practices in the United States. Domestically, this includes consideration of improving product speed to market, creating increased regulatory flexibility, and harmonizing inconsistent laws and regulations.	Congress	Federal and State Financial Regulators	F, G

## Appendix B • Table of Recommendations

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Treasury's Federal Insurance Office, which provides insurance expertise in the federal government, should work closely with state insurance regulators, the NAIC, and federal agencies on InsurTech issues.		Treasury, Insurance Regulators, NAIC	F, G
<b>Payments</b>			
<b>Money Transmitters</b>			
Treasury supports the Bureau's ongoing efforts to reassess Regulation E. Treasury recommends that the Bureau provide more flexibility regarding the issuance of Regulation E disclosures and raise the current 100 transfer per annum threshold for applicability of the de minimis exemption.		Bureau	A, C, F, G
<b>Faster Payments</b>			
Treasury recommends that the Federal Reserve set public goals and corresponding deadlines consistent with the overall conclusions of the Faster Payments Task Force's final report.		FRB	C, D, F
Treasury recommends that the Federal Reserve move quickly to facilitate a faster retail payments system, such as through the development of a real-time settlement service, that would also allow for more efficient and ubiquitous access to innovative payment capabilities. In particular, smaller financial institutions, like community banks and credit unions, should also have the ability to access the most-innovative technologies and payment services.		FRB	C, D
<b>Secure Payments</b>			
Treasury recommends that continued work in the area of payment security include an actionable plan for future work, and ensure that solutions, especially in security, do not include specific tech mandates.		FRB, Treasury, Federal Financial Regulators	D, F
<b>Wealth Management and Digital Financial Planning</b>			
Treasury believes that appropriate protection for clients of financial planners, digital and otherwise, can be achieved without imposing either a fragmented regulatory structure or creating new regulatory entities. Treasury recommends that an appropriate existing regulator of a financial planner, whether federal or state, be tasked as the primary regulator with oversight of that financial planner and other regulators should exercise regulatory and enforcement deference to the primary regulator. To the extent that the financial planner is providing investment advice, the relevant regulator will likely be the SEC or a state securities regulator.		SEC, FINRA, DOL, Bureau, FRB, OCC, FDIC, State Regulators	A, F, G

## Enabling the Policy Environment

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Agile and Effective Regulation for a 21st Century Economy			
Regulatory Sandboxes			
Treasury recommends that federal and state financial regulators establish a unified solution that coordinates and expedites regulatory relief under applicable laws and regulations to permit meaningful experimentation for innovative products, services, and processes. Such efforts would form, in essence, a “regulatory sandbox” that can enhance and promote innovation. If financial regulators are unable to fulfill those objectives, however, Treasury recommends that Congress consider legislation to provide for a single process consistent with the principles detailed in the report, including preemption of state laws if necessary.	Congress	Federal and State Financial Regulators, SROs	D, F, G
Agile Regulation			
Treasury recommends that Congress enact legislation authorizing financial regulators to use other transaction authority for research and development and proof-of-concept technology projects. Regulators should use this authority to engage with the private sector to better understand new technologies and innovations and their implications for market participants, and to carry out their regulatory responsibilities more effectively and efficiently.	Congress	Federal Financial Regulators	D, F
Treasury encourages regulators to appropriately tailor regulations to ensure innovative technology companies providing tools to regulated financial services companies can continue to drive technological efficiencies and cost reductions. Treasury encourages regulators to seek out and explore innovative partnerships with financial services companies and regtech firms alike to better understand new technologies that have the potential to improve the execution of their own regulatory responsibilities more effectively and efficiently.		Federal and State Financial Regulators	D, F
Treasury recommends that financial regulators pursue robust engagement efforts with industry and establish clear points of contact for industry and consumer outreach. Treasury recommends that financial regulators increase their efforts to bridge the gap between regulators and start-ups, including efforts to engage in different parts of the country rather than requiring entities to come to Washington, D.C.		Federal and State Financial Regulators, SROs	D, F, G
Treasury recommends that financial regulators periodically review existing regulations as innovations occur and new technology is developed and determine whether such regulations fulfill their original purpose in the least costly manner.		Federal and State Financial Regulators, SROs	D, F, G

## Appendix B • Table of Recommendations

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Treasury recommends that financial regulators engage at both the domestic and international levels, as financial technology in many cases is borderless. Treasury encourages international initiatives by financial regulators to increase their knowledge of fintech developments in other nations.		Federal Financial Regulators	D, E, F
<b>Critical Infrastructure</b>			
Treasury recommends that financial regulators thoroughly consider cybersecurity and other operational risks as new technologies are implemented, firms become increasingly interconnected, and consumer data are shared among a growing number of firms, including third parties.		Federal and State Financial Regulators, SROs	B, C, D, F
Treasury recommends that the FBIIC consider establishing a technology working group charged with better understanding the technologies that firms are increasingly relying upon, and staying well-informed regarding innovation taking place within the sector.		FBIIC	F, G
Treasury commits to leading a multiyear program with the financial services industry to identify, properly protect, and remediate vulnerabilities.		Treasury	F, G
<b>International Approaches and Consideration</b>			
<b>International Engagement</b>			
Treasury recommends continued participation by relevant experts in international forums and standard-setting bodies to share experiences regarding respective regulatory approaches and to benefit from lessons learned. Treasury will work to ensure actions taken by international organizations align with U.S. national interests and the domestic priorities of U.S. regulatory authorities.		Federal Financial Regulators, Treasury	D, E
Treasury and U.S. financial regulators should engage with the private sector with respect to ongoing work programs at international bodies to ensure regulatory approaches are appropriately calibrated.		Federal Financial Regulators, Treasury	D, E
Treasury and U.S. financial regulators should proactively engage with international organizations to ensure that they are adhering to their core mandates.		Federal Financial Regulators, Treasury	D, E



# **Appendix C**

## **Additional Background**



# Additional Background

## Payments

### **Credit Card Networks**

There are four predominant credit card networks in the United States that function through two different business models. These networks and business models were started, built, and remain as private-sector solutions that continue to be largely governed by private agreements instead of government mandates. The first model, a decentralized “open-loop” model of networks (e.g., Visa and Mastercard), began as associations that were jointly owned by banking institutions, but today are public companies. In this model, banks control the relationships with customers by issuing credit cards to consumers and signing up merchants for acquirer relationships. In this sense, the network is essentially a clearinghouse that facilitates acceptance and transaction routing for a fee; the banks generally set terms with their individual and business customers through contract.

Open-loop networks maintain their own rulebooks and limit their membership to licensed and regulated financial institutions. For example, in the United States, a member is required to be a depository institution or a chartered limited purpose national bank; in Europe, a member is required to be either a depository institution or a Payment Service Provider licensed under the Payment Services Directive.<sup>540</sup> The difference in licensing and chartering of various types of financial firms between the United States and other jurisdictions is a factor in the breadth of direct access to payment networks. Other jurisdictions such as the United Kingdom and India allow for a specialty kind of payment firm to be licensed and regulated by the Financial Conduct Authority<sup>541</sup> or Reserve Bank of India,<sup>542</sup> respectively. Such a licensing regime creates a regulatory framework for nondepository institutions that sets eligibility requirements for potential card network access.<sup>543</sup> However, these are baseline institutional eligibility criteria, and membership is not guaranteed just because such criteria are met — the card networks also have additional requirements and standards that must be met, such as having an effective AML regime.

The second model is a more centralized “closed-loop” structure (e.g., American Express and Discover). These firms, which also maintain their own rulebooks, are bank holding companies that run the payment network and control customer relationships by issuing cards and contracting with

---

540. See Visa, *Visa Europe Membership* (2015), at 4, available at: [https://www.visaeurope.com/media/images/44959\\_visa\\_membership\\_access\\_a4\\_pdf-73-25878.pdf](https://www.visaeurope.com/media/images/44959_visa_membership_access_a4_pdf-73-25878.pdf).

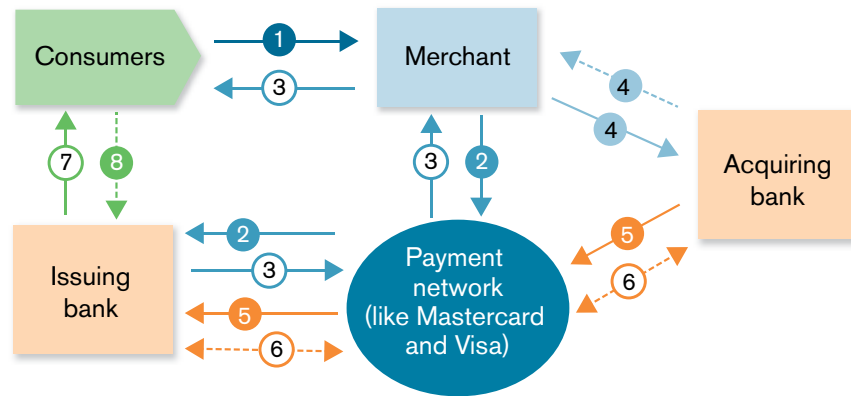
541. See Financial Conduct Authority, *Authorisation and Registration: E-money and Payment Institutions* (last updated Mar. 23, 2018), available at: <https://www.fca.org.uk/firms/authorisation-registration-emonney-payment-institutions>.

542. Reserve Bank of India, *Press Release—RBI Releases Guidelines for Licensing of Payments Banks* (Nov. 27, 2014), available at: [https://rbi.org.in/scripts/BS\\_PressReleaseDisplay.aspx?prid=32615](https://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=32615).

543. U.S. law allows the OCC to charter a special purpose credit card national bank, including a version that is exempt from requirements of the Bank Holding Company Act. This charter is only for banks whose predominant business is credit cards. See Office of the Comptroller of the Currency, *Comptroller's Licensing Manual: Charters* (Sept. 2016), at 51–54, available at: <https://www.occ.treas.gov/publications/publications-by-type/licensing-manuals/charters.pdf>. This charter is not common. As of March 31, 2018, only nine such bank charters were active. Office of the Comptroller of the Currency, *Credit Card Banks Active As of 3/31/2018*, available at: <https://www.occ.treas.gov/topics/licensing/national-banks-fed-savings-assoc-lists/credit-card-by-name-pdf.pdf>.

merchants themselves.<sup>544</sup> The open-loop networks authorize and clear the majority of credit card transactions. The open-loop, four-party credit card network model is illustrated below.

Figure C1: Credit Card Networks



- 1 The consumer pays a merchant with a credit card
- 2 The merchant then electronically transmits the data through the applicable Association's electronic network to the issuing bank for authorization
- 3 If approved, the merchant receives authorization to capture the transaction, and the cardholder accepts liability, usually by signing the sales slip
- 4 The merchant receives payment, net of fees, by submitting the captured credit card transactions to its bank (the acquiring bank) in batches or at the end of the day
- 5 The acquiring bank forwards the sales draft data to the applicable Association, which in turn forwards the data to the issuing bank.  
The Association determines each bank's net debit position. The Association's settlement financial institution coordinates issuing and acquiring settlement positions. Members with net debit positions (normally the issuing banks) send funds to the Association's settlement financial institution, which transmits owed funds to the receiving bank (generally the acquiring banks).
- 6 The settlement process takes place using a separate payment network such as Fedwire
- 7 The issuing bank presents the transaction on the cardholder's next billing statement
- 8 The cardholder pays the bank, either in full or via monthly payments

Source: Federal Deposit Insurance Corporation, *Risk Management Examination Manual for Credit Card Activities* (2007), at 165.

American Express and Discover, as bank holding companies, are subject to supervision and oversight by the Federal Reserve (and the banking regulator with jurisdiction over their banking subsidiaries) and the full suite of banking regulations. Visa and Mastercard are subject to regulation through the Bank Service Company Act as third-party service providers to banking organizations.

544. American Express and Discover now license their brands for issuance by other banking institutions in certain cases.

### Debit Card Networks

Debit card networks are similar to credit card networks in that they are all private entities that maintain their own rules, regulations, and fee structures through private agreements and industry standards. Debit card networks are distinct in that they process a different type of transaction. Credit cards underlie a loan account with a bank — in authorizing the transaction, the card network is asking if the bank wants to approve addition to an open line of credit. Debit cards are attached to a pre-funded bank account — in authorizing the transaction, the card network is, in essence, asking the bank if sufficient funds are available for payment.<sup>545</sup>

There are two different types of debit networks in the United States: signature debit<sup>546</sup> and PIN debit.<sup>547</sup> Whereas all debit networks generally function as four-party systems (like the credit card networks) the infrastructure differs slightly between signature and PIN networks. Signature debit uses the credit card network infrastructure, and thus requires a “dual-message” — one message for authentication and one message for clearing. PIN debit, which evolved from ATM networks, uses a “single-message” authentication and clearing method whereby all the information is transmitted in one message.<sup>548</sup> This affects the speed of clearance and settlement between the two types of networks. Dual-message transactions are stored and then combined in a batch that is sent all at one time to the network providers. This is typically done once a day, but depending on merchant volume could be done more or less frequently. Single-message transactions have all the information necessary to clear the transaction at the time of authentication, with no need for batching or separate clearance. For both network types, there is only one settlement cutoff time, which is when funds are moved and interchange fees are determined. The speed at which this process is completed varies from same day for single-message, and upward of two days for dual-message.<sup>549</sup>

Signature debit networks generally charge higher interchange fees than PIN debit networks. According to the Federal Reserve, for all transactions for year-end 2016, the average interchange fees per transaction were for signature debit \$0.33 (0.89% of average transaction value), and for PIN debit \$0.24 (0.64% of average transaction value).<sup>550</sup> Signature debit networks are owned by the branded credit card networks whose logo is shown on the front of a debit card. PIN debit networks are owned both by credit card networks as well as merchant processors that provide back-end service; they are listed on the reverse side of a debit card.

545. This represents the basic structure of the transactions. Nuances may exist, for instance, banks may allow customers to overdraw, or let the balance go below zero on their bank accounts.

546. Signature debit networks: Visa, Mastercard, and Discover.

547. PIN debit networks (parent company): ACCEL (Fiserv), AFFN (FIS), ATH (Evertec), Credit Union 24 (Credit Union co-op), Interlink (Visa), Jeanie (Vantiv), Maestro (Mastercard), NetWorks, NYCE (FIS), PULSE (Discover), SHAZAM (member owned), STAR (First Data), and China UnionPay.

548. Debit Card Interchange Fees and Routing (June 30, 2011) [76 Fed. Reg. 43394, 43395 (July 20, 2011)].

549. Susan Herbst-Murphy, *Clearing and Settlement of Interbank Card Transactions: A MasterCard Tutorial for Federal Reserve Payments Analysts*, Federal Reserve Bank of Philadelphia Discussion Paper (2013), at 7-13, 22, available at: <https://www.philadelphiafed.org/-/media/consumer-finance-institute/payment-cards-center/publications/discussion-papers/2013/D-2013-October-Clearing-Settlement.pdf>.

550. Board of Governors of the Federal Reserve System, *Average Debit Card Interchange Fee by Payment Card Network* (last updated July 14, 2017), available at: <https://www.federalreserve.gov/paymentsystems/regii-average-interchange-fee.htm>.

Regulation of debit cards and credit cards is different. While both types of card transaction are regulated for consumer protection purposes, the rules derive from different statutes<sup>551</sup> and the implementing regulations<sup>552</sup> are codified separately. In some cases, these two regulations may have similar requirements that are implemented differently due to the nature of the product, such as consumer disclosures. Other requirements may be completely distinct, like the Durbin Amendment's application solely for debit cards.<sup>553</sup> And yet other requirements may be superseded by stricter contractual requirements imposed by the card networks, such as the card networks' requirement that all unauthorized card transactions carry zero liability for the cardholder.<sup>554</sup>

As for usage, debit cards see higher transaction volumes and values than credit cards. This disparity has been true for more than a decade and the popularity of debit cards in relation to credit cards continues to grow.

Figure C2: Total Number of Card Payments (billions) and Value (\$ trillions)

	2015		2016	
	Number	Value	Number	Value
<b>Total card payments</b>	<b>103.5</b>	<b>5.65</b>	<b>111.1</b>	<b>5.98</b>
<b>Debit cards</b>	<b>69.6</b>	<b>2.56</b>	<b>73.8</b>	<b>2.7</b>
<b>Non-prepaid</b>	<b>59</b>	<b>2.27</b>	<b>63</b>	<b>2.41</b>
In person	49.5	1.58	52.1	1.66
Chip	0.4	0.02	8.4	0.37
No chip	49.1	1.56	43.7	1.29
Remote	9.5	0.69	10.9	0.75
<b>Prepaid</b>	<b>10.6</b>	<b>0.3</b>	<b>10.7</b>	<b>0.29</b>
General purpose	4.3	0.15	4.4	0.15
In person	3.6	0.1	3.6	0.1
Chip	0	0	0.1	0.01
No chip	3.6	0.1	3.5	0.1
Remote	0.8	0.05	0.8	0.05
Private label	3.6	0.07	3.8	0.07
Electronic benefits transfers (EBT)	2.6	0.08	2.5	0.07
<b>Credit cards</b>	<b>33.9</b>	<b>3.08</b>	<b>37.3</b>	<b>3.27</b>
General purpose	31	2.8	34.3	3
In person	21.7	1.3	23.4	1.36
Chip	1	0.08	6.6	0.47
No chip	20.7	1.22	16.8	0.89
Remote	9.3	1.5	10.9	1.64
Private label	2.8	0.28	3.1	0.27

Source: Federal Reserve System, *The Federal Reserve Payments Study - 2017 Annual Supplement*.

551. Credit cards: Truth in Lending Act, 15 U.S.C. § 1601 et seq.; Debit cards: Electronic Fund Transfer Act, 15 U.S.C. § 1693 et seq.

552. Credit cards: Regulation Z, 12 C.F.R. § 1026 et seq.; Debit cards: Regulation E, 12 C.F.R. § 1005 et seq.

553. 15 U.S.C. § 1693o-2.

554. See Visa, *Visa Core Rules and Visa Product and Service Rules*, Rule 1.4.6.1 (updated Oct. 2017), available at: <https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf>.

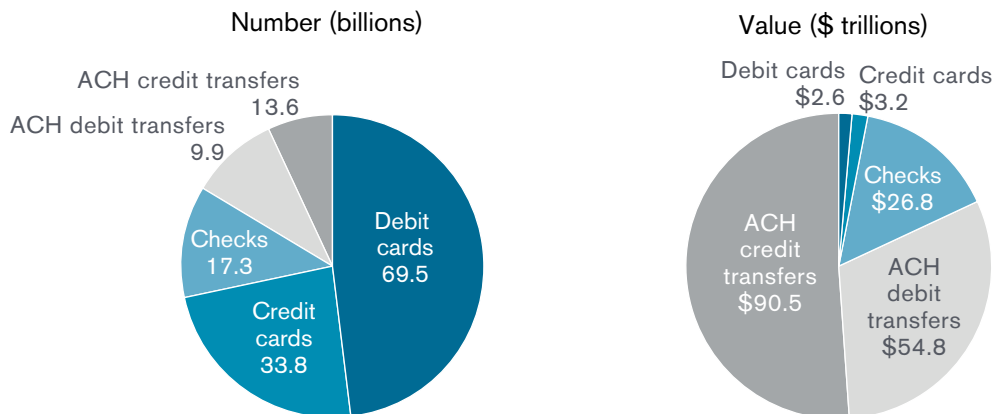
Access to card networks in the United States is largely set by private agreement and the system includes controls that ensure that each firm with direct access has a comprehensive and robust regulatory framework in place. Treasury believes that this system is working well and has supported innovative new solutions in the payments space. Treasury supports the private card networks' continual evaluation of their rulebooks in light of new entrants and innovations to the payments infrastructure to ensure that the systems continue to work well for all involved players.

### **Automated Clearing House (ACH)**

The ACH network<sup>555</sup> is at the core of the payments system as one of the chief payment systems in the United States. It is a system that processes payments and moves money between financial institutions. There are currently two network operators, Electronic Payments Network and FedACH (owned by the Federal Reserve Banks). The ACH system is used for payments such as: direct deposit, government benefits delivery, bill pay, and transfers between consumers and businesses, among others. The rules for ACH networks are set by NACHA — a private, not-for-profit, industry association. Importantly, by rule, only insured depository institutions are allowed access to the ACH networks.

According to NACHA, in 2017 ACH networks processed approximately 21.5 billion transactions with a total value of about \$46.8 trillion.<sup>556</sup> An originator — which could be an individual or an entity — first provides payment instructions that then enter the banking system. ACH

Figure C3: Distribution of Core Noncash Payments by Type for 2015



Note: Debit card includes non-prepaid debit, general-purpose prepaid, private-label prepaid, and electronic benefit transfers. Credit card includes general purpose and private label. Check, automated clearinghouse (ACH) credit transfers, and ACH debit transfers include interbank and on-us.

Source: Federal Reserve System, *The Federal Reserve Payments Study 2016*, at 3.

555. See generally NACHA, *ACH Network: How It Works*, available at: <https://www.nacha.org/ach-network>.

556. NACHA, *2017 ACH Network Volume & Value*, available at: [https://www.nacha.org/system/files/resources/ACH-Network-Volume-and-Value-2017\\_2.pdf](https://www.nacha.org/system/files/resources/ACH-Network-Volume-and-Value-2017_2.pdf).

payments are processed in batches by banks — the originating financial institution aggregates payment information into batches before sending to the two network operators who then net and route payments to receiving financial institutions. ACH payments can be either debit (pull)<sup>557</sup> or credit (push)<sup>558</sup> payments. Debit payments settle in one day while credit payments settle in one to two days. In 2015, ACH transferred the highest value of payments among retail payment options.

### **Wire Transfer Services**

Wire transfer services are systems that are primarily used for large value, wholesale payments between banks and businesses. In the United States, there are two primary wire service networks that operate domestically — Fedwire and CHIPS. Fedwire is owned and operated by the Federal Reserve Banks; CHIPS is a competing private sector network with 50 direct bank participants.<sup>559</sup> Unlike the ACH networks, the wire networks' operating rules are set by the operators themselves.

Fedwire is a real time gross settlement service that clears and settles transactions immediately. In 2017, Fedwire processed over 150 million transactions with a total value of over \$740 trillion; the average Fedwire transaction value was \$4.85 million.<sup>560</sup> In comparison, CHIPS is a real-time final settlement system that matches, nets, and settles payments. In order to function in real time, member banks must prefund (using Fedwire) a joint CHIPS account at the New York Federal Reserve Bank. In 2017, CHIPS processed over 112 million transactions with a total value of over \$393 trillion; the average CHIPS transaction value was \$3.49 million.<sup>561</sup>

### **Checks and Cash**

Checks and cash are two other ways to make payments. Checks are cleared in one of five ways:<sup>562</sup> (1) clearing “on-us” checks internally on a bank’s own books; (2) presenting checks directly to the paying bank; (3) forwarding checks to a correspondent bank; (4) exchanging checks through a private clearinghouse; (5) forwarding checks to the Federal Reserve for processing. Today, nearly all of the checks that the Federal Reserve processes are electronic images of the paper checks.

557. For example, when a consumer pays a utility bill by authorizing the utility company to pull the payment from his or her bank account. This could be done by visiting the company’s website to input payment information, for instance.

558. For example, when a consumer logs on to his or her bank’s online banking portal and schedules an online bill pay transaction that the bank will then push to the payee.

559. See Fedwire at <https://www.frb services.org/financial-services/wires/index.html> and CHIPS at <https://www.theclearinghouse.org/payment-systems/chips>.

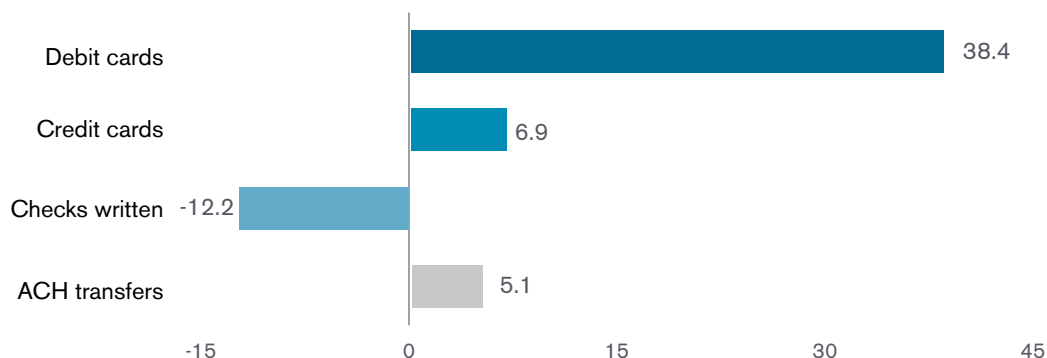
560. Board of Governors of the Federal Reserve System, *Fedwire Funds Service – Annual* (2018), available at: [https://www.federalreserve.gov/paymentsystems/files/fedfunds\\_ann.pdf](https://www.federalreserve.gov/paymentsystems/files/fedfunds_ann.pdf).

561. The Clearing House, *Annual Statistics from 1970 to 2018* (2018), available at: <https://www.theclearinghouse.org/-/media/tch/pay%20co/chips/reports%20and%20guides/chips%20volume%20through%20jan%202018.pdf>.

562. Federal Reserve Bank of New York, *Check Processing* (Mar. 2013), available at: <https://www.newyorkfed.org/aboutthefed/fedpoint/fed03.html>.

Check usage has been declining since the 1990s and continues to decline.

Figure C4: Changes in the Number of Consumer Noncash Payments Per Household, Per Month, 2000-2015

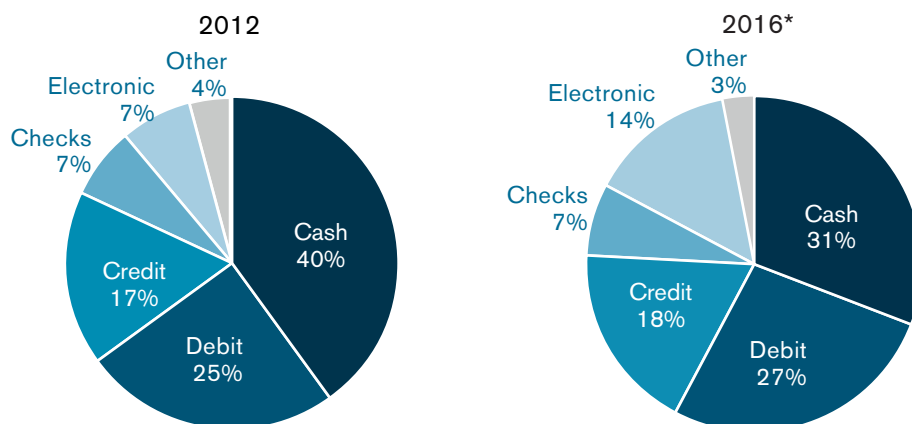


Note: ACH is automated clearinghouse. Debit card includes non-prepaid debit, general-purpose prepaid, and private-label prepaid (including electronic benefits transfers). Credit card includes general purpose and private label.

Source: Federal Reserve System, *The Federal Reserve Payments Study 2016*, at 4.

Cash is still the most frequently used payment method, however, its share of total payments is declining.

Figure C5: Transactions by Each Payment Instrument (percent)



Source: Diaries of Consumer Payment Choice, 2012 and 2016, Federal Reserve Bank of Boston.

\* This pie chart differs from the chart in the 7/31/18 version of the Nonbank Financials, Fintech, and Innovation Report. The previous pie chart used data from the 2017 Survey of Consumer Payment Choice and has been replaced with data from the 2016 Diary of Consumer Payment Choice to match the methodology and data source used for the pie chart depicting transactions in 2012.

## Other Payments Players

In addition to the core payment systems that connect financial institutions with other financial institutions, there are a number of nonbank firms that serve as intermediaries and layer between the banking system and the ultimate end user. In some cases, other intermediaries may also layer on top or beside these intermediate firms to provide a specific or supplementary specialty service (such as tokenization, for example), which adds to the complexity of the payments system. This



section provides only a brief, high-level overview of the general categories of players in this space. While not always the most well-known, these firms provide crucial services to connect end users.

### **Nonbank Payment Processors**

Payment processors are generally nonbank technology companies that provide vendor services to bank clients by processing electronic payments. These firms specialize in processing card payments on both sides of a transaction — as merchant acquirer and/or issuer processor. Some banks process their own payments in-house; some banks enter into a co-owned joint venture with a payment processor, whereby the processor supplies the technology to process payments and the bank maintains the merchant relationships; many banks wholly outsource the processing function to a third-party processor.<sup>563</sup> The role of processors in the payments ecosystem is best understood through the outsourcing model. Here, the processor in essence stands in the shoes of the acquiring bank and/or the issuing bank during the authorization, routing, and clearing of card transactions.<sup>564</sup>

Since payment processors are nonbank institutions, they must have a bank sponsor in order to access the card networks. Processors must follow the rules of the card networks, and are examined regularly by the networks. Processors are also examined by the banking agencies through uniform FFIEC guidance under the bank regulators' Bank Service Company Act authorities; however as these authorities regulate the third-party and vendor services that are provided to the bank, the bank sponsors are generally responsible for the processors' conduct when processing on the card networks.

Payment processing is a very competitive business that is largely driven by the firm that can charge the lowest fees. Processors themselves have diversified and tried to gain a competitive advantage by engaging in related businesses that include products and services such as: prepaid cards, PIN debit network ownership, providing hardware (such as payment terminals), and providing software solutions for small businesses (such as for accounts and inventory management, etc.).

### **Payment Service Providers (PSPs)**

Technology has allowed new entrants to enter the business of accepting and processing merchant's and consumer's point of sale or online/mobile payments. In many cases, these firms are serving small businesses who may not have merchant relationships with banks, or compete with bank services through the quality of the software and user experience. PSPs are generally nonbank technology companies that are responding to customer demand for faster, more convenient services for both end users and merchants.

While PSPs provide merchants, for example, with a way to accept and process payments, they do not directly compete with traditional payment processors — instead they function as yet another

563. Office of the Comptroller of the Currency, *Merchant Processing, Comptroller's Handbook* (Aug. 2014), at 2-5, available at: <https://www.occ.treas.gov/publications/publications-by-type/comptrollers-handbook/merchant-processing/pub-ch-merchant-processing.pdf>.

564. See, e.g., First Data Corporation, *Form 10-K Annual Report* (Feb. 20, 2018), at 6-7, available at: <https://www.sec.gov/Archives/edgar/data/883980/000088398018000006/a12311710-k.htm>.

layer.<sup>565</sup> As nonbank entities, PSPs also do not have direct access to the payment infrastructure and therefore must have a business relationship with a bank. There may also be a traditional nonbank payment processor between these firms and their bank for payment processing purposes. Since PSPs layer on top of the existing payments infrastructure, they are disrupters more on the front-end consumer-facing side of user experience than on the back-end processes affecting the ultimate movement of money.

PSPs, like payment processors, must adhere to the rules of the card networks, even if they rely on banks and payment processors to process transactions through the system. To be a service provider for a card network, a firm generally must register with the card network, ensure that they are PCI-DSS compliant, and be examined annually by the card network.<sup>566</sup> Additionally, PSPs are generally licensed money transmitters and are therefore subject to the applicable licensing, registration, and oversight requirements in multiple jurisdictions.

---

565. See, e.g., Square, Inc., *Form 10-K Annual Report* (Feb. 27, 2018), at 9-11, 19, 22, available at: <https://www.sec.gov/Archives/edgar/data/1512673/000151267318000004/a10-kfilingsquareinc2017.htm>; PayPal Holdings, Inc., *Form 10-K Annual Report* (Feb. 7, 2018), at 15, available at: <https://www.sec.gov/Archives/edgar/data/1633917/000163391718000029/pypl201710-k.htm>.

566. See, e.g., Visa, *The Visa Payment Facilitator Model: A Framework for Merchant Aggregation* (May 2, 2014), available at: <https://usa.visa.com/dam/VCOM/download/merchants/02-MAY-2014-Visa-Payment-FacilitatorModel.pdf>, and Mastercard, *What Service Providers Need to Know About PCI Compliance*, available at: <https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/service-providers-need-to-know.html>.



# Tab 18

**UNITED STATES OF AMERICA**  
**Before the**  
**SECURITIES AND EXCHANGE COMMISSION**

**SECURITIES ACT OF 1933**

**Release No. 10539 / August 27, 2018**

**SECURITIES EXCHANGE ACT OF 1934**

**Release No. 83947 / August 27, 2018**

**INVESTMENT ADVISERS ACT OF 1940**

**Release No. 4996 / August 27, 2018**

**INVESTMENT COMPANY ACT OF 1940**

**Release No. 33215 / August 27, 2018**

**ADMINISTRATIVE PROCEEDING**

**File No. 3-18681**

**In the Matter of**

**AEGON USA INVESTMENT  
MANAGEMENT, LLC,**

**TRANSAMERICA ASSET  
MANAGEMENT, INC.,**

**TRANSAMERICA CAPITAL,  
INC., AND**

**TRANSAMERICA  
FINANCIAL ADVISORS,  
INC.,**

**Respondents.**

**ORDER INSTITUTING ADMINISTRATIVE  
AND CEASE-AND-DESIST PROCEEDINGS,  
PURSUANT TO SECTION 8A OF THE  
SECURITIES ACT OF 1933, SECTION 15(b)  
OF THE SECURITIES EXCHANGE ACT OF  
1934, SECTIONS 203(e) AND 203(k) OF THE  
INVESTMENT ADVISERS ACT OF 1940,  
AND SECTION 9(f) OF THE INVESTMENT  
COMPANY ACT OF 1940, MAKING  
FINDINGS, AND IMPOSING REMEDIAL  
SANCTIONS AND A CEASE-AND-DESIST  
ORDER**

**I.**

The Securities and Exchange Commission (“Commission”) deems it appropriate and in the public interest that public administrative and cease-and-desist proceedings be, and hereby are, instituted pursuant to Section 8A of the Securities Act of 1933 (“Securities Act”), Section 15(b) of the Securities Exchange Act of 1934 (“Exchange Act”), Sections 203(e) and 203(k) of the Investment Advisers Act of 1940 (“Advisers Act”), and Section 9(f) of the Investment Company Act of 1940 (“Investment Company Act”) against AEGON USA Investment Management, LLC

(“AUIM”), Transamerica Asset Management, Inc. (“TAM”), Transamerica Capital, Inc. (“TCI”), and Transamerica Financial Advisors, Inc. (“TFA”) (collectively, the “Respondents”).

## II.

In anticipation of the institution of these proceedings, Respondents have submitted Offers of Settlement (the “Offers”) which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission’s jurisdiction over them and the subject matter of these proceedings, which are admitted, Respondents consent to the entry of this Order Instituting Administrative and Cease-and-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933, Section 15(b) of the Securities Exchange Act of 1934, Sections 203(e) and 203(k) of the Investment Advisers Act of 1940, and Section 9(f) of the Investment Company Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order (“Order”), as set forth below.

## III.

On the basis of this Order and Respondents’ Offers, the Commission finds<sup>1</sup> that

### Summary

1. Between July 2011 and June 2015 (the “Relevant Period”), Respondents violated the federal securities laws and rules thereunder while offering, selling, and managing 15 quantitative-model-based mutual funds, variable life insurance investment portfolios, and variable annuity investment portfolios (each of which was a registered investment company and collectively are the “Products”) and separately managed account (“SMA”) strategies (the “Strategies”) (collectively, the “Products and Strategies”). Respondents marketed all of the Products and Strategies as “managed using a proprietary quant model,” and highlighted, when marketing certain of the Products and Strategies, their “emotionless,” “model-driven,” or “model-supported” investment management process and described how the models were supposed to operate. These claims necessarily implied that the models worked as intended. Respondents, however, launched the Products and Strategies without first confirming that the models worked as intended and/or without disclosing any recognized risks associated with using the models. During the summer of 2013, AUIM (the subadviser of the Products and Strategies) discovered that certain of the models contained errors and concluded that that these errors rendered at least one of the models “to not be fit for purpose.” AUIM stopped using, running, or relying on at least one of the models in September 2013. AUIM and TAM (the adviser of the Products) failed to disclose the

---

<sup>1</sup> The findings herein are made pursuant to Respondents’ Offers of Settlement and are not binding on any other person or entity in this or any other proceeding.

models' errors and AUIM's decision to stop using the model to the board of trustees of Transamerica Funds (the "Funds Boards"). Certain of the Respondents never publicly disclosed the discovery of errors or AUIM's decision to discontinue use of the model.

2. In addition, TAM and AUIM failed to disclose to investors and the Funds Board that an inexperienced quantitative research analyst (the "Analyst") was the day-to-day manager of certain of the Products. Instead, TAM and AUIM initially disclosed that a senior, experienced asset manager (the "Senior Manager") was the sole portfolio manager of these products and then later disclosed that other employees, as well as the Analyst, were these products' portfolio managers.

3. TAM and AUIM disclosed in filings with the Commission that the primary objective of one of the Products, the Transamerica Tactical Income Fund (the "TTI Fund"), was high current income, with a goal of a monthly dividend that was relatively consistent in amount, in the range of 4%-7%. TAM and AUIM disclosed that the dividend would be calculated based on estimates of expected dividends from the fund's holdings. Yet, TAM and AUIM failed to: (i) determine that the TTI Fund's holdings could support the disclosed dividend yield range; or (ii) calculate the dividend based on the disclosed methodology. Eighteen of the TTI Fund's first 22 monthly dividend payments were attributable, at least in part, to an estimated return of investors' capital, and eight of those payments actually included a return of capital.

4. In 2011, TAM and AUIM added volatility "guidelines" (the "Volatility Overlays") to the variable life insurance and variable annuity investment portfolios without disclosing to investors in those portfolios or the board of trustees of the Transamerica Series Trust (the "Trust Board") that these Volatility Overlays would control and determine the portfolios' asset allocations, and could, in certain market conditions, reduce their exposure to the equity markets below stated target percentages. TAM and AUIM did not take reasonable steps to check the accuracy of the Volatility Overlays. In the fall of 2013, after AUIM discovered and disclosed to TAM errors in the Volatility Overlays, TAM and AUIM failed to disclose those errors to investors in the portfolios or to the Trust Board.

5. TFA negligently relied upon and distributed to its advisory clients: (i) marketing materials stating that AUIM would achieve the Strategies' investment objectives by "using a quantitative econometric model to drive weekly allocations" without disclosing any risks related to the use of a model or verifying that the models worked as intended; and (ii) in connection with an additional set of SMA strategies managed by the unaffiliated investment adviser F-Squared Investments, Inc. ("F-Squared"), marketing materials, most notably an F-Squared-hosted web site, which contained a materially inflated, and hypothetical and back-tested, performance track record.

### **Respondents**

6. **AEGON USA Investment Management, LLC ("AUIM")** (SEC File No. 801-60667) is registered with the Commission as an investment adviser and is headquartered in Cedar

Rapids, Iowa. AUIM is a wholly owned indirect subsidiary of Aegon N.V., a multinational insurance and asset management company headquartered in the Netherlands, and is an affiliate of TAM, TCI, and TFA. AUIM currently has more than \$106 billion in assets under management. AUIM acted as the sub-adviser of the Products and the “Model Manager” that developed, managed, and ran the models used with the Strategies. In its role as Model Manager, AUIM periodically sent the model output to TFA for use with the Strategies.

7. **Transamerica Asset Management, Inc. (“TAM”)** (SEC File No. 801-53319) is registered with the Commission as an investment adviser and is headquartered in Denver, Colorado. TAM is an indirect subsidiary of Aegon N.V. and an affiliate of AUIM and TCI. TAM currently has more than \$79 billion in assets under management. TAM acted as the adviser of the Products and hired AUIM to act as sub-adviser of the Products.

8. **Transamerica Capital, Inc. (“TCI”)** (SEC File No. 8-24829) is registered with the Commission as a broker-dealer and is headquartered in Denver, Colorado. TCI underwrites and distributes mutual funds and investment portfolios, including each of the Products at issue here. It is an indirect, wholly owned subsidiary of Aegon N.V. and an affiliate of TAM and AUIM.

9. **Transamerica Financial Advisors, Inc. (“TFA”)** (SEC File Nos. 801-38618; 8-33429) is dually registered with the Commission as an investment adviser and broker-dealer, is headquartered in St. Petersburg, Florida, and is an indirect subsidiary of Aegon N.V. and an affiliate of AUIM. TFA currently has more than \$969 million in assets under management. TFA sponsors the “Transamerica I-Series program,” a wrap fee program that enables its clients, through TFA investment adviser representatives, to invest in one or more investment strategies within separately managed accounts. TFA licensed and sold each of the Strategies at issue here, as well as investment strategies managed by F-Squared Investments, Inc. and other registered investment advisers.

#### **Other Relevant Entities**

10. **F-Squared Investments, Inc. (“F-Squared”)** (SEC File No. 801-69937) is an investment adviser that was registered with the Commission from March 2009 until January 2016, and was headquartered in Wellesley, Massachusetts. In October 2008, F-Squared launched its first AlphaSector index. F-Squared sub-licensed its approximately 75 AlphaSector indexes to unaffiliated third parties, including TFA, which managed assets pursuant to three of these indexes. On December 22, 2014, the Commission instituted a settled fraud action against F-Squared in which F-Squared admitted, among other things, making the materially false claims that: (i) the signals that formed the basis of the AlphaSector Premium index returns had been used to manage client assets from April 2001 to September 2008; and (ii) the signals resulted in a track record that significantly outperformed the S&P 500 Index from April 2001 to September 2008. *See In the Matter of F-Squared Investments, Inc.*, Admin. Proceeding No. 3-16325 (Dec. 22, 2014).



11. **Transamerica Funds** is registered with the Commission as an open-end management investment company and is organized as a Delaware statutory trust headquartered in Denver, Colorado.

12. **Transamerica Series Trust** is registered with the Commission as an open-end management investment company and is organized as a Delaware statutory trust headquartered in Denver, Colorado.

13. **The Products and Strategies:**

a. **Transamerica AEGON Active Asset Allocation – Conservative VP Portfolio (“AAA-Conservative Portfolio”)**, a series of Transamerica Series Trust and an open-end fund.<sup>2</sup> One of TFA’s SMAs, the Global Tactical Allocation – Conservative, strategy tracked the AAA-Conservative Portfolio.

b. **Transamerica AEGON Active Asset Allocation – Moderate VP Portfolio (“AAA- Moderate Portfolio”)**, a series of Transamerica Series Trust and an open-end fund. One of TFA’s SMAs, the Global Tactical Allocation – Moderate strategy, tracked the AAA-Moderate Portfolio.

c. **Transamerica AEGON Active Asset Allocation – Moderate Growth VP Portfolio (“AAA-Moderate Growth Portfolio”)**, a series of Transamerica Series Trust and an open-end fund. One of TFA’s SMAs, the Global Tactical Allocation – Moderate Growth strategy, tracked the AAA-Moderate Growth Portfolio.

d. **Transamerica Index 35 VP Portfolio (“Index 35 Portfolio”)**, a series of Transamerica Series Trust and an open-end fund. On May 1, 2013, the Index 35 Portfolio was renamed Transamerica Vanguard ETF Portfolio – Conservative VP Portfolio.

e. **Transamerica Index 50 VP Portfolio (“Index 50 Portfolio”)**, a series of Transamerica Series Trust and an open-end fund. On May 1, 2013, the Index 50 Portfolio was renamed Transamerica Vanguard ETF Portfolio – Balanced VP Portfolio.

f. **Transamerica Index 75 VP Portfolio (“Index 75 Portfolio”)**, a series of Transamerica Series Trust and an open-end fund. On May 1, 2013, the Index 75 Portfolio was renamed Transamerica Vanguard ETF Portfolio – Growth VP Portfolio.

g. **Transamerica Tactical Allocation Fund (“TTA Fund”)**, a series of Transamerica Funds and an open-end mutual fund. On May 1, 2015, the TTA Fund was renamed Transamerica Dynamic Allocation II Fund and its investment objectives, principal investment strategies, and subadviser, changed. Later in 2015, TTA was reorganized. One of TFA’s SMAs, the Global Tactical Allocation (“GTA”) strategy, initially tracked the AAA Portfolios. After the TTA Fund was launched, the GTA strategy was realigned to track the TTA Fund.

---

<sup>2</sup> Each of the AAA and Index Portfolios discussed herein was offered as an investment option available under variable life insurance policies and variable annuity contracts issued by select insurance companies.

h. **Transamerica Tactical Income Fund (“TTI Fund”)**, a series of Transamerica Funds and an open-end mutual fund. One of TFA’s SMAs, the Global Tactical Income strategy, tracked the TTI Fund.

i. **Transamerica Tactical Rotation Fund (“TTR Fund”)**, a series of Transamerica Funds and an open-end mutual fund. On May 1, 2015, the TTA Fund was renamed Transamerica Dynamic Allocation Fund, and its investment objectives, principal investment strategies, and subadviser changed. One of TFA’s SMAs, the Global Tactical Rotation strategy, tracked the TTR Fund.

### **Background**

#### **A. Respondents Marketed the Products and Strategies as “Model-Driven” and “Model Supported” Without Confirming That the Models Worked as Intended or Disclosing Risks**

14. Starting in 2010, AUIM tasked the Analyst, who had recently earned his MBA, but had no experience in portfolio management or any formal training in financial modeling, with developing quantitative models for use in managing investment strategies (*i.e.*, models making investment allocation and models making trading decisions). AUIM ultimately used these models to manage each of the Products and Strategies. The Analyst did not follow any formal process to confirm the accuracy of his work, and AUIM failed to provide him meaningful guidance, training, or oversight as he developed the models or to confirm that the models worked as intended before using them to manage client assets.

15. AUIM identified potential risks associated with using models to manage third-party assets no later than 2011, but, by the fall of 2011, it had not reviewed its models for accuracy or formally validated them. By the fall of 2011, AUIM had launched ten of the Products and Strategies — all of the Index and AAA Portfolios and their related SMAs.

16. During the fall of 2011, an internal audit found that “AUIM does not have formal controls or policies and procedures to ensure quantitative model development is controlled and models function as expected.” It also concluded that AUIM “does not periodically perform independent validation of modeling results,” and therefore “transparency to modeling errors is potentially impaired and at worst may be concealed.” In response, two of AUIM’s senior managers informed the internal auditors that AUIM estimated it could resolve these concerns by March 31, 2012, and the company began taking steps to adopt and implement a formal validation process. AUIM continued to offer the Products and Strategies while the models remained unvalidated.

17. Additionally, after an AUIM risk department employee learned in the fall of 2011 that AUIM intended to launch a new product, the TTI Fund, before its model had been finalized and validated, he informed senior AUIM management in an email:

It doesn't seem like we've got the right chain of events to say we're going to launch a fund based on a new model . . . at the end of October; get documentation in place a bit afterwards; and ask for it to be reviewed later in November. I do appreciate the importance of getting products out there to start gathering assets. But we've all heard that model validation is an area where we need to do some serious catch-up. It seems like we're continuing to put the cart before the horse, though.

18. AUIM did not change plans for the TTI Fund launch in response to this email or inform TAM that it had not validated that the model worked as intended. AUIM conducted a high-level "peer review" of the model that would not be complete until after launch and that would not examine logic, methodology, or formulas as a full validation would. Within three days of the launch, preliminary findings from the peer review included the discovery of several glaring errors, such as the fact that the allocation weights did not add up to 100% as they should have. AUIM corrected those errors, but it did not subject the model to further scrutiny until the summer of 2013, when it began formal validation.

19. TFA, an investment adviser that selected AUIM to manage the Strategies, also recognized the risks associated with the "model-driven" Strategies. For example, TFA employees exchanged emails in May 2011 — before selecting AUIM to manage the Strategies — in which they discussed the risks associated with errors in the Analyst's models, noting that "we take the hit if he screws it up." Similarly, in August 2011 — when TFA clients began investing assets in earnest in the Strategies — TFA employees again discussed via email that "we run the risk of [the Analyst] making an error which is easy to do." TFA never disclosed these risks to its clients.

20. AUIM launched each of the Products and Strategies without taking steps to confirm that all of the models worked as intended. Indeed, AUIM did not create, adopt, or implement a written model validation policy until July 2013. Moreover, while AUIM's parent company had a policy in place requiring its subsidiaries, including AUIM, to test models before using them to manage assets, AUIM did not follow this policy.

21. TAM, TCI, and TFA understood that AUIM's models were used to manage each of the Products and Strategies and made affirmative statements to that effect without taking steps to confirm that AUIM had determined that its models worked as intended or disclosing recognized risks related to the use of such models. In particular, consistent with their respective understandings, Respondents drafted, approved, and used marketing materials that discussed the use of quantitative models in the Products and Strategies for "emotionless," "model-driven," or "model-supported" investment management that "eliminates emotional bias." Additionally, TAM informed the Funds Board, in connection with the approval of the TTI Fund, that allocation decisions for the fund would be made "as dictated by the model." TFA claimed in written marketing materials that the Strategies' investment objectives would be achieved "using a quantitative econometric model to drive weekly allocations." TCI (a broker-dealer that distributed

the Products) emphasized the use of models in its dealings with brokers, investment advisers, and other intermediaries when marketing the Products, stating, for example, that “[b]y using econometric modeling, the portfolio manager uses a 3-step process to identify proper allocations,” that “a quantitative strategy helps remove manager bias and limits the potential for human error,” and that the funds would “[u]tilize Econometric Modeling to identify credible signals from over 40 leading indicators.” TAM and TFA made such statements without a reasonable basis, and TAM, TCI, and TFA failed to disclose recognized risks associated with using the quantitative models, which rendered the statements misleading.

22. Additionally, the Analyst, who was not disclosed as a portfolio manager of the Products until March 2012, explained in a June 21, 2012 publicly-available podcast concerning the Products and Strategies:

I don’t really manage the trades on a day-to-day basis or the allocations on a weekly basis, that’s all handled by the model. It’s totally unemotional. I have no, I don’t even have override power but my job is to make sure the models are right, the assumptions are still valid, so, we’ll constantly look at, look for new indicators, test them and see if we get a better outcome, and, of course, annually, we’ll test all the indicators that are in the model to see if the level of accuracy that we are getting in the predictions is still, is still true, so, that is what I try to do.

23. In November 2012, AUIM launched two new Products: the TTA Fund and the TTR Fund. These funds incorporated versions of the TTI Fund’s models. AUIM and TAM believed that these new funds would build upon the TTI Fund’s popularity, as they, too, would address financial advisors’ desire to “reduce or eliminate portfolio manager discretion.” Despite AUIM’s initial estimate of a March 31, 2012 validation completion, AUIM still had not validated the models it used to manage asset allocations in the Products – including the TTI Fund’s asset allocation model, which the Analyst described as the “engine” of these two new funds – before it launched the TTA and TTR Funds.

24. Though marketing materials emphasized the use of models, the Products’ prospectuses did not reference models (or disclose any risks associated with the use of the models) until March 2014, after the discovery of significant errors in the models. This disconnect occurred in part because TAM drafted the prospectuses using a “library” of approved disclosures, the library did not contain any disclosures relating to the use of models, and no one at TAM considered whether a new disclosure regarding model use should be added to the library. The Strategies’ marketing materials also never disclosed any risks associated with using models.<sup>3</sup>

---

<sup>3</sup> Unlike the Products, the Strategies did not have prospectuses.

25. During the summer of 2013, AUIM determined that its allocation models used to manage the TTI Fund and AAA Portfolios contained material errors. For example, AUIM found that the TTI Fund asset allocation model contained “numerous errors in logic, methodology, and basic math” and concluded that these errors rendered it to “not be fit for purpose.” AUIM stopped using, running, or relying on the model to manage the TTI Fund in September 2013, and failed to disclose this decision or its discovery of these errors to the Funds Board, the Trust Board (collectively, the “Boards”), TAM, TCI, TFA, shareholders, and clients. Ultimately, more than 50 errors were discovered in AUIM’s quantitative models used to manage the Products and Strategies. Such errors included incorrect calculations, inconsistent formulas, and the use of whole numbers where percentages were intended (such as 1.77 instead of 1.77%). The errors impacted the models’ allocation outputs.

26. By early March of 2014, TAM and TCI learned that AUIM’s models contained errors and were no longer being used or were largely being ignored. However, neither TAM nor TCI disclosed these facts to investors. Further, TAM failed to disclose these facts to the Boards as a general matter and despite the Boards’ request in the spring of 2014 for such information during the information gathering process required by Section 15(c) of the Investment Company Act, when they were engaged in the adviser and sub-adviser contract renewal process.

27. Instead, in early March 2014, TAM revised the Products’ prospectuses to state, for the first time, that they “may” use a “proprietary quantitative model,” and TCI stopped using certain marketing materials, concluding that they did “not accurately reflect the current process being used to manage these funds.”

28. In May 2014, AUIM directed TFA to amend TFA’s description of AUIM’s investment process in its marketing materials by replacing the phrase, “using a quantitative econometric model,” as the marketing materials had disclosed since inception, with “using a combination of qualitative and quantitative factors.” TFA did not make inquiries in response to this change, however, and AUIM offered no explanation of why the change was necessary. As a result, TFA did not learn until August 2014 that AUIM had discovered errors in its models and was no longer using them or was largely ignoring them.

29. In May 2014, AUIM implemented a validated asset allocation model for the TTI Fund. In September 2014, AUIM implemented a validated asset allocation model for the TTA and TTR Funds. AUIM ultimately implemented validated asset allocation models for the AAA Portfolios in April 2015.

30. In March 2015, TAM recommended that the Boards approve TAM’s termination of the Investment Sub-Advisory Agreement with AUIM. The Boards accepted that recommendation, and AUIM’s Investment Sub-Advisory Agreement with respect to the Products was terminated on March 18, 2015 (effective May 1, 2015). TAM informed investors of the termination on March 18, 2015, but it did not disclose the discovery of errors, the change in investment management process, or the reason for the termination of AUIM’s Investment Sub-Advisory Agreement.

31. AUIM terminated its Model Manager Agreement with TFA on April 2, 2015 (effective May 29, 2015). TFA promptly advised its clients that it was no longer offering AUIM's Strategies, but it did not disclose the discovery of errors, the change in investment management process, or the reason that the AUIM-TFA agreement ended.

**B. TAM and AUIM Failed to Disclose to Investors and the Funds Board the Analyst's Role in Managing the TTI Fund and the AAA Portfolios.**

32. TAM and AUIM failed to disclose to investors in the TTI Fund and the AAA Portfolios and the Funds Board that the Analyst, who had no portfolio management experience, was responsible for the day-to-day management of these products at all times from May 2011 through his termination in August 2013. Instead, TAM and AUIM made inaccurate statements about the portfolio manager. Between May 2011 and March 2012, TAM and AUIM stated in the prospectuses for these products and in their marketing materials that the Senior Manager was the sole portfolio manager of these products. Between March 2012 and March 2013, TAM and AUIM disclosed the Senior Manager, as well as the Analyst and two other employees, as the named portfolio managers for these products. Finally, on March 31, 2013, AUIM removed the Senior Manager as a named portfolio manager for the products, but TAM and AUIM continued to disclose the Analyst and the two other employees as the named portfolio managers.

33. TAM approved disclosures reflecting AUIM's naming of the Senior Manager as the sole portfolio manager of these products (until March 2012) despite knowing, at least with regard to the TTI Fund, that "[the Analyst] selected the ETFs and is the sole architect of the quant model" and that "[the Analyst] doesn't have a backup right now."

34. The Analyst's involvement in the management of these products was so significant that internal auditors attributed "key person risk" to him since "AUIM cannot manage or maintain Passive and Tactical models in the event that [the Analyst] is unavailable." The Analyst also was involved in the marketing of these products, as, for example, he alone was interviewed by The Wall Street Journal and the Market Technicians Association regarding the TTI Fund. In contrast, the Senior Manager and the other two identified portfolio managers had virtually no knowledge of these products or role in their management or marketing.

35. The Senior Manager's knowledge, and involvement in the management, of these products was so limited that he was unable to confirm the accuracy of the investment process description in a draft 2011 prospectus for the AAA Portfolios. For example, he forwarded a request to approve the prospectus to another AUIM employee with the message, "Help." The AUIM employee responded, "I will have [the Analyst] check over the one paragraph that describes the asset allocation strategy . . . ." The Senior Manager also affirmatively refused to market the TTI Fund on at least one occasion because he "was not knowledgeable on the product."

36. Additionally, the Senior Manager did not know that TAM and AUIM intended to disclose him as the sole portfolio manager of the TTI Fund until after the Funds Board had approved the fund. The Funds Board's approval was based, in part, on its comfort with the Senior Manager's involvement. When the Senior Manager learned of his designation, he objected and asked to be removed from all disclosures and marketing materials regarding the TTI Fund, but AUIM's Chief Investment Officer declined to do so.

37. The other two named portfolio managers also lacked fundamental knowledge and meaningful roles in the management of these products. For instance, TAM issued a report after a June 2013 "due diligence" visit in which it observed that "[the Analyst] is currently operating on an island" and observed that two other individuals "are listed as Portfolio Managers but do not have any day-to-day involvement in the portfolio" and "seem to have zero impact on any of the quant strategies." TAM took no action in response to these observations and did not relay them to the Boards. Further, AUIM, in July 2013, devised a "strategy to get [these two individuals] acquainted with the portfolios for mock and potentially real SEC examination" but took no steps to change any disclosures concerning the named portfolio managers of these products.

**C. The TTI Fund Included an Undisclosed Return of Capital in its Dividend Payments.**

38. TAM and AUIM disclosed in filings with the Commission that the TTI Fund's primary objective was high current income, with a goal of a monthly dividend that was "relatively consistent in amount," in the range of 4%-7%. They further disclosed that "[t]he dividend will be calculated based on estimates of expected dividends from the fund's holdings." They also informed the TCI wholesalers who marketed the fund that they projected it to pay a monthly dividend yield of "4.5% to 6.5%," and that the monthly dividend stream would be "handled by using a dividend smoothing algorithm with a quarterly true-up."

39. While from November 2011 through August 2013, the TTI Fund did pay out purported "dividends" within the 4% to 7% range, for 18 of those 22 months TAM and AUIM included short-term capital gains in those dividend calculations, causing the dividends to include an estimated return of capital. For 17 of those dividends, TAM and AUIM did not send investors required notices under Section 19(a) of the Investment Company Act specifying that the payments included estimated return of capital. Additionally, eight of those dividends, all paid in 2013, did in fact include a return of capital. This occurred for two reasons. First, TAM and AUIM did not complete the "dividend smoothing algorithm." Second, until the fall of 2013, AUIM lacked sufficient controls to determine that any particular asset would be held through its "ex-dividend" date and therefore could not accurately predict expected dividends of fund holdings. In June 2013, TAM issued an internal report noting this failure and the conclusion that therefore "income expectations of the tactical income fund were a bit exaggerated."

40. In June of 2013, TAM and AUIM told the TCI wholesalers to inform financial advisers of the return of capital and lowered the distribution yield of the fund by "setting the distribution policy more directly to what the underlying ETFs are generating," which they expected to be around 3-4% prospectively.

**D. TAM and AUIM Added Volatility Overlays to the Index and AAA Portfolios Without Adequate Disclosure and Without First Confirming the Overlays' Accuracy.**

41. In 2011, at TAM's direction, AUIM added Volatility Overlays to the Index Portfolios and also launched the AAA Portfolios with these Volatility Overlays. The Index and AAA Portfolios were offered through variable annuity contracts and variable universal life insurance policies that provided purchasers a rider option with guaranteed minimum withdrawal benefits. Purchasers could choose among a list of investment options for this rider, some of which provided the opportunity, at an additional cost, to increase their benefits above the guaranteed minimum. The Index and AAA Portfolios were among these options; they purported to offer greater exposure to the equities markets and therefore the potential for greater appreciation during market upswings.

42. The Index Portfolios historically targeted a stated equity concentration over time that was reflected in each portfolio's name. For instance, the Index 35 Portfolio targeted a mix over time of approximately 35% equity concentration, and the portfolio's equity exposure over time was to remain within 4% of that target (*i.e.*, 31% to 39%). In September 2010, TAM proposed expanding the equity concentration range to 18% of the target (*i.e.*, 15% to 51% for the Index 35 Fund) and using the Volatility Overlays to limit equity exposure in times of greater volatility, thus reducing the chance that the portfolios would lose money and require the insurance company to use its own assets to pay guaranteed benefits. The change would limit losses in periods when the prices of equities were dropping. Yet, certain investors purchased rider options with guaranteed minimum withdrawal benefits to obtain greater appreciation during rising equity markets, and this change also would limit such potential appreciation. The Trust Board approved TAM's proposals, and AUIM implemented them on May 1, 2011.

43. TAM disclosed the use of the Volatility Overlays in the Index Portfolios' May 1, 2011 prospectuses, but it did not disclose associated risks or explain that the Volatility Overlays were controls that would dictate the portfolios' asset allocations in certain markets, instead referring to them as "guidelines."

44. Though TAM and AUIM applied the same Volatility Overlays to both the Index Portfolios and the AAA Portfolios, TAM did not disclose in the AAA Portfolios' initial May 1, 2011 prospectuses that they were also subject to the Volatility Overlays. TAM did not disclose the application of these Volatility Overlays to the AAA Portfolios until their April 26, 2012 prospectuses.

45. AUIM notified TAM in 2012 that it believed the Volatility Overlays were dampening the Index and AAA Portfolios' equity exposure below the portfolios' equity targets. AUIM also questioned whether the Index and AAA Portfolios' prospectuses misled investors by calling the Volatility Overlays "guidelines." Nonetheless, the prospectuses continued to refer to the Volatility Overlays as "guidelines."



46. In June 2012, certain insurance companies notified TAM that they intended to cease offering the Index and AAA Portfolios at the end of the year because the products were no longer profitable. In the summer of 2012, TAM approached AUIM about modifying the Volatility Overlays so that insurance companies would continue to offer these portfolios. AUIM developed the requested modifications but informed TAM that, although the back-tests showed a potential benefit to some investors, the modified Volatility Overlays could also result in average equity exposures below the long-term targets stated in the prospectuses. For example, AUIM predicted that the Index 75 Fund would see average equity exposures of 59.08% compared to the stated target of 75%.

47. In October 2012, TAM recommended that the Trust Board adopt the modified Volatility Overlays for most of the Index and AAA Portfolios. TAM warned that “[t]he proposed modifications may cause the [Portfolios’] equity allocation to deviate from the established benchmarks,” but advised that the modified Volatility Overlays provide “a significant benefit to the shareholder.” While the modified Volatility Overlays may have provided downside protection to shareholders by reducing equity exposure, that reduced equity exposure was not what shareholders reasonably would have expected based on the Index and AAA Portfolios’ disclosures, and that reduced equity exposure diminished shareholder returns in up markets. The Trust Board followed TAM’s recommendation. The modified Volatility Overlays were implemented on December 10, 2012.

48. In January 2013, TAM recommended that the Trust Board change the names of the Index Portfolios to eliminate the equity percentage numbers because, among other things, the current “name of these [Portfolios] may cause confusion to investors.” The Index Portfolios were renamed effective May 1, 2013, but TAM did not disclose the reason for the name change.

49. In October 2013, AUIM reviewed the modified Volatility Overlays and discovered errors in their back-tests and implementation. AUIM informed TAM of its discovery shortly after it identified the errors. AUIM then began correctly implementing the modified Volatility Overlays starting in late October 2013. AUIM shared its conclusions and analysis with TAM, but neither AUIM nor TAM disclosed the information to investors or the Boards.

**E. TFA Negligently Relied Upon and Distributed to Its Advisory Clients Marketing Materials Regarding AUIM’s Use of Econometric Models and F-Squared’s Materially Inflated, and Hypothetical and Back-tested, Performance Track Record.**

50. From mid-2011 to 2015, TFA offered strategies managed by AUIM and F-Squared through its wrap fee program without having in place or implementing written compliance policies and procedures reasonably designed to determine it had a reasonable basis for its public disclosures regarding these strategies.

51. These deficiencies contributed to TFA’s failings regarding AUIM’s strategies as discussed in paragraphs 19, 21, 28, and 31 *supra*. Additionally, in part because of these same failings, TFA contracted with F-Squared in December 2010 and ultimately offered three F-

Squared-managed SMA investment strategies between June 2011 and October 12, 2015: (1) the AlphaSector Rotation strategy (offered beginning mid-June 2011), (2) the AlphaSector Rotation Premium strategy (offered beginning late February 2012), and (3) the AlphaSector World Allocator Premium strategy (offered beginning late December 2012).

52. In addition, TFA relied on F-Squared's marketing efforts, including allowing F-Squared to create a dedicated website for TFA and to communicate directly with TFA's investment adviser representatives and advisory clients. F-Squared falsely marketed the strategies using hypothetical historical performance that it described as "not backtested" and based on an actual strategy used to manage live assets. In embracing F-Squared's marketing efforts, TFA violated its own compliance policies and procedures, including, specifically, those regarding the use of internet web sites and third party advertising.

53. With regard to F-Squared's performance claims concerning the period April 2001 to September 2008, TFA also relied solely on documents and information that came directly or indirectly from F-Squared while it was aware or should have been aware of risks associated with using this information. While TFA did review performance returns calculated by a third-party, the input data that that third-party used to calculate the returns also came from F-Squared. Having taken insufficient steps to confirm the accuracy of F-Squared's performance data and not having obtained sufficient documentation that would have substantiated F-Squared's advertised performance and performance-related claims in the F-Squared advertising materials distributed by TFA, TFA failed to have a reasonable basis to believe that F-Squared's performance was accurate when it distributed advertisements to clients considering F-Squared's strategies.

54. Additionally, TFA did not reasonably respond to concerns that arose concerning F-Squared between October 2013 and July 2015. For example, during the spring of 2014, TFA learned that the Investment Company Institute had published an article claiming that F-Squared "clearly overstated" past returns in its marketing materials. In response, TFA requested that F-Squared "provide the corrected back tested monthly returns for the period April 2001 – September 2008," but it took no action when F-Squared replied that it could not because "1/1/03 is the first date we had the information we needed to run the back test."

### **Violations**

55. As a result of the conduct described above, AUIM and TCI willfully<sup>4</sup> violated Section 17(a)(2) of the Securities Act, which prohibits any person, in the offer or sale of securities, from obtaining money or property by means of any untrue statement of material fact

---

<sup>4</sup> A willful violation of the securities laws means merely "that the person charged with the duty knows what he is doing." *Wonsover v. SEC*, 205 F.3d 408, 414 (D.C. Cir. 2000) (quoting *Hughes v. SEC*, 174 F.2d 969, 977 (D.C. Cir. 1949)). There is no requirement that the actor "also be aware that he is violating one of the Rules or Acts." *Id.* (quoting *Gearhart & Otis, Inc. v. SEC*, 348 F.2d 798, 803 (D.C. Cir. 1965)).

or any omission to state a material fact necessary in order to make statements made not misleading. Proof of scienter is not required to establish a violation of Section 17(a)(2) of the Securities Act; negligence is sufficient. *Aaron v. SEC*, 446 U.S. 680 (1980); *SEC v. Hughes Capital Corp.*, 124 F.3d 449, 453-54 (3d Cir. 1997)

56. As a result of the conduct described above, AUIM and TAM willfully violated Section 15(c) of the Investment Company Act, which requires an investment adviser (and, in this case, also the sub-adviser) to a registered investment company, such as a mutual fund, “to furnish, such information as may reasonably be necessary to evaluate the terms of any contract whereby [it] undertakes regularly to serve or act as investment adviser . . . .” to the fund.

57. As a result of the conduct described above, AUIM, TAM, and TFA willfully violated Section 206(2) of the Advisers Act, which prohibits any investment adviser from engaging in any transaction, practice, or course of business which operates as a fraud or deceit upon any client or prospective client. A violation of Section 206(2) may rest on a finding of simple negligence. *SEC v. Steadman*, 967 F.2d 636, 643 n.5 (D.C. Cir. 1992) (citing *SEC v. Capital Gains Research Bureau, Inc.*, 375 U.S. 180, 195 (1963)). Proof of scienter is not required to establish a violation of Section 206(2) of the Advisers Act. *Id.*

58. As a result of the conduct described above, AUIM and TFA willfully violated Section 206(4) of the Advisers Act and Rule 206(4)-1(a)(5) thereunder, which makes it a fraudulent, deceptive, or manipulative act, practice, or course of business within the meaning of Section 206(4) of the Advisers Act to, among other things, directly or indirectly publish, circulate or distribute an advertisement which contains any untrue statement of material fact, or which is otherwise false or misleading. Proof of scienter is not required to establish a violation of Section 206(4) of the Advisers Act and the rules thereunder. *Steadman*, 967 F.2d at 647.

59. As a result of the conduct described above, AUIM, TAM, and TFA willfully violated Section 206(4) of the Advisers Act and Rule 206(4)-7 thereunder by failing to adopt and implement written policies and procedures reasonably designed to prevent violations of the Advisers Act and the rules thereunder. Proof of scienter is not required to establish a violation of Section 206(4) of the Advisers Act and the rules thereunder. *Steadman*, 967 F.2d at 647.

60. As a result of the conduct described above, AUIM and TAM willfully violated Section 206(4) of the Advisers Act and Rule 206(4)-8 thereunder, which make it unlawful for any investment adviser to a pooled investment vehicle to make any untrue statement of material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which they were made, not misleading, to any investor or prospective investor in the pooled investment vehicle, or otherwise engage in any act, practice, or course of business that is fraudulent, deceptive, or manipulative with respect to any investor or prospective investor in the pooled investment vehicle. Proof of scienter is not required to establish a violation of Section 206(4) of the Advisers Act and the rules thereunder. *Steadman*, 967 F.2d at 647.

61. As a result of the conduct described above, TFA willfully violated Section 204(a) of the Advisers Act and Rule 204-2(a)(16) thereunder. Section 204(a) of the Advisers Act requires investment advisers to make and keep certain records as the Commission, by rule, may prescribe as necessary or appropriate in the public interest or for the protection of investors. Rule 204-2 under the Advisers Act requires investment advisers registered or required to be registered to make and keep true, accurate and current various books and records relating to their investment advisory business, including all accounts, books, internal working papers, and any other records or documents that are necessary to form the basis for or demonstrate the calculation of the performance or rate of return of any or all managed accounts or securities recommendations in any notice, circular, advertisement, newspaper article, investment letter, bulletin or other communication that the investment adviser publishes, circulates, or distributes, directly or indirectly, to ten or more persons. Proof of scienter is not required to establish a violation of Section 204 of the Advisers Act and the rules thereunder. *Steadman*, 967 F.2d at 647.

#### **Respondents' Cooperation and Remedial Efforts**

62. In determining to accept the Offers, the Commission considered the substantial cooperation afforded the Commission staff. Respondents cooperated with the Commission's investigation throughout its entirety, and their efforts assisted the Commission staff in its collection of evidence, including information that might not otherwise have been available to the staff.

63. In 2016, after the start of the Commission's investigation, Respondents voluntarily retained a compliance consultant (the "Consultant") to conduct a comprehensive, independent review related to their respective compliance policies and procedures, internal controls and related practices, with an emphasis on product development, use of investment models and algorithms, due diligence, disclosures in prospectuses and marketing materials, and enterprise compliance functions and the operation of those controls within and among the Respondents. Respondents received the Consultant's written findings and implemented the Consultant's proposed changes. Respondents have retained the Consultant for further reviews through the Consultant's completion of the follow-up review for fiscal year 2019.

64. In addition, in advance of receiving the Consultant's recommendations, Respondents began revising and improving their compliance and due diligence policies and procedures related to the use of models and the creation and use of marketing communications, product development, and investment management.

#### **IV.**

In view of the foregoing, the Commission deems it appropriate, in the public interest, and for the protection of investors to impose the sanctions agreed to in Respondents' Offers.

Accordingly, pursuant to Section 8A of the Securities Act, Section 15(b) of the Exchange Act, Sections 203(e) and 203(k) of the Advisers Act, and Section 9(f) of the Investment Company Act, it is hereby ORDERED that:

A. AUIM shall cease and desist from committing or causing any violations and any future violations of Section 17(a)(2) of the Securities Act, Sections 206(2) and 206(4) of the Advisers Act and Rules 206(4)-1(a)(5), 206(4)-7, and 206(4)-8 promulgated thereunder, and Section 15(c) of the Investment Company Act.

B. TAM shall cease and desist from committing or causing any violations and any future violations of Sections 206(2) and 206(4) of the Advisers Act and Rules 206(4)-7 and 206(4)-8 promulgated thereunder, and Section 15(c) of the Investment Company Act.

C. TCI shall cease and desist from committing or causing any violations and any future violations of Section 17(a)(2) of the Securities Act.

D. TFA shall cease and desist from committing or causing any violations and any future violations of Sections 204, 206(2) and 206(4) of the Advisers Act and Rules 204-2(a)(16), 206(4)-1(a)(5), and 206(4)-7 promulgated thereunder.

E. Respondents are censured.

F. Respondents shall pay disgorgement, prejudgment interest, and civil monetary penalties totaling \$97,602,040 as follows:

- i. AUIM shall pay disgorgement of \$24,599,896, prejudgment interest of \$3,682,195, and a civil monetary penalty of \$21,000,000, consistent with the provisions of this Subsection F.
- ii. TAM shall pay disgorgement of \$15,000,000, prejudgment interest of \$2,235,765, and a civil monetary penalty of \$10,500,000, consistent with the provisions of Subsection F.
- iii. TCI shall pay disgorgement of \$12,000,000, prejudgment interest of \$1,826,022, and a civil monetary penalty of \$4,000,000, consistent with the provisions of Subsection F.
- iv. TFA shall pay disgorgement of \$1,700,000, prejudgment interest of \$258,162, and a civil monetary penalty of \$800,000, consistent with the provisions of Subsection F.
- v. Pursuant to Section 308(a) of the Sarbanes-Oxley Act of 2002, as amended, a Fair Fund for distribution to account holders who purchased or held an

interest in any of the Products and Strategies or F-Squared strategies during the Relevant Period (each, an “affected investor”) is created for the \$97,602,040 in disgorgement, prejudgment interest, and penalties paid by Respondents as described above, as well as any penalties paid by Bradley J. Beman and Kevin A. Giles, within 30 days of the entry of the orders in the parallel proceedings, *In the Matter of Bradley J. Beman*, Admin. Proc. File No. 3-18682 and *In the Matter of Kevin A. Giles*, Admin. Proc. File No. 3-18683. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondents agree that in any Related Investor Action, they shall not argue that they are entitled to, nor shall they benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondents’ payment of a civil penalty in this action (“Penalty Offset”). If the court in any Related Investor Action grants such a Penalty Offset, Respondents agree that they shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission’s counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a “Related Investor Action” means a private damages action brought against Respondents by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

- vi. Within ten (10) days of issuance of this Order, Respondents shall deposit \$97,602,040 of the disgorgement, prejudgment interest, and civil monetary penalties (the “Fair Fund”) into an escrow account at a financial institution not unacceptable to the Commission staff and Respondents shall provide the Commission staff with evidence of such deposit in a form acceptable to the Commission staff. If timely payment into the escrow account is not made, additional interest shall accrue pursuant to SEC Rule of Practice 600 and 31 U.S.C. § 3717.
- vii. Respondents shall be responsible for administering the Fair Fund and may hire a professional to assist them in the administration of the distribution. The costs and expenses of administering the Fair Fund, including any such professional services, shall be borne by Respondents and shall not be paid out of the Fair Fund.
- viii. Respondents shall pay from the Fair Fund to each affected investor an amount representing the *pro-rata* fees and commissions paid by the affected investor during the Relevant Period pursuant to a disbursement

calculation (the “Calculation”) that will be submitted to, reviewed, and approved by the Commission staff in accordance with this Subsection F. No portion of the Fair Fund shall be paid to any affected investor account in which any Respondents or any of their current or former officers or directors have a financial interest.

- ix. Respondents shall, within ninety (90) days of the entry of this Order, submit a proposed Calculation to the Commission staff for review and approval. At or around the time of submission of the proposed Calculation to the staff, Respondents, along with any third-parties or professionals retained by Respondents to assist in formulating the methodology for its Calculation and/or administration of the Distribution, shall make themselves available for a conference call with the Commission staff to explain the methodology used in preparing the proposed Calculation and its implementation, and to provide the staff with an opportunity to ask questions. Respondents shall also provide to the Commission staff such additional information and supporting documentation as the Commission staff may request for the purpose of its review. In the event of one or more objections by the Commission staff to Respondents’ proposed Calculation or any of its information or supporting documentation, Respondents shall submit a revised Calculation for the review and approval of the Commission staff or additional information or supporting documentation within ten (10) days of the date that Respondents are notified of the objection. The revised Calculation shall be subject to all of the provisions of this Subsection F.
- x. After the Calculation has been approved by the Commission staff, Respondents shall submit a payment file (the “Payment File”) for review and acceptance by the Commission staff demonstrating the application of the methodology to each affected investor. The Payment File should identify, at a minimum: (1) the name of each affected investor, (2) the exact amount of the payment to be made from the Fair Fund to each affected investor, and (3) the amount of any *de minimis* threshold to be applied.
- xi. Respondents shall complete the disbursement of all amounts payable to affected investor accounts within 90 days of the date the Commission staff accepts the Payment File unless such time period is extended as provided in Paragraph xv of this Subsection F.
- xii. If Respondents are unable to distribute or return any portion of the Fair Fund for any reason, including an inability to locate an affected investor or a beneficial owner of an affected investor account or any factors beyond Respondents’ control, Respondents shall transfer any such undistributed funds to the Commission for transmittal to the United States Treasury in accordance with Section 21F(g)(3) of the Securities Exchange Act of 1934,

pursuant to the instructions set forth in Subsection G, below, when the distribution of the funds is complete and before the final accounting provided for in Paragraph xii of this Subsection F is submitted to Commission staff.

- xiii. A Fair Fund is a Qualified Settlement Fund (“QSF”) under Section 468B(g) of the Internal Revenue Code (“IRC”), 26 U.S.C. §§ 1.468B.1-1.468B.5. Respondents shall be responsible for any and all tax compliance responsibilities associated with the Fair Fund, including but not limited to tax obligations resulting from the Fair Fund’s status as a QSF and the Foreign Account Tax Compliance Act (“FATCA”), and may retain any professional services necessary. The costs and expenses of tax compliance, including any such professional services, shall be borne by Respondents and shall not be paid out of the Fair Fund.
- xiv. Within 150 days after Respondents complete the distribution of all amounts payable to affected investors, Respondents shall return all undistributed funds to the Commission pursuant to the instructions set forth in Subsection G, below. The Respondents shall then submit to the Commission staff a final accounting and certification of the disposition of the Fair Fund for Commission approval, which final accounting and certification shall be in a format to be provided by the Commission staff. The final accounting and certification shall include, but not be limited to: (1) the amount paid to each payee, with reasonable interest amount, if any, reported separately; (2) the date of each payment; (3) the check number or other identifier of money transferred; (4) the amount of any returned payment and the date received; (5) a description of any effort to locate a prospective payee whose payment was returned or to whom payment was not made for any reason; (6) the total amount, if any, to be forwarded to the Commission for transfer to the United States Treasury; and (7) an affirmation that Respondents have made payments from the Fair Fund to affected investors in accordance with the Calculation approved by the Commission staff. The final accounting and certification shall be submitted under a cover letter that identifies AUIM, TAM, TCI and TFA as Respondents in these proceedings and the file number of these proceedings to Paul A. Montoya, Assistant Regional Director, Asset Management Unit, Division of Enforcement, Securities and Exchange Commission, 175 West Jackson Boulevard, Suite 1450, Chicago, Illinois 60604. Respondents shall provide any and all supporting documentation for the accounting and certification to the Commission staff upon its request and shall cooperate with any additional requests by the Commission staff in connection with the accounting and certification.
- xv. The Commission staff may extend any of the procedural dates set forth in Paragraphs vi through xiv of this Subsection F for good cause shown. Deadlines for dates relating to the Fair Fund shall be counted in calendar



days, except if the last day falls on a weekend or federal holiday, the next business day shall be considered the last day.

G. Payments ordered pursuant to Subsections F.xii and/or F.xiv must be made in one of the following ways:

1. Respondents may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;
2. Respondents may make direct payment from a bank account via Pay.gov through the SEC website at <http://www.sec.gov/about/offices/ofm.htm>; or
3. Respondents may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center  
Accounts Receivable Branch  
HQ Bldg., Room 181, AMZ-341  
6500 South MacArthur Boulevard  
Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying each Respondent as a Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to Paul A. Montoya, Assistant Regional Director, Asset Management Unit, Division of Enforcement, Securities and Exchange Commission, 175 West Jackson Boulevard, Suite 1450, Chicago, Illinois 60604.

By the Commission.

Brent J. Fields  
Secretary

**UNITED STATES OF AMERICA**  
**Before the**  
**SECURITIES AND EXCHANGE COMMISSION**

**INVESTMENT ADVISERS ACT OF 1940**  
**Release No. 4997 / August 27, 2018**

**ADMINISTRATIVE PROCEEDING**  
**File No. 3-18682**

**In the Matter of**

**BRADLEY J. BEMAN**

**Respondent.**

**ORDER INSTITUTING CEASE-AND-DESIST  
PROCEEDINGS PURSUANT TO SECTION  
203(k) OF THE INVESTMENT ADVISERS  
ACT OF 1940, MAKING FINDINGS, AND  
IMPOSING A CEASE-AND-DESIST ORDER**

**I.**

The Securities and Exchange Commission (“Commission”) deems it appropriate and in the public interest that public cease-and-desist proceedings be, and hereby are, instituted pursuant to Section 203(k) of the Investment Advisers Act of 1940 (“Advisers Act”) against Bradley J. Beman (“Beman” or “Respondent”).

**II.**

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the “Offer”) which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission’s jurisdiction over him and the subject matter of these proceedings, which are admitted, and except as provided herein in Section V, Respondent consents to the entry of this Order Instituting Cease-and-Desist Proceedings Pursuant to Section 203(k) of the Investment Advisers Act of 1940, Making Findings, and Imposing a Cease-and-Desist Order (“Order”), as set forth below.

### III.

On the basis of this Order and Respondent's Offer, the Commission finds<sup>1</sup> that:

#### Summary

1. Between July 2011 and June 2015, AEGON USA Investment Management, LLC ("AUIM"), a registered investment adviser, violated certain provisions of the federal securities laws in connection with the offer, sale, and management of six variable life insurance investment portfolios and variable annuity investment portfolios ("Investment Portfolios") and three mutual funds (collectively, the "Products"), all nine of which employed quantitative models for allocation and trading decisions.<sup>2</sup> Among those violations, AUIM marketed the Products by highlighting their "emotionless," "model-driven," or "model-supported" investment management process and describing how the models were supposed to operate, but did not confirm that the models worked as intended and/or disclose any recognized risks associated with using the models. Additionally, AUIM failed to disclose to investors that an inexperienced quantitative research analyst (the "Analyst") was the day-to-day manager of certain of the Products.

2. AUIM also failed to adopt and implement certain compliance policies and procedures, including failing to take reasonable steps to ensure that: (1) its quantitative models worked as intended both before the Products launched and on a periodic basis after they launched; (2) it adopted and implemented reasonable controls regarding the testing, approval, and documentation of any changes to its quantitative models; and (3) the Products' portfolio managers' discretion to depart from model-directed trades was defined, monitored, and documented. Each of these risks was identified in a November 2011 internal audit report.

3. Beman, who served as AUIM's Global Chief Investment Officer at all relevant times, was a cause of these violations. Beman, despite being aware of the risks that the models would not work as intended, did not take sufficient steps to have AUIM confirm the accuracy of the models. He also did not identify the Analyst as the portfolio manager of certain of the Products despite being aware of his role in developing and managing the models. Beman agreed to be responsible for addressing the risks identified in the 2011 audit report, but failed to do so.

---

<sup>1</sup> The findings herein are made pursuant to Respondent's Offer of Settlement and are not binding on any other person or entity in this or any other proceeding.

<sup>2</sup> See *In the Matter of AEGON USA Investment Management, LLC, et al.*, Admin. Proc. File No. 3-18681 (Aug. 27, 2018) (the "Aegon Proceeding").

### **Respondent**

4. Bradley J. Beman, age 54, is a resident of Iowa. Beman joined AUIM in 1987 and served as AUIM's Global Chief Investment Officer from 2010 through January 2015. Beman also was a member of AUIM's U.S. Risk and Control Committee from September 2011 through January 2015. Beman is a Chartered Financial Analyst and was previously licensed as a certified public accountant.

### **Other Relevant Entities**

5. **AEGON USA Investment Management, LLC ("AUIM")** (SEC File No. 801-60667) is registered with the Commission as an investment adviser and is headquartered in Cedar Rapids, Iowa. AUIM is a wholly owned indirect subsidiary of Aegon N.V., a multinational insurance and asset management company headquartered in the Netherlands, and is an affiliate of Transamerica Asset Management, Inc. ("TAM"). AUIM currently has more than \$106 billion in assets under management. AUIM acted as the sub-adviser to the Products, under the supervision of TAM, which was the adviser to the Products.

6. **Transamerica Asset Management, Inc. ("TAM")** (SEC File No. 801-53319) is registered with the Commission as an investment adviser and is headquartered in Denver, Colorado. TAM is an indirect subsidiary of Aegon N.V. and an affiliate of AUIM. TAM currently has more than \$79 billion in assets under management. TAM acted as the adviser to the Products and hired AUIM to act as sub-adviser to the Products.

### **Facts**

#### **A. Beman's Role in AUIM's Failures to Confirm That the Models Worked as Intended**

7. Beman was responsible for guiding AUIM's investment strategy for its clients and overseeing investment performance across multiple asset classes in the U.S. and internationally. Beman's oversight responsibilities included each of the Products, and he approved on behalf of AUIM who was identified as the portfolio manager for the Products. As a member of AUIM's U.S. Risk and Control Committee (which, in addition to Beman, included employees from AUIM's compliance, human resources, legal, and risk departments), Beman received monthly reports that discussed investment risk, operational risk, compliance risk, and legal risk issues both generally and with specific regard to the Products. These monthly reports were sent to all members of AUIM's U.S. Risk and Control Committee and included status updates of efforts to address identified risks.

8. Starting in 2010, AUIM tasked the Analyst, who had recently earned his MBA, but had no experience in portfolio management or any formal training in financial modeling, with developing quantitative models for use in managing investment strategies (*i.e.*, models making investment allocation and models making trading decisions). AUIM ultimately used these models to manage each of the Products. The Analyst did not follow any formal process to confirm the accuracy of his work, and AUIM failed to provide him meaningful guidance, training, or oversight

as he developed the models or to confirm that the models worked as intended before using them to manage client assets.

9. By the fall of 2011, because of the significant growth of assets under management in the Investment Portfolios, Beman requested the help of an affiliated insurance company internal audit team to conduct an audit of the control environment supporting these six products.

10. On October 6, 2011, the audit team issued an interim status report to Beman and AUIM's Director of New Initiatives (the "AUIM Director"). The interim status report identified certain risks concerning AUIM's use of quantitative models, including that:

- (i) "AUIM does not have formal controls or policies and procedures to ensure quantitative model development is controlled and models function as expected";
- (ii) "AUIM does not periodically perform independent validation of modeling results to ensure the integrity of [the Investment Portfolios'] models remains intact," and therefore "transparency to modeling errors is potentially impaired and at worst may be concealed"; and
- (iii) "AUIM has not formally defined the discretion Portfolio Managers have in managing [the Investment Portfolios] regarding trade orders not aligned with modeling results."

11. The interim status report also observed that the Analyst developed and maintained the models and warned: "In the event [the Analyst] is unavailable and model enhancements are required or models are not functioning as designed, AUIM backup personnel do not have sufficient knowledge to enhance, validate, or troubleshoot the models. In the event [the Analyst] is unavailable, models may be inadequately administered, potentially exposing client's [sic] to excessive or unnecessary risk, negatively affecting fund performance, and potentially impairing AUIM's ability to meet its investment objectives." The interim report then assigned "key person risk" to the Analyst.

12. On or about October 10, 2011, Beman and the AUIM Director met with the internal auditors to discuss the interim status report. During this and subsequent meetings, Beman and the AUIM Director were designated as the AUIM management employees responsible for addressing each of the risks identified in the interim status report.

13. Shortly thereafter, a senior manager in AUIM's risk department learned that AUIM intended to launch one of the Products, the Transamerica Tactical Income Fund (the "TTI Fund"), which had been developed from the same quantitative models used to manage the Investment Portfolios studied in the audit. That senior risk manager understood that AUIM planned to launch the TTI Fund before its model had been finalized and validated, and emailed Beman and other senior AUIM management to inform them:

It doesn't seem like we've got the right chain of events to say we're going to launch a fund based on a new model . . . at the end of

October; get documentation in place a bit afterwards; and ask for it to be reviewed later in November. I do appreciate the importance of getting products out there to start gathering assets. But we've all heard that model validation is an area where we need to do some serious catch-up. It seems like we're continuing to put the cart before the horse, though.

14. Beman responded, "True-I think this has been a gap in our process historically and we are trying to address and will have a more rigorous process in the future. Unfortunately, I think the launch date for this product is already set and ready to go." The risk manager replied, "We definitely need to be involved in the independent review and validation of these models. Appreciate your support here." Though Beman was someone who could have stopped or delayed the launch of the TTI Fund, neither he nor anyone else took any steps to do so.

15. The TTI Fund was launched on October 31, 2011.

16. On November 4, 2011, the internal audit team issued a final report that included the three risks concerning AUIM's use of quantitative models identified in Paragraph 10, above, and the risk regarding the firm's reliance on the Analyst identified in Paragraph 11, above. This report identified Beman and the AUIM Director as the members of management responsible for: (i) the implementation of internal controls and other policies and procedures to address each of the identified risks; (ii) the execution of specific steps to address these risks; and (iii) the establishment of specific dates by which such steps would be completed. The report was distributed throughout the company.

17. Beman and the AUIM Director informed the auditors that AUIM estimated it could resolve these concerns by March 31, 2012, and AUIM began taking steps to adopt and implement a formal validation process, which would address some of the audit's findings. AUIM continued to offer the then existing Products while the models remained unvalidated.

18. Between October 2011 and the summer of 2013, Beman discussed internally the importance of validating the models on multiple occasions. For example, on May 19, 2012, Beman emailed the AUIM Director and others at AUIM:

[U]nfortunately the larger the funds get[,] the bigger the risk becomes . . . a major operational glitch at this point would be a big issue as this has already been flagged as an operational issue by audit . . . I need your priority and that of the team to make sure these models are buttoned down very tightly.

Beman, however, was aware that the models were not being "buttoned down." In particular, Beman attended monthly meetings of the U.S. Risk and Control Committee during which the status of model validation was discussed. The committee's meeting minutes reflect that, between the fall of 2011 and the spring of 2013, the deadlines for validation of the Products' models had been repeatedly pushed back. Thus, Beman was aware that the models were not being "buttoned

down” and did not take any additional, reasonable steps to address the risks that the models would not work as intended.

19. In November 2012, more than a year after Beman and AUIM’s Director had been designated with responsibility for the implementation of internal controls and other policies and procedures to address each of the identified risks, AUIM launched two of the Products: the Transamerica Tactical Allocation Fund (the “TTA Fund”) and the Transamerica Tactical Rotation Fund (the “TTR Fund”). These funds incorporated versions of the TTI Fund’s models, and, thus, also employed models developed from the same quantitative models used to manage the Investment Portfolios studied in the audit.

20. Despite Beman’s and the AUIM Director’s initial estimate of a March 31, 2012 validation completion, AUIM still had not validated any of the models it used to manage asset allocations in the Products — including the TTI Fund’s asset allocation model, which the Analyst had described as the “engine” of these two new funds — before it launched the TTA and TTR Funds. Thus, like the TTI Fund’s models, the TTA and TTR Funds’ models were not validated when these products were launched. Beman was aware of these facts when he approved the TTA and TTR Funds’ launches.

21. The marketing efforts for each of the Products highlighted their “emotionless,” “model-driven,” or “model-supported” investment management process and described how the models were supposed to operate. For instance, marketing materials stated that the TTA, TTI, and TTR Funds, among other things, employed a “disciplined quantitative process” that “removes emotion and manager bias through mathematical-based models.”

**B. Beman’s Role in AUIM’s Failure to Disclose the Analyst’s Role in Managing Four of the Products**

22. The prospectuses and marketing materials for four of the Products (the TTI Fund and three of the Investment Portfolios) also failed at all times through the Analyst’s termination in August 2013 to disclose that the Analyst, who had no portfolio management experience, was responsible for the day-to-day management of those products. Instead: (i) between May 2011 and March 2012, these Products’ prospectuses and marketing materials identified a senior, experienced asset manager (the “Senior Manager”) as the sole portfolio manager; (ii) between March 2012 and March 2013, the Senior Manager, as well as the Analyst and two other employees, were disclosed as the named portfolio managers for these products; and (iii) on March 31, 2013, the Senior Manager was removed as a named portfolio manager for the products, but the Analyst and the two other employees continued to be disclosed as the named portfolio managers. Beman was aware of the prospectus and marketing disclosures regarding the Products’ portfolio managers.

23. Beman approved on behalf of AUIM who would be identified as the portfolio manager for these four Products, which was repeated in these Products’ prospectuses and marketing materials. Beman was aware of the Analyst’s role — and the Senior Manager’s and other employees’ lack of involvement — in managing these products at the time he approved AUIM’s decision to name the portfolio manager of these products. For instance, Beman

understood that the auditors had assigned “key person risk” to the Analyst given his involvement in the management of these products. Indeed, when the Senior Manager learned that he had been disclosed as the sole portfolio manager of the TTI Fund, he objected to Beman and asked to be removed from all disclosures and marketing materials regarding the TTI Fund, but Beman declined to do so until March 31, 2013.

**C. Beman’s Role in AUIM’s Failure to Adopt or Implement Certain Compliance Policies and Procedures**

24. AUIM failed to adopt or implement policies and procedures to address the risks identified in the internal audit report before launching the mutual funds and for many months after launching all of the Products.

25. Beman failed to take reasonable steps to revise AUIM’s policies and procedures. For example, though Beman was one of those responsible for addressing the risks related to model validation and model functioning, he failed to take reasonable steps to accomplish this. AUIM failed to adopt a policy requiring model validation until July 2013 and began validating the quantitative models used to make allocation decisions in the Products only at that point — nearly two years after the launch of the TTI Fund and nearly a year after the launches of the TTA and TTR Funds.

**Violations**

26. As a result of the negligent conduct described above, Beman was a cause of AUIM’s violations of Section 206(4) of the Advisers Act and Rule 206(4)-8 thereunder, which make it unlawful for any investment adviser to a pooled investment vehicle to make any untrue statement of material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which they were made, not misleading, to any investor or prospective investor in the pooled investment vehicle, or otherwise engage in any act, practice, or course of business that is fraudulent, deceptive, or manipulative with respect to any investor or prospective investor in the pooled investment vehicle.

27. As a result of the negligent conduct described above, Beman was a cause of AUIM’s violations of Section 206(4) of the Advisers Act and Rule 206(4)-7 thereunder, which require a registered investment adviser to adopt and implement written policies and procedures reasonably designed to prevent violations of the Advisers Act and its rules, and to review, no less frequently than annually, the adequacy of the policies and procedures and the effectiveness of their implementation.



#### IV.

In view of the foregoing, the Commission deems it appropriate and in the public interest to impose the sanctions agreed to in Respondent's Offer.

Accordingly, pursuant to Section 203(k) of the Advisers Act, it is hereby ORDERED that:

A. Respondent Beman shall cease and desist from committing or causing any violations and any future violations of Section 206(4) of the Advisers Act and Rules 206(4)-7 and 206(4)-8 promulgated thereunder.

B. Respondent Beman shall, within 30 days of the entry of this Order, pay a civil money penalty in the amount of \$65,000.00 to the Fair Fund established in the Aegon Proceeding for distribution to affected investors. The \$65,000.00 shall be deposited into the same escrow account established in the Aegon Proceeding.

Payments by check or money order must be accompanied by a cover letter identifying Bradley J. Beman as a Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to Paul A. Montoya, Division of Enforcement, Securities and Exchange Commission, 175 West Jackson Blvd., Suite 1450, Chicago, IL 60604.

C. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondent agrees that in any Related Investor Action, he shall not argue that he is entitled to, nor shall he benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondent's payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondent agrees that he shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondent by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

#### V.

It is further Ordered that, solely for purposes of exceptions to discharge set forth in Section 523 of the Bankruptcy Code, 11 U.S.C. § 523, the findings in this Order are true and admitted by Respondent, and further, any debt for disgorgement, prejudgment interest, civil penalty or other amounts due by Respondent under this Order or any other judgment, order, consent order, decree or settlement agreement entered in connection with this proceeding, is a debt for the violation by

Respondent of the federal securities laws or any regulation or order issued under such laws, as set forth in Section 523(a)(19) of the Bankruptcy Code, 11 U.S.C. § 523(a)(19).

By the Commission.

Brent J. Fields  
Secretary

**UNITED STATES OF AMERICA**  
**Before the**  
**SECURITIES AND EXCHANGE COMMISSION**

**INVESTMENT ADVISERS ACT OF 1940**  
**Release No. 4998 / August 27, 2018**

**ADMINISTRATIVE PROCEEDING**  
**File No. 3-18683**

**In the Matter of**

**KEVIN A. GILES**

**Respondent.**

**ORDER INSTITUTING CEASE-AND-DESIST  
PROCEEDINGS, PURSUANT TO SECTION  
203(k) OF THE INVESTMENT ADVISERS  
ACT OF 1940, MAKING FINDINGS, AND  
IMPOSING A CEASE-AND-DESIST ORDER**

**I.**

The Securities and Exchange Commission (“Commission”) deems it appropriate and in the public interest that public cease-and-desist proceedings be, and hereby are, instituted pursuant to Section 203(k) of the Investment Advisers Act of 1940 (“Advisers Act”) against Kevin A. Giles (“Giles” or “Respondent”).

**II.**

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the “Offer”) which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission’s jurisdiction over him and the subject matter of these proceedings, which are admitted, and except as provided herein in Section V, Respondent consents to the entry of this Order Instituting Cease-and-Desist Proceedings, Pursuant to Section 203(k) of the Investment Advisers Act of 1940, Making Findings, and Imposing a Cease-and-Desist Order (“Order”), as set forth below.

### III.

On the basis of this Order and Respondent's Offer, the Commission finds<sup>1</sup> that:

#### **Summary**

1. Between July 2011 and June 2015, AEGON USA Investment Management, LLC ("AUIM"), a registered investment adviser, violated certain provisions of the federal securities laws in connection with the offer, sale, and management of three mutual funds and six variable life insurance investment portfolios and variable annuity investment portfolios ("Investment Portfolios") that employed quantitative models for allocation and trading decisions (collectively, the "Products").<sup>2</sup> Among those violations, AUIM failed to adopt and implement certain compliance policies and procedures, including failing to take reasonable steps to ensure that: (1) its quantitative models worked as intended both before the Products' launched and on a periodic basis after they launched; (2) it adopted and implemented reasonable controls regarding the testing, approval, and documentation of any changes to its quantitative models; and (3) the Products' portfolio managers' discretion to depart from model-directed trades was defined, monitored, and documented. Each of these risks was identified in a November 2011 internal audit report, and Giles agreed to be responsible for addressing them, but failed to do so. As a result, Respondent was a cause of AUIM's compliance failures.

#### **Respondent**

2. Kevin A. Giles, age 55, is a resident of Iowa and was AUIM's Director of New Initiatives from October 2006 through July 2015.

#### **Other Relevant Entities**

3. **AEGON USA Investment Management, LLC ("AUIM")** (SEC File No. 801-60667) is registered with the Commission as an investment adviser and is headquartered in Cedar Rapids, Iowa. AUIM is a wholly owned indirect subsidiary of Aegon N.V., a multinational insurance and asset management company headquartered in the Netherlands, and is an affiliate of Transamerica Asset Management, Inc. ("TAM"). AUIM currently has more than \$106 billion in assets under management. AUIM acted as the sub-adviser to the Products, under the supervision of TAM, which was the adviser to the Products.

4. **Transamerica Asset Management, Inc. ("TAM")** (SEC File No. 801-53319) is registered with the Commission as an investment adviser and is headquartered in Denver,

---

<sup>1</sup> The findings herein are made pursuant to Respondent's Offer of Settlement and are not binding on any other person or entity in this or any other proceeding.

<sup>2</sup> See *In the Matter of AEGON USA Investment Management, LLC, et al.*, Admin. Proc. File No. 3-18681 (Aug. 27, 2018) (the "Aegon Proceeding").

Colorado. TAM is an indirect subsidiary of Aegon N.V. and an affiliate of AUIM. TAM currently has more than \$79 billion in assets under management. TAM acted as the adviser to the Products and hired AUIM to act as sub-adviser to the Products.

### **Facts**

5. As Director of New Initiatives at AUIM, Giles was responsible for identifying and developing opportunities for AUIM to manage third-party assets. Giles worked with TAM to develop investment vehicles that AUIM could manage as a sub-adviser to TAM, including all of the Products. After TAM decided to offer a product suggested by AUIM, Giles would work with the AUIM project management team to sign off on the reasonableness of their development plans and led efforts to design, build, and launch products.

6. By the fall of 2011, because of the significant growth of assets under management in the Investment Portfolios, senior management at AUIM requested the help of an affiliated insurance company internal audit team to conduct an audit of the control environment supporting these six products.

7. On October 6, 2011, the audit team issued an interim status report to Giles and AUIM's Chief Investment Officer ("CIO"). The interim status report identified certain risks concerning AUIM's use of quantitative models, including that:

(i) "AUIM does not have formal controls or policies and procedures to ensure quantitative model development is controlled and models function as expected";

(ii) "AUIM does not periodically perform independent validation of modeling results to ensure the integrity of [the Investment Portfolios'] models remains intact," and therefore "transparency to modeling errors is potentially impaired and at worst may be concealed"; and

(iii) "AUIM has not formally defined the discretion Portfolio Managers have in managing [the Investment Portfolios] regarding trade orders not aligned with modeling results."

8. On or about October 10, 2011, Giles and AUIM's CIO met with the internal auditors to discuss the interim status report. During this and subsequent meetings, Giles and AUIM's CIO were designated as the AUIM management employees responsible for addressing each of the risks identified in the interim status report.

9. On November 4, 2011, the internal audit team issued a final report that included the three risks concerning AUIM's use of quantitative models identified in Paragraph 7, above. This report identified Giles and AUIM's CIO as the members of management responsible for: (i) the implementation of internal controls and other policies and procedures to address each of the identified risks; (ii) the execution of specific steps to address these risks; and (iii) the establishment of specific dates by which such steps would be completed.

10. After Giles and AUIM's CIO were designated with responsibility for the implementation of internal controls and other policies and procedures to address each of the identified risks, AUIM launched three mutual funds that employed models developed from the same quantitative models used to manage the Investment Portfolios studied in the audit. As Director of New Initiatives, Giles led efforts to prepare these mutual funds for launch.

11. AUIM failed to adopt or implement policies and procedures to address the risks identified in the internal audit before launching the mutual funds and for many months after launching all of the Products.

12. Giles failed to take reasonable steps to revise AUIM's policies and procedures. For example, though Giles was one of those responsible for addressing the risks related to model validation and model functioning, he failed to take reasonable steps to accomplish this. AUIM failed to adopt a policy requiring model validation until July 2013 and began validating the quantitative models used to make allocation decisions in the Products only at that point — nearly two years after the launch of the first mutual fund and nearly a year after the launches of the second and third mutual funds.

13. As a result of the negligent conduct described above, Giles was a cause of AUIM's violations of Section 206(4) of the Advisers Act and Rule 206(4)-7 promulgated thereunder, which require a registered investment adviser to adopt and implement written policies and procedures reasonably designed to prevent violations of the Advisers Act and its rules, and to review, no less frequently than annually, the adequacy of the policies and procedures and the effectiveness of their implementation.

#### IV.

In view of the foregoing, the Commission deems it appropriate and in the public interest to impose the sanctions agreed to in Respondent's Offer.

Accordingly, pursuant to Section 203(k) of the Advisers Act, it is hereby ORDERED that:

A. Respondent Giles shall cease and desist from committing or causing any violations and any future violations of Section 206(4) of the Advisers Act and Rule 206(4)-7 promulgated thereunder.

B. Respondent Giles shall, within 30 days of the entry of this Order, pay a civil money penalty in the amount of \$25,000.00 to the Fair Fund established in the Aegon Proceeding for distribution to affected investors. The \$25,000 shall be deposited into the same escrow account established in the Aegon Proceeding.

Payments by check or money order must be accompanied by a cover letter identifying Kevin A. Giles as a Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to Paul A. Montoya, Division of

Enforcement, Securities and Exchange Commission, 175 West Jackson Blvd., Suite 1450, Chicago, IL 60604.

C. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondent agrees that in any Related Investor Action, he shall not argue that he is entitled to, nor shall he benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondent's payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondent agrees that he shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondent by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

## V.

It is further Ordered that, solely for purposes of exceptions to discharge set forth in Section 523 of the Bankruptcy Code, 11 U.S.C. § 523, the findings in this Order are true and admitted by Respondent, and further, any debt for disgorgement, prejudgment interest, civil penalty or other amounts due by Respondent under this Order or any other judgment, order, consent order, decree or settlement agreement entered in connection with this proceeding, is a debt for the violation by Respondent of the federal securities laws or any regulation or order issued under such laws, as set forth in Section 523(a)(19) of the Bankruptcy Code, 11 U.S.C. § 523(a)(19).

By the Commission.

Brent J. Fields  
Secretary

# Tab 19





# NATIONAL EXAM PROGRAM

## RISK ALERT

By the Office of Compliance Inspections and Examinations\*

October 31, 2018

### Investment Adviser Compliance Issues Related to the Cash Solicitation Rule

**Key Takeaway:**  
*Advisers should review their practices and policies to ensure compliance with the Cash Solicitation Rule.*

#### I. Introduction

The Office of Compliance Inspections and Examinations (“OCIE”) is issuing this Risk Alert to provide investment advisers, investors and other market participants with information concerning the most common deficiencies the staff has cited relating to Rule 206(4)-3 (the “Cash Solicitation Rule”) under the Investment Advisers Act of 1940 (the “Advisers Act”).<sup>1</sup> This Risk Alert includes observations by OCIE staff and is intended to assist investment advisers in identifying potential issues and adopting and implementing effective compliance programs.<sup>2</sup>

In general, investment advisers required to be registered under the Advisers Act (“advisers”) are prohibited from paying a cash fee, directly or indirectly, to any person who solicits clients for the adviser (a “solicitor”) unless the arrangement complies with a number of conditions.<sup>3</sup> Among other things, the cash fee must be paid pursuant to a written agreement to which the adviser is a party (the “solicitation agreement”).<sup>4</sup> The solicitor may not be a person subject to certain disqualifications specified in the Cash Solicitation Rule.

There are additional requirements when the solicitor is not a partner, officer, director or employee of the adviser or of an entity that controls, is controlled by, or is under common control with, the adviser (a “third-party solicitor”).<sup>5</sup> The Cash Solicitation Rule imposes the

\* The views expressed herein are those of the staff of OCIE. The Securities and Exchange Commission (the “SEC” or the “Commission”) has expressed no view on the contents of this Risk Alert. This document was prepared by OCIE staff and is not legal advice.

<sup>1</sup> This Risk Alert reflects issues identified during a review of deficiency letters from investment adviser examinations completed during the past three years.

<sup>2</sup> The SEC has brought enforcement actions charging advisers with violations of the Cash Solicitation Rule. *See, e.g., In the Matter of Essex Fin. Servs., Inc.*, Advisers Act Rel. No. 4603 (Jan. 9, 2017) (settled order) (finding that adviser violated the Cash Solicitation Rule by paying a cash fee to a solicitor despite knowing that the solicited clients had not received the necessary disclosures).

<sup>3</sup> Advisers Act Rule 206(4)-3.

<sup>4</sup> A copy of the solicitation agreement must be retained by the adviser under Advisers Act Rule 204-2(a)(15).

<sup>5</sup> Advisers are subject to narrower requirements under the Cash Solicitation Rule when (1) the solicitor is a partner, officer, director or employee of the adviser or of an entity that controls, is controlled by, or is under

following additional requirements when an adviser uses a third-party solicitor:

- (1) the solicitation agreement must contain certain specified provisions (e.g., a description of the solicitation activities and compensation to be received);
- (2) the solicitation agreement must require that, at the time of any solicitation activities, the solicitor provide the prospective client with a copy of (a) the adviser's brochure pursuant to Advisers Act Rule 204-3 ("adviser brochure") and (b) a separate, written disclosure document containing required information that highlights the solicitor's financial interest in the client's choice of an adviser (the "solicitor disclosure document");
- (3) the adviser must receive from the client, before or at the time of entering into any written or oral agreement with the client, a signed and dated acknowledgment that the client received the adviser brochure and the solicitor disclosure document ("client acknowledgement"); and
- (4) the adviser must make a bona fide effort to ascertain whether the solicitor has complied with the solicitation agreement, and must have a reasonable basis for believing that the solicitor has so complied.<sup>6</sup>

## II. Most Frequent Compliance Issues Related to the Cash Solicitation Rule

Below are some of the most frequent deficiencies that OCIE staff has identified pertaining to the Cash Solicitation Rule.<sup>7</sup>

- *Solicitor disclosure documents.* OCIE staff observed advisers whose third-party solicitors did not provide solicitor disclosure documents to prospective clients or provided solicitor disclosure documents that did not contain all the information required by the Cash Solicitation Rule. For example, staff observed solicitor disclosure documents that did not:
  - Disclose the nature of the relationship, including any affiliation, between the solicitor and the adviser.
  - Contain the terms of the compensation arrangement between the adviser and the solicitor.
  - Specify the actual compensation terms agreed to in the solicitation agreement and instead used vague or hypothetical terms to describe the solicitor's compensation.

---

common control with, the adviser or (2) the cash fee is paid with respect to solicitation activities for the provision of impersonal advisory services only. Advisers Act Rule 206(4)-3(a)(2)(i)-(ii). This Risk Alert generally includes observations relating to an adviser's use of third-party solicitors subject to the broader requirements of the Cash Solicitation Rule.

<sup>6</sup> Advisers Act Rule 206(4)-3(a)(2)(iii).

<sup>7</sup> This Risk Alert does not address all deficiencies or weaknesses related to the Cash Solicitation Rule that have been identified by OCIE staff.

- Specify the additional solicitation cost the solicited client will be charged in addition to the advisory fee.
- *Client acknowledgements.* OCIE staff observed advisers that did not timely receive a signed and dated client acknowledgement of receipt of the adviser brochure and the solicitor disclosure document.<sup>8</sup> Staff also observed advisers that received client acknowledgements, but such client acknowledgements were undated or dated after the clients had entered into an investment advisory contract.
- *Solicitation agreements.* OCIE staff observed advisers that paid cash fees to a solicitor without a solicitation agreement in effect or pursuant to an agreement that did not contain certain specific provisions.<sup>9</sup> For example, staff observed solicitation agreements with third-party solicitors that did not:
  - Contain an undertaking by the solicitor to perform its duties under the solicitation agreement in a manner consistent with the instructions of the adviser.
  - Describe the solicitor's activities and the compensation to be paid.
  - Oblige solicitors to provide clients (including prospective clients) with a current copy of the adviser brochure and the solicitor disclosure document.
- *Bona fide efforts to ascertain solicitor compliance.* OCIE staff observed advisers that did not make a bona fide effort to ascertain whether third-party solicitors complied with solicitation agreements and appeared to not have a reasonable basis for believing that the third-party solicitors so complied.<sup>10</sup> For example, staff observed advisers that were unable to describe any efforts they took to confirm compliance with solicitation agreements.

OCIE also observed advisers with similar conflicts that may implicate other provisions of the Advisers Act, such as an adviser's fiduciary duty under Sections 206(1) and 206(2). For example, OCIE observed advisers that recommended service providers to clients in exchange for client referrals without full and fair disclosure of the conflicts of interest.

### III. Conclusion

The examinations within the scope of this review resulted in a range of actions. In response to the staff's observations, some advisers elected to amend their disclosure documents and solicitation agreements, revise their compliance policies and procedures, or otherwise change their practices regarding the Cash Solicitation Rule.

---

<sup>8</sup> Advisers Act Rule 206(4)-3(a)(2)(iii)(B).

<sup>9</sup> Advisers Act Rule 206(4)-3(a)(2)(iii)(A).

<sup>10</sup> Advisers Act Rule 206(4)-3(a)(2)(iii)(C).

In sharing the information in this Risk Alert, OCIE encourages advisers to review their practices, policies, and procedures in these areas and to promote improvements in adviser compliance programs.




---

*This Risk Alert is intended to highlight for firms risks and issues that OCIE staff has identified. In addition, this Risk Alert describes risks that firms may consider to (i) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm's business. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.*

---

# Morgan Lewis

At Morgan Lewis, we see our clients as partners. Whether you've been with us for days or decades, whether you're today's industry leader or tomorrow's game-changer, we're always responsive and always on.

Connect with us:   

**[www.morganlewis.com](http://www.morganlewis.com)**

© 2018 Morgan, Lewis & Bockius LLP

© 2018 Morgan Lewis Stamford LLC

© 2018 Morgan, Lewis & Bockius UK LLP

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

\*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners.

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising.

