Office of the Comptroller of the Currency
U.S. Department of the Treasury

OCC BULLETIN 2017-21

Subject: Third-Party Relationships
Date: June 7, 2017

To: Chief Executive Officers and Chief Risk Officers of All National Banks and Federal Savings Associations, Technology Service Providers, Department and Division Heads, All Examining Personnel, and Other Interested Parties

Description: Frequently Asked Questions to Supplement OCC Bulletin 2013-29

Summary

The Office of the Comptroller of the Currency (OCC) is issuing frequently asked questions (FAQ) to supplement OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," issued October 30, 2013.

Note for Community Banks

This bulletin addresses questions from national banks and federal savings associations (collectively, banks) regarding guidance in OCC Bulletin 2013-29. This bulletin and OCC Bulletin 2013-29 are applicable to all banks..

1. What is a third-party relationship?

OCC Bulletin 2013-29 defines a third-party relationship as any business arrangement between the bank and another entity, by contract or otherwise. Third-party relationships include activities that involve outsourced products and services; use of outside consultants, 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. Recently, many banks have developed relationships with financial technology (fintech) companies that involve some of these activities, including performing services or delivering products to a bank's customer base. If a fintech company performs services or delivers products on behalf of a bank or banks, the relationship meets the definition of a third-party relationship and the OCC would expect bank management to include the fintech company in the bank's third-party risk management process.

Bank management should conduct in-depth due diligence and ongoing monitoring of each of the bank's third-party service providers that support critical activities. The OCC realizes that although banks may want in-depth information, they may not receive all the information they seek on each critical third-party service provider, particularly from new companies. When a bank does not receive all the information it seeks about third-party service providers that support the bank's critical activities, the OCC expects the bank's board of directors and management to

- develop appropriate alternative ways to analyze these critical third-party service providers.
- establish risk-mitigating controls.

- be prepared to address interruptions in delivery (for example, use multiple payment systems, generators for power, and multiple telecommunications lines in and out of critical sites).
- make risk-based decisions that these critical third-party service providers are the best service providers available to the bank despite the fact that the bank cannot acquire all the information it wants.
- retain appropriate documentation of all their efforts to obtain information and related decisions.
- ensure that contracts meet the bank's needs.

2. OCC Bulletin 2013-29 defines third-party relationships very broadly and reads like it can apply to lower-risk relationships. How can a bank reduce its oversight costs for lower-risk relationships?

Not all third-party relationships present the same level of risk. The same relationship may present varying levels of risk across banks. Bank management should determine the risks associated with each third-party relationship and then determine how to adjust risk management practices for each relationship. The goal is for the bank's risk management practices for each relationship to be commensurate with the level of risk and complexity of the third-party relationship. This risk assessment should be periodically updated throughout the relationship. It should not be a one-time assessment conducted at the beginning of the relationship.

The OCC expects banks to perform due diligence and ongoing monitoring for all third-party relationships. The level of due diligence and ongoing monitoring, however, may differ for, and should be specific to, each third-party relationship. The level of due diligence and ongoing monitoring should be consistent with the level of risk and complexity posed by each third-party relationship. For critical activities, the OCC expects that due diligence and ongoing monitoring will be robust, comprehensive, and appropriately documented. Additionally, for activities that bank management determines to be low risk, management should follow the bank's board-established policies and procedures for due diligence and ongoing monitoring.

3. How should banks structure their third-party risk management process?

There is no one way for banks to structure their third-party risk management process. OCC Bulletin 2013-29 notes that the OCC expects banks to adopt an effective third-party risk management process commensurate with the level of risk and complexity of their third-party relationships. Some banks have dispersed accountability for their third-party risk management process among their business lines. Other banks have centralized the management of the process under their compliance, information security, procurement, or risk management functions. No matter where accountability resides, each applicable business line can provide valuable input into the third-party risk management process, for example, by completing risk assessments, reviewing due diligence questionnaires and documents, and evaluating the controls over the third-party relationship. Personnel in control functions such as audit, risk management, and compliance programs should be involved in the management of third-party relationships. However a bank structures its third-party risk management process, the board is responsible for overseeing the development of an effective third-party risk management process commensurate with the level of risk and complexity of the third-party relationships. Periodic board reporting is essential to ensure that board responsibilities are fulfilled.

4. When multiple banks use the same third-party service providers, can they collaborate[1] to meet expectations for managing third-party relationships specified in OCC Bulletin 2013-29?

If they are using the same service providers to secure or obtain like products or services, banks may collaborate[2] to meet certain expectations, such as performing the due diligence, contract negotiation, and ongoing monitoring responsibilities described in OCC Bulletin 2013-29. Like products and services may, however, present a different level of risk to each bank that uses those products or services, making collaboration a useful tool but insufficient to fully meet the bank's responsibilities under OCC Bulletin 2013-29. Collaboration can leverage resources by distributing costs across multiple banks. In addition, many banks that use like products and services from technology or other service providers may become members of user groups. Frequently, these user groups create the opportunity for banks, particularly community banks, to collaborate with their peers on innovative product ideas, enhancements to existing

products or services, and customer service and relationship management issues with the service providers. Banks that use a customized product or service may not, however, be able to use collaboration to fully meet their due diligence, contract negotiation, or ongoing responsibilities.

Banks may take advantage of various tools designed to help them evaluate the controls of third-party service providers. In general, these types of tools offer standardized approaches to perform due diligence and ongoing monitoring of third-party service providers by having participating third parties complete common security, privacy, and business resiliency control assessment questionnaires. After third parties complete the questionnaires, the results can be shared with numerous banks and other clients. Collaboration can result in increased negotiating power and lower costs to banks during the contract negotiation phase of the risk management life cycle.

Some community banks have joined an alliance to create a standardized contract with their common third-party service providers and improve negotiating power.

5. When collaborating to meet responsibilities for managing a relationship with a common third-party service provider, what are some of the responsibilities that each bank still needs to undertake individually to meet the expectations in OCC Bulletin 2013-29?

While collaborative arrangements can assist banks with their responsibilities in the life cycle phases for third-party risk management, each individual bank should have its own effective third-party risk management process tailored to each bank's specific needs. Some individual bank-specific responsibilities include defining the requirements for planning and termination (e.g., plans to manage the third-party service provider relationship and development of contingency plans in response to termination of service), as well as

- integrating the use of product and delivery channels into the bank's strategic planning process and ensuring consistency with the bank's internal controls, corporate governance, business plan, and risk appetite.
- assessing the quantity of risk posed to the bank through the third-party service provider and the ability of the bank to monitor and control the risk.
- implementing information technology controls at the bank.
- ongoing benchmarking of service provider performance against the contract or service-level agreement.
- evaluating the third party's fee structure to determine if it creates incentives that encourage inappropriate risk taking.
- monitoring the third party's actions on behalf of the bank for compliance with applicable laws and regulations.
- monitoring the third party's disaster recovery and business continuity time frames for resuming activities and recovering data for consistency with the bank's disaster recovery and business continuity plans.

6. What collaboration opportunities exist to address cyber threats to banks as well as to their third-party relationships?

Banks may engage with a number of information-sharing organizations to better understand cyber threats to their own institutions as well as to the third parties with whom they have relationships. Banks participating in information-sharing forums have improved their ability to identify attack tactics and successfully mitigate cyber attacks on their systems. Banks may use the Financial Services Information Sharing and Analysis Center (FS-ISAC), the U.S. Computer Emergency Readiness Team (US-CERT), InfraGard, and other information-sharing organizations to monitor cyber threats and vulnerabilities and to enhance their risk management and internal controls. Banks also may use the FS-ISAC to share information with other banks.

7. Is a fintech company arrangement considered a critical activity?

A bank's relationship with a fintech company may or may not involve critical bank activities, depending on a number of factors. OCC Bulletin 2013-29 provides criteria that a bank's board and management may use to determine what critical activities are. It is up to each bank's board and management to identify the

critical activities of the bank and the third-party relationships related to these critical activities. The board (or committees thereof) should approve the policies and procedures that address how critical activities are identified. Under OCC Bulletin 2013-29, critical activities can include significant bank functions (e.g., payments, clearing, settlements, and custody), significant shared services (e.g., information technology), or other activities that

- could cause the bank to face significant risk if a third party fails to meet expectations.
- could have significant bank customer impact.
- require significant investment in resources to implement third-party relationships and manage risks.
- could have major impact on bank operations if the bank has to find an alternative third party or if the outsourced activities have to be brought in-house.

The OCC expects banks to have more comprehensive and rigorous management of third-party relationships that involve critical activities.

8. Can a bank engage with a start-up fintech company with limited financial information?

OCC Bulletin 2013-29 states that banks should consider the financial condition of their third parties during the due diligence stage of the life cycle before the banks have selected or entered into contracts or relationships with third parties. In assessing the financial condition of a start-up or less established fintech company, the bank may consider a company's access to funds, its funding sources, earnings, net cash flow, expected growth, projected borrowing capacity, and other factors that may affect the third party's overall financial stability. Assessing changes to the financial condition of third parties is an expectation of the ongoing monitoring stage of the life cycle. Because it may be receiving limited financial information, the bank should have appropriate contingency plans in case the start-up fintech company experiences a business interruption, fails, or declares bankruptcy and is unable to perform the agreed-upon activities or services.

Some banks have expressed confusion about whether third-party service providers need to meet a bank's credit underwriting guidelines. OCC Bulletin 2013-29 states that depending on the significance of the third-party relationship, a bank's analysis of a third party's financial condition may be as comprehensive as if the bank were extending credit to the third-party service provider. This statement may have been misunderstood as meaning a bank may not enter into relationships with third parties that do not meet the bank's lending criteria. There is no such requirement or expectation in OCC Bulletin 2013-29.

9. How can a bank offer products or services to underbanked or underserved segments of the population through a third-party relationship with a fintech company?

Banks have collaborated with fintech companies in several ways to help meet the banking needs of underbanked or underserved consumers. Banks may partner with fintech companies to offer savings, credit, financial planning, or payments in an effort to increase consumer access. In some instances, banks serve only as facilitators for the fintech companies' products or services with one of the products or services coming from the banks. For example, several banks have partnered with fintech companies to establish dedicated interactive kiosks or automated teller machines (ATM) with video services that enable the consumer to speak directly to a bank teller. Frequently, these interactive kiosks or ATMs are installed in retail stores, senior community centers, or other locations that do not have branches to serve the community. Some fintech companies offer other ways for banks to partner with them. For example, a bank's customers can link his or her savings account with the fintech company's application, which can offer incentives to the bank's customers to save for short-term emergencies or achieve specific savings goals.

In these examples, the fintech company is considered to have a third-party relationship with the bank that falls under the scope of OCC Bulletin 2013-29.

10. What should a bank consider when entering a marketplace lending arrangement with nonbank entities?

When engaging in marketplace lending activities, a bank's board and management should understand the relationships among the bank, the marketplace lender, and the borrowers; fully understand the legal, strategic, reputation, operational, and other risks that these arrangements pose; and evaluate the marketplace lender's practices for compliance with applicable laws and regulations. As with any third-party relationship, management at banks involved with marketplace lenders should ensure the risk exposure is consistent with their boards' strategic goals, risk appetite, and safety and soundness objectives. In addition, boards should adopt appropriate policies, inclusive of concentration limitations, before beginning business relationships with marketplace lenders.

Banks should have the appropriate personnel, processes, and systems so that they can effectively monitor and control the risks inherent within the marketplace lending relationship. Risks include reputation, credit, concentrations, compliance, market, liquidity, and operational risks. For credit risk management, for example, banks should have adequate loan underwriting guidelines, and management should ensure that loans are underwritten to these guidelines. For compliance risk management, banks should not originate or support marketplace lenders that have inadequate compliance management processes and should monitor the marketplace lenders to ensure that they appropriately implement applicable consumer protection laws, regulations, and guidance. When banks enter into marketplace lending or servicing arrangements, the banks' customers may associate the marketplace lenders' products with those of the banks, thereby introducing reputation risk if the products underperform or harm customers. Also, operational risk can increase quickly if the operational processes of the banks and the marketplace lenders do not include appropriate limits and controls, such as contractually agreed-to loan volume limits and proper underwriting.

To address these risks, banks' due diligence of marketplace lenders should include consulting with the banks' appropriate business units, such as credit, compliance, finance, audit, operations, accounting, legal, and information technology. Contracts or other governing documents should lay out the terms of service-level agreements and contractual obligations. Subsequent significant contractual changes should prompt reevaluation of bank policies, processes, and risk management practices.

11. Does OCC Bulletin 2013-29 apply when a bank engages a third party to provide bank customers the ability to make mobile payments using their bank accounts, including debit and credit cards?

When using third-party service providers in mobile payment environments, banks are expected to act in a manner consistent with OCC Bulletin 2013-29. Banks often enter into business arrangements with third-party service providers to provide software and licenses in mobile payment environments. These third-party service providers also provide assistance to the banks and the banks' customers (for example, payment authentication, delivering payment account information to customers' mobile devices, assisting card networks in processing payment transactions, developing or managing mobile software (apps) or hardware, managing back-end servers, or deactivating stolen mobile phones).

Many bank customers expect to use transaction accounts and credit, debit, or prepaid cards issued by their banks in mobile payment environments. Because almost all banks issue debit cards and offer transaction accounts, banks frequently participate in mobile payment environments even if they do not issue credit cards. Banks should work with mobile payment providers to establish processes for authenticating enrollment of customers' account information that the customers provide to the mobile payment providers.

12. May a community bank outsource the development, maintenance, monitoring, and compliance responsibilities of its compliance management system?

Banks may outsource some or all aspects of their compliance management systems to third parties, so long as banks monitor and ensure that third parties comply with current and subsequent changes to consumer laws and regulations. Some banks outsource maintenance or monitoring or use third parties to automate data collection and management processes (for example, to file compliance reports under the Bank Secrecy Act or for mortgage loan application processing or disclosures). The OCC expects all banks to develop and maintain an effective compliance management system and provide fair access to financial services, ensure fair treatment of customers, and comply with consumer protection laws and regulations.

Strong compliance management systems include appropriate policies, procedures, practices, training, internal controls, and audit systems to manage and monitor compliance processes as well as a commitment of appropriate compliance resources.

13. Can banks obtain access to interagency technology service providers' (TSP) reports of examination?

TSP reports of examination[3] are available only to banks that have contractual relationships with the TSPs at the time of the examination. Because the OCC's (and other federal banking regulators') statutory authority is to examine a TSP that enters into a contractual relationship with a regulated financial institution, the OCC (and other federal banking regulators) cannot provide a copy of a TSP's report of examination to financial institutions that are either considering outsourcing activities to the examined TSP or that enter into a contract after the date of examination.

Banks can request TSP reports of examination through the banks' respective OCC supervisory office. TSP reports of examination are provided on a request basis. The OCC may, however, proactively distribute TSP reports of examination in certain situations because of significant concerns or other findings to banks with contractual relationships with that particular TSP.

Although a bank may not share a TSP report of examination or the contents therein with other banks, a bank that has not contracted with a particular TSP may seek information from other banks with information or experience with a particular TSP as well as information from the TSP to meet the bank's due diligence responsibilities.

14. Can a bank rely on a third party's Service Organization Control (SOC) report, prepared in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No. 18 (SSAE 18)?

In meeting its due diligence and ongoing monitoring responsibilities, a bank may review a third party's SOC report prepared in accordance with SSAE 18 to evaluate the effectiveness of the third party's risk management program, including policies, processes, and internal controls.[4] If a third party uses subcontractors (also referred to as fourth parties), a bank may find the third party's SSAE 18 report particularly useful, as SSAE 18 requires the auditor to determine and report on the effectiveness of controls the third party has implemented to monitor the controls of the subcontractor. In other words, the SSAE 18 report will address the question as to whether the third party has effective oversight of its subcontractors. A bank should consider whether an SSAE 18 report contains sufficient information and is sufficient in scope to assess the third party's risk environment or whether additional audit or review is required for the bank to properly assess the third party's control environment.

Further Information

The OCC encourages banks to contact their assigned local field office portfolio manager, assistant deputy comptroller, or appropriate large bank supervision staff members to discuss products and services involving third parties they are considering or to better understand how to meet their responsibilities for managing third-party relationships under OCC Bulletin 2013-29.

For questions regarding this bulletin or OCC Bulletin 2013-29, please contact Judi McCormick, Governance and Operational Risk Policy Analyst, Operational Risk Policy Division, at (202) 649-6550. The OCC intends to review banks' questions on OCC Bulletin 2013-29 from time to time and issue future FAQs or other guidance when it deems necessary.

Bethany A. Dugan
Deputy Comptroller for Operational Risk

[1] Refer to OCC News Release 2015-1, "Collaboration Can Facilitate Community Banks Competitiveness, OCC Says," January 13, 2015.

[2] Any collaborative activities among banks must comply with antitrust laws. Refer to the Federal Trade Commission and U.S. Department of Justice's "Antitrust Guidelines for Collaborations Among Competitors."

[3] The OCC conducts examinations of services provided by significant TSPs based on authorities granted by the Bank Service Company Act, 12 USC 1867. These examinations typically are conducted in coordination with the Board of Governors of the Federal Reserve Board, Federal Deposit Insurance Corporation, and other banking agencies with similar authorities. The scope of examinations focus on the services provided and key technology and operational controls communicated in the *FFIEC Information Technology Examination Handbook* and other regulatory guidance.

[4] As of May 2017, SSAE 18 replaced SSAE 16 for SOC 1 engagements.