
Morgan Lewis
LITIGATION AND ENFORCEMENT DEVELOPMENTS IN CONNECTION WITH ACCESS AND USE OF DATA
Richard S. Taffet
Bryan R. Woll
May 14, 2020
© 2020 Morgan, Lewis & Bockius LLP

# Before we begin: Morgan Lewis and Global Technology

Be sure to follow us at our website and on social media:

**Web:** **www.morganlewis.com/sectors/technology**

**Twitter:** **@MLGlobalTech**

**LinkedIn Group:** **ML Global Tech**

Check back to our Technology May-rathon page frequently for updates and events covering the following timely topics:

| | | |
|---|---|---|
| **21st Century Workplace** | **Cybersecurity, Privacy and Big Data** | **Medtech, Digital Health and Science** |
| **Artificial Intelligence and Automation** | **Fintech** | **Mobile Tech** |
| **COVID-19** | **Global Commerce** | **Regulating Tech** |

# Litigation and Enforcement Developments in Connection with Access and Use of Data

This presentation will discuss the following topics:

1. The Growth in Financial Institutions' Use of Technology (FinTech)
2. Consumer Expectations About the Security of Their Financial Data
3. Federal and State Enforcement Responses
4. Private Consumer and Commercial Litigation

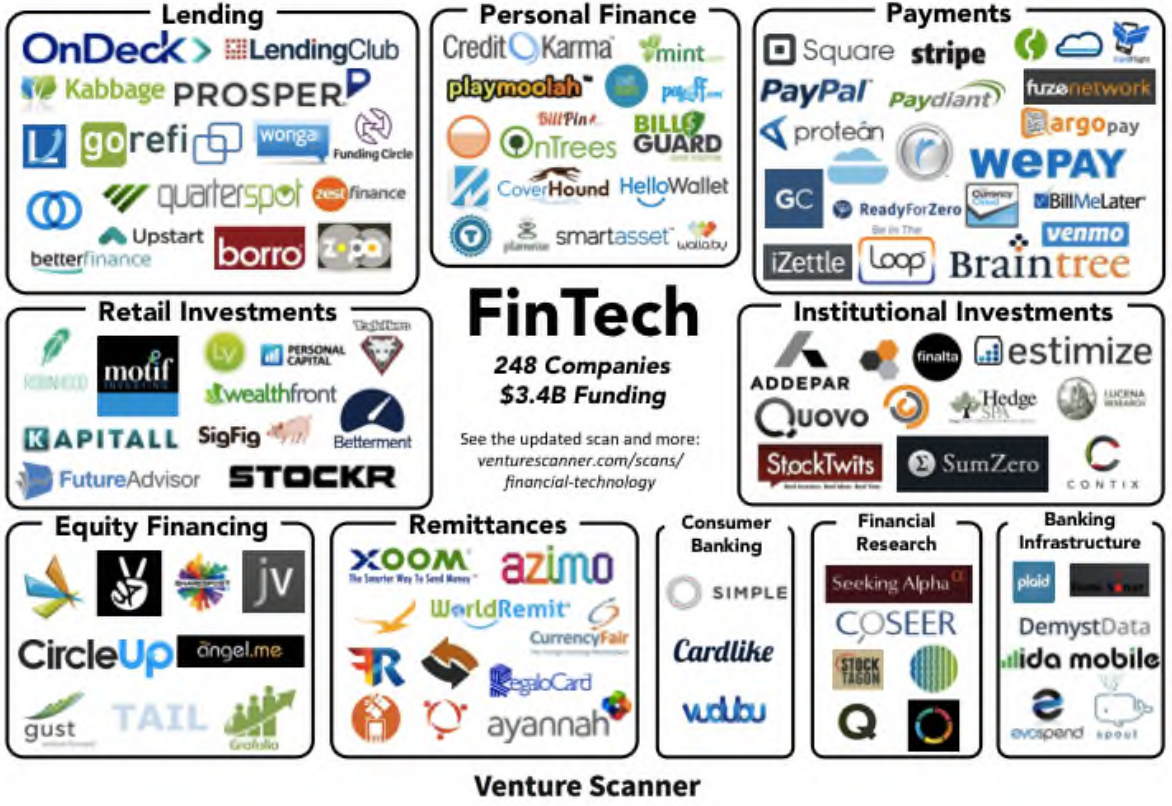
# FINTECH GROWTH AND CONSUMER EXPECTATIONS

# Rapid Growth in the FinTech Space

- "FinTech" describes technology-enabled innovation in financial services. FinTechs promise to expand access to credit and financial services, increase speed and convenience, and reduce costs of financial services by leveraging technology.
- The biggest FinTech market segment is **digital payments**, with an expected total transaction value of over $4 trillion in 2019 worldwide, and nearly $1 trillion in the United States alone.
- "**Overall investment in FinTech** surged in 2018, **hitting $55 billion worldwide**, double the year before." [Forbes]
- Many traditional financial services companies also developing FinTech businesses.

# The Biggest FinTech Companies in the U.S.

- Stripe
- Ripple
- Coinbase
- Robinhood
- Chime
- Plaid
- SoFi
- Credit Karma
- Opendoor
- Root




Jeff Kauflin, *The 10 Biggest Fintech Companies in America 2020*, FORBES (Feb. 12, 2020), https://www.forbes.com/sites/jeffkauflin/2020/02/12/the-10-biggest-fintech-companies-in-america-2020/#18ce5ee21259

# Interdependence Between FinTechs and Traditional Financial Services Providers

- Many FinTechs depend on interconnection with and access to traditional financial services providers and services:
  - Interconnections with traditional financial services products and providers are important for many FinTech business models:
    - Need access to bank accounts, brokerage accounts, etc. of customers.
    - Use existing payment rails – e.g., real-time, ACH, wire, checks.
  - Utilize consumer data held by financial services firms to support business models – e.g., mobile wallets, payment processing, data aggregation.
    - Financial services firms hold substantial consumer information.
    - Data-driven business models for FinTechs.

# Consumers' Adoption and Expectations of FinTech

- Hhalf of all consumers (54%) use financial apps, and 7 out of 10 believe their data is "private and secure."
- But there is a "growing disconnect" between consumers' expectations about the privacy of their financial data and reality.

| | |
|---|---|
| "Less than 20% of users are aware that the apps may use third parties to access consumers' personal and financial information."<br><br>"80% are not fully aware that the apps or third parties may store their bank account username and password."<br><br>Only "21% are aware that financial apps have access to their data until they revoke their bank account username and password." | **"Nearly two-thirds of users (65%) express discomfort with these arrangements."** |

THE CLEARING HOUSE, CONSUMER SURVEY: FINANCIAL APPS AND DATA PRIVACY (Nov. 2019), https://www.theclearinghouse.org/payment-systems/articles/2019/11/-/media/ec23413b9f98467ea7bdf55e93854278.ashx.

# Effects of the Disconnect Between Consumers' Privacy Expectations and Reality

- **Consumers may avoid using FinTech products.**
  - 53% of consumers "are less likely to continue using financial apps" once they understand the ***extent to which apps have access*** to their information and how those apps ***use and share that data***.
  - The share of consumers reducing financial app use because of data security concerns varies by age:
    - 63% of consumers over 45 years old
    - 47% of consumers between 18 and 34 years old
- **Majority of the public supports stronger controls on how apps use consumer data.**
  - 65% of consumers want financial apps to provide clear disclosures about third parties' access to their personal and financial information.
  - 59% support giving consumers more control of how apps use and access their data.

THE CLEARING HOUSE, CONSUMER SURVEY: FINANCIAL APPS AND DATA PRIVACY (Nov. 2019), https://www.theclearinghouse.org/payment-systems/articles/2019/11/-/media/ec23413b9f98467ea7bdf55e93854278.ashx.

# Data-Related Trends in the COVID-19 Crisis

- **Consumers and business are poised to increase their use of digital banking and other FinTech applications as they adjust to daily work and life routines confined to the home.**
  - 80% of consumers report anxiety about visiting their bank in the midst of the pandemic.
  - 63% of consumers stated that they have been more inclined to use a FinTech app since the crisis began.
  - Early evidence from one European financial services firm showed a 72% increase in use of its FinTech apps.
- **The federal government's response to COVID-19 may also facilitate greater adoption of FinTech.**
  - FinTech lenders were authorized to make small business loans alongside traditional lenders as part of the federal recovery package.
  - The IRS has allowed some citizens to receive their $1,200 stimulus check via apps like Cash App and Venmo.

*See* Jim Dobbs, *Coronavirus Throws Digital Banking into the Crucible*, AM. BANKER (Mar. 19, 2020), https://www.americanbanker.com/news/coronavirus-throws-digital-banking-into-the-crucible; Simon Chandler, *Coronavirus Drives 72% Rise In Use Of Fintech Apps*, Forbes (Mar. 30, 2020), https://www.forbes.com/sites/simonchandler/2020/03/30/coronavirus-drives-72-rise-in-use-of-fintech-apps/#48a8271b66ed; Jen Wieczner, *The Coronavirus Crisis is Fintech's Biggest Test Yet—And Greatest Opportunity To Go Mainstream,* FORTUNE (Apr. 15, 2020), https://fortune.com/2020/04/15/fintech-coronavirus-stimulus-checks-loans-paypal-square-chime-stripe-sofi/.

# Data-Related Trends in the COVID-19 Crisis

- **Changes in how people work and live during the crisis may expose businesses' existing security vulnerabilities.**
  - For example, the dramatic rise in usage of video conference service Zoom and the resulting scrutiny of its privacy practices have already led to several lawsuits. Plaintiffs in these cases allege that, among other things, Zoom used substandard encryption and allowed Facebook and others to track users.
- **Cybercriminals may take advantage of the current crisis.**
  - There have been reports of phishing schemes using fake communications from the CDC and WHO about COVID-19.
  - The rise in remote working means that employees may be using unsecure internet connections and otherwise not practicing the same level of cybersecurity diligence as they would if they were in the office.
- **The increased demands of business continuity efforts on company leadership and security professionals during the crisis may divert attention and resources from important data security practices—risking future litigation and enforcement actions as a result.**

*See* Debra Cassens Weiss, *Another Lawsuit Is Filed Against Zoom Over Alleged Privacy Problems*, ABA JOURNAL (Apr. 14, 2020), https://www.abajournal.com/news/article/another-lawsuit-is-filed-against-zoom-over-alleged-privacy-problems; Ben Kochman, *How Cybercriminals Are Exploiting The Coronavirus Outbreak,* LAW360 (Mar. 20, 2020), https://www.law360.com/articles/1255130/how-cybercriminals-are-exploiting-the-coronavirus-outbreak; *Multiple Phishing Attacks Discovered Using the Coronavirus Theme*, TRUSTWAVE (Feb. 13, 2020), https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/multiple-phishing-attacks-discovered-using-the-coronavirus-theme/.

# FEDERAL ENFORCEMENT RESPONSES

# Federal Enforcement Responses

- **Federal Trade Commission Enforcement Actions**
  - The U.S. Federal Trade Commission (FTC) is an independent federal agency tasked with protecting consumers and enhancing competition in markets.
  - Section 5(a) of the Federal Trade Commission Act (FTC Act) provides the FTC with authority to take enforcement action on data and privacy issues.
    - This statute makes **"unfair or deceptive acts or practices"** unlawful.
    - The FTC also enforces various other consumer protection statutes.
  - FTC brings an **enforcement action** when it determines that there is "reason to believe" that a violation of law has occurred. In the data and privacy context, the FTC uses enforcement actions to obtain orders that:
    - Prevent a company from continuing its unlawful conduct; and
    - Require it to take affirmative, remedial actions—like establishing privacy programs.

# Federal Enforcement Responses

- ***LabMD, Inc. v. Fed. Trade Comm'n***, 894 F.3d 1221 (11th Cir. 2018).
  - In 2018, the Court of Appeals for the Eleventh Circuit invalidated as insufficiently specific an FTC order directing LabMD to take certain actions relating to its data security program.
  - LabMD, now defunct, was a medical company that provided diagnostic testing services for various cancers. The FTC's investigation originated after a LabMD employee downloaded a peer-to-peer file sharing program, which caused the disclosure of more than 9,000 individuals' personal information.
  - In 2016, the FTC obtained an order finding that LabMD's inadequate data security policies were an "unfair act or practice" violating Section 5(a) of the FTC Act.
  - The order went on to direct LabMD to establish a data security program that complied with the "FTC's standard of reasonableness."
  - The Court of Appeals rejected the order as lacking sufficient specificity to be enforceable against LabMD and amounting to the FTC "micromanaging" Lab MD's business. The court further noted that the FTC order did not enjoin LabMD from engaging in any specific conduct.

# Federal Enforcement Responses

- **The Aftermath of *LabMD* – "New and Improved" Data Security Orders**
  - In the wake of the Eleventh Circuit's decision in *LabMD*, the FTC's Bureau of Consumer Protection revised its approach to data security orders.
  - The FTC established the following parameters for drafting future data security orders.
    - **Terms tailored** to the allegations against the company, including identifying specific changes required of the company's data security plans.
    - **Improved accountability** for third-party assessors who review the company's data security programs.
    - **Company executives' responsibility** for annually presenting written data security plans to their boards and certifying compliance to the FTC.
  - Since 2019, the FTC has obtained seven data security orders using this new approach.

# Federal Enforcement Responses

- **Examples of Post-*LabMD* FTC Data Security and Privacy Orders**
  - ***In re James V. Grago d/b/a ClixSense***, F.T.C. Docket No. C-1723003 (June 19, 2019).
    - ClixSense and the FTC entered into a settlement to resolve claims that the company had insufficient protections for the consumer data that it collected and misrepresented the level of data security it provided.
    - The company collects personal information including user names, passwords, and Social Security numbers for individuals who use the site to earn money completing online tasks like surveys.
    - The FTC alleged that, while the company claimed that it "utilizes the latest security and encryption techniques," it in fact did not use encryption and had generally unreasonable security practices. Further, the FTC asserted that the company failed to protect logins and passwords and maintained consumers' personal information in clear text format.
    - As a result of these alleged deficiencies, hackers obtained the information of over 500,000 consumers in the United States and millions more abroad. The hackers then published the personal information of 2.7 million individuals.
    - The terms of the settlement prohibit ClixSense's owner from misrepresenting the extent of any of his companies' data security policies. It further requires him to put in place a "comprehensive data security program" with biannual outside evaluations if his companies collect consumer data in the future.

# Federal Enforcement Responses

- **Examples of Post-*LabMD* FTC Data Security and Privacy Orders, continued**
  - ***U.S. v. Unixiz, Inc. d/b/a i-Dressup.com***, No. 5:19-cv-2222 (N.D. Cal. May 2, 2019).
    - i-Dressup and the FTC entered into a settlement agreement to resolve claims that i-Dressup's information collection and data collection practices violated the Children's Online Privacy Protection Act (COPPA).
    - i-Dressup's website allows users (including children) to play clothing-related games and engage in other fashion-related activities. The company collects data on these users.
    - The FTC alleged that i-Dressup collected personal information from children users without their parents' consent. Further, the FTC claimed that i-Dressup did not adequately protect this data, stored and transmitted it in plain text, and lacked a system for monitoring potential security risks.
    - These shortcomings in i-Dressup's data security plans allowed a hacker to obtain the personal information of 1.2 million users, about one-fifth of whom were children.
    - The settlement included a $35,000 fine and required i-Dressup to, among other actions, implement a documented, staffed, and regularly assessed data security program.

# Federal Enforcement Responses

- ***FTC v. Interbill Ltd.***, No. 2:06-cv-01644-JCM-PAL (D. Nev. Apr. 10, 2019).
  - Payment processor Interbill and its owner entered into a settlement with the FTC to resolve claims that the company debited customers' bank accounts without their authorization on behalf of merchants that Interbill knew or should have known were engaged in deceptive or unfair practices.
  - The defendants were subject to a court order in 2009 enjoining them from such conduct.
  - The FTC alleged that Interbill and its owner violated that order when they failed to undertake appropriate vetting and monitoring of the merchants whose customer payments Interbill processed. For example, Interbill processed payments for at least two companies that settled FTC enforcement actions for running fraudulent telemarketing and debt collection operations.
  - This settlement requires the defendants to pay $1.8 million—the amount of unauthorized consumer debits—and permanently bans them from future involvement in payment processing businesses.

# Federal Enforcement Responses

- ***In re Pay Pal, Inc.***, F.T.C. Docket No. C-4651 (May 23, 2018).
  - PayPal, Inc. entered into a settlement with the FTC over allegations that its peer-to-peer payment service, Venmo, made various misrepresentations to consumers about the accessibility of payments, privacy settings, and data security and failed to implement adequate security practices.
  - As part of the settlement, Venmo is required to make certain disclosures to consumers and obtain biannual compliance assessments. It is prohibited from making misrepresentations or violating other laws.
  - The FTC's complaint alleged that Venmo:
    - Mischaracterized the time it takes to process transfers from Venmo to consumers' bank accounts;
    - Misled consumers about the steps to make their Venmo activity private, causing some consumers to inadvertently publish their activity;
    - Misrepresented its data security as "bank-grade" when in fact it was not;
    - Failed to provide consumers with sufficient privacy notices; and
    - Lacked an adequate information security program.

# Federal Enforcement Responses

- ***In re BLU Prods***, F.T.C. Docket No. C-4657 (Apr. 30, 2018).
  - BLU Products, Inc. entered into a settlement with the FTC to resolve a complaint alleging that BLU misled consumers about the extent to which it provided third parties access to their data and failed to ensure the security of consumers' personal information from such entities.
  - BLU manufactures mobile phones. It engaged a third-party security service provider who, without authorization, accessed and obtained significant amounts of BLU customers' personal information—including text messages and location data.
  - The FTC alleged that BLU and its president did not properly vet or design security policies for third-party contractors. Even after the unauthorized disclosure became public, BLU maintained a business relationship with the contractor.
  - In settling the matter, BLU and its president agreed to execute a data security program focused on protecting personal information on mobile devices.

# Federal Enforcement Responses

- ***U.S. v. VTech Elecs. Ltd.***, No. 1:18-cv-114 (N.D. Ill. Jan. 23, 2018).
  - VTech and the federal government entered into a settlement for various violations of the Children's Online Privacy Protection Act regarding VTech's data collection and protection practices for its internet-connected toys.
  - As part of the settlement, VTech agreed to implement a comprehensive data security program, refrain from misrepresenting its security and privacy practices, and pay $650,000.
  - The DOJ, on behalf of the FTC, alleged that VTech's platforms:
    - collected children's personal information without giving proper notice on the collection and use;
    - failed to reasonably protect the data it did collect; and
    - did not encrypt that data as promised in its privacy policy.

# Federal Enforcement Responses

- ***Upstart Network, Inc.***, CFPB No Action Letter (Sept. 14, 2017).
  - For the first time in its history, the Consumer Financial Protection Bureau (CFBP) issued a No Action Letter to a firm that sought guidance confirming that its FinTech product *would not be the subject* of a CFPB enforcement action.
  - Upstart uses a large volume of nontraditional data, artificial intelligence, and machine learning to make lending decisions. Its goal is to increase access to credit among people who may not be able to obtain a loan from a traditional financial institution.
  - The No Action Letter is part of a CFPB program to support innovative financial services products.

# Federal Enforcement Responses

- ***In re Dwolla***, CFPB No. 2016-CFPB-0007 (Feb. 27, 2016).
  - The CFPB entered a consent order against Dwolla after finding that it misrepresented the quality of its data security.
  - Dwolla is a payment processor which claimed publically that (a) it encrypted users' personal information, and (b) its data security program exceeded industry standards.
  - The CFPB found that, in fact, some sensitive information was not encrypted, applications were released without testing, and Dwolla overall did not take reasonable steps to protect consumers' data.
  - The CFPB's order required Dwolla to:
    - Implement a comprehensive data security program and accurately describe security measures to its users;
    - Remediate any existing data security issues and train staff on how to spot and resolve such problems in the future; and
    - Pay a $100,000 civil penalty.

# STATE ENFORCEMENT RESPONSES

# State Enforcement Responses

- **States are giving their regulators more tools to police companies in the financial services industry.**
  - **New York** has sought to expand the reach of its Department of Financial Services (DFS).
    - In 2015, New York became the first state to implement a formal, comprehensive licensing regime for cryptocurrency.
    - In early 2020, the governor announced his intention to authorize DFS to bring enforcement actions against companies engaged in unfair, deceptive, and abusive acts or practices.
  - **California** reoriented its financial services enforcement agency to focus on marshalling the development of innovation and technology.
    - The state intends to expand its reach to sectors, like FinTech, that have developed outside of traditional licensing regimes.
- **State Attorneys General are also increasingly active in bringing actions against companies for data-related misconduct.**

# State Enforcement Responses

- **State Law Example: New York's "Shield Act"**
  - Breach Notification: As of October 2019, businesses must notify state residents whose private information was acquired or *accessed* without authorization via the businesses' computerized data.
  - Security Measures: As of March 2020, companies must "develop, implement and maintain reasonable safeguards" to protect state residents' private information. The statute details various safeguards that will bring businesses into compliance, including risk assessments; protocols to detect and prevent system attacks or failures; employee training; and the disposal of personal information within a reasonable time after which the business no longer needs it.
  - Enforcement:
    - The Attorney General can seek restitution and civil penalties for violations of the Shield Act.
    - While the statute does not provide a private right of action for consumers, the standard that it sets for "reasonable safeguards" of private information could help plaintiffs substantiate other data security and breach claims against businesses.

# State Enforcement Responses

- **States are also joining together to litigate claims in cases like data breaches.**
  - **Uber Privacy Breach State Actions**
    - Attorneys General from all 50 states and the District of Columbia brought state law claims against Uber for not disclosing a data breach in a timely manner, which eventually resulted in a settlement of $148 million.
    - In 2017, a hacker was able to obtain the personal information of 57 million Uber drivers and passengers. The hacker contacted Uber and sought a ransom, which Uber paid. Uber did not disclose or publicize the breach until a year later.
    - The settlement obligated Uber to pay a $148 million penalty and take certain affirmative actions including:
      - Developing a data breach notification policy;
      - Adopting data security policies;
      - Creating a system for employees to report unethical behavior; and
      - Retaining an outside expert to evaluate the company's data security program.

# COMMERCIAL LITIGATION

ACCESS TO DATA
CYBER ATTACKS
INSURANCE
DATA BREACH
PERMISSIONS

# Commercial Litigation – Access to Data

- ***hiQ Labs, Inc. v. LinkedIn***, No. 3:17-cv-03301-EMC (N.D. Cal. Apr. 14, 2020).
  - In September 2019, the Court of Appeals for the Ninth Circuit held that hiQ Labs' (hiQ) practice of screen-scraping information from LinkedIn profiles likely did not violate the Computer Fraud and Abuse Act ("CFAA").
  - The court reasoned that because LinkedIn makes its users' information publically accessible, it cannot claim that hiQ violated CFAA's prohibition on accessing data without authorization.
  - hiQ uses bots to scrape public-facing information that LinkedIn users post on their profiles for use in the company's analytical products, including those predicting which employees are likely to leave their jobs. After LinkedIn sent hiQ a cease-and-desist letter, hiQ filed suit seeking injunctive and declaratory relief that it was not, in fact, violating the CFAA.
  - In February 2020, hiQ Labs amended its complaint to add claims that LinkedIn is engaged in anticompetitive conduct and monopolized the market for "people analytics services."
  - In March 2020, LinkedIn announced its intent to file a cert petition for the US Supreme Court to review the Ninth Circuit's decision, which split from other circuits on the issue of data scraping.
  - On April 14, 2020, LinkedIn filed a motion to dismiss hiQ's amended complaint, arguing that hiQ fails to state a monopolization claim because, among other things, LinkedIn has no duty to deal with hiQ and hiQ has not properly defined the purported market for "people analytics services."

# Commercial Litigation – Cyber Attacks

- ***Williams v. AT&T Mobility, LLC***, No. 5:19-cv-475-BO (E.D.N.C. Apr. 15, 2020).
  - In March 2020, the court denied AT&T's motion to dismiss plaintiff's claims that AT&T executed seven unauthorized "SIM swaps" on his phones at the behest of a hacker over a three-month period.
  - After the first SIM swap, plaintiff alerted AT&T, informed them that he was at high risk for such cyber attacks, and asked that future SIM changes only occur in person. AT&T nevertheless processed six additional SIM swaps without plaintiff's authorization.
  - Plaintiff alleged that these repeated cyber attacks resulted in a loss of $1,500 in bitcoin, put plaintiff's bitcoin investment and mining businesses at substantial risk (one of which eventually closed as a result), exposed his personal information, and led to threats against his family.
  - Plaintiff's claims sounded in negligence, state consumer protection and computer trespass laws, the Federal Communications Act, and the Computer Fraud and Abuse Act.
  - The court concluded that, among other things, (a) plaintiff's losses were foreseeable (and foreseen) because plaintiff repeatedly alerted AT&T to the attacks, and (b) plaintiff stated a plausible claim that AT&T violated state law when its employees initiated SIM swaps at the request of the hacker and without plaintiff's permission.
  - AT&T filed its Answer and Affirmative Defenses on April 15, 2020.

# Commercial Litigation – Cyber Attacks, Insurance

- ***Nat'l Ink & Stich, LLC v. State Auto Prop. & Cas. Ins. Co.***, No. 1:18-cv-02138 (D. Md. Feb. 5, 2020).
  - The parties settled out of court after the district court held, for the first time, that a traditional insurer can be liable to cover the costs that a policyholder incurred in dealing with the aftermath of a ransomware attack.
  - In the face of a ransomware hacker who refused to halt its attack even after receiving payment, plaintiff National Ink installed new security software. When that software failed to fully eradicate the malicious virus and slowed the plaintiff's computer system significantly, National Ink replaced its entire computer system. National Ink sought recovery from defendant State Auto under its business owner insurance policy.
  - The court concluded that the impaired functioning and lingering presence of the malware virus in National Ink's computer system constituted a "physical loss or damage," which its policy with State Auto covered. The court rejected State Auto's argument that the policy did not apply because the loss of intangible data was the only harm that National Ink experienced.

# Commercial Litigation – Insurance, Data Breach

- ***Am. Family Mut. Ins. Co. S.I. v. Amore Enters. Inc.***, No. 1:20-cv-01659 (N.D. Ill. Mar. 9, 2020).
  - In March 2020, American Family filed a complaint seeking a declaratory judgement that its business owners liability insurance policies do not cover liability for McDonald's franchisees' violations of the Illinois Biometric Information Privacy Act (BIPA).
  - In July 2019, employees of defendant franchisees brought suit against them in state court, alleging that the franchisees' collection, storage, and distribution of employees' fingerprint scans without proper notice and consent violated the BIPA.
  - The franchisees then turned to American Family to defend these claims under the franchisees' business owners liability insurance policies.
  - American Family argues in its action for declaratory judgment that the franchisees' policies exclude claims arising from their disclosure of personal, confidential information or their violation of statutes prohibiting the distribution of material or information.

# Commercial Litigation – Data Breach

- ***In Re Arby's Restaurant Group Inc.***, No.1:17-mi-55555 (N.D. Ga. Mar. 5, 2020).
  - The court preliminarily approved a $3 million settlement to resolve claims from a class of financial institutions that Arby's inadequate security measures caused tens of millions of dollars of fraudulent charges on payment cards that plaintiffs issued.
  - Plaintiffs alleged that Arby's various security failures—including missing a deadline to update its system to chip-reading technology and inadequate firewall, antivirus, and encryption capabilities—allowed hackers to obtain customer data from nearly 1,000 locations.
  - Plaintiffs sought damages relating to canceling customers' cards and accounts, refunding unauthorized charges to customers, and enhancing their fraud prevention systems.

# Commercial Litigation – Data Breach

- ***Paymentech, LLC v. Landry's Inc.***, No. 4:18-cv-01622 (S.D. Tex. Mar. 4, 2020).
  - In February 2020, the court denied Landry's motion for summary judgement on claims for indemnification of Visa assessment fees brought by Landry's payment processor Paymentech and JP Morgan Chase as a result of a data breach across a number of Landry's properties.
  - Landry's unsuccessfully argued that the fees were an unenforceable penalty. The court disagreed, finding that the fees were reasonably determined given the complexity of calculating losses from a data breach.
  - On March 4, 2020, Paymentech and JPMorgan Chase filed a motion for partial summary judgment, arguing that Landry's agreed to indemnify plaintiffs for fee assessments resulting from its failure to comply with industry data security standards relating to payment cards.

# Commercial Litigation – Data Breach

- ***Branch Banking & Trust Co. v. Hitachi Vantara Corp.***, No. 1:19-cv-01168 (M.D.N.C. Apr. 10, 2020).
  - In November 2020, Branch Banking & Trust ("BB&T") filed a complaint against Hitachi to recover damages incurred as a result of a 15-hour-long system failure of the bank's computer programs, including online banking.
  - BB&T alleges that Hitachi negligently installed fiber optic cables and failed to properly inspect and test the system.
  - As a result of the 15-hour outage and at least eight other incidents over the previous year, BB&T claims to have lost data on hundreds of thousands of transactions and argues that its customers were unable to engage in online banking and other services during the outages.
  - On January 22, 2020, Hitachi filed a motion to dismiss, arguing that BB&T's claims amount to, at most, a simple breach of contract rather than a case of gross negligence or unfair and deceptive trade practices, as BB&T alleges.
  - On April 10, 2020, the court denied Hitachi's motion to dismiss.

# Commercial Litigation – Data Breach

- ***Minsky v. Capital One Fin. Corp.***, No. 1:19-cv-01472 (E.D. Va. Mar. 10, 2010).
  - Plaintiff investors filed suit against Capital One alleging that, as the bank implemented a digital, information-based business strategy, it misled investors about its cybersecurity vulnerabilities.
  - In July 2019, Capital One suffered a data breach that exposed the personal information of over 100 million people, including tens of thousands of pieces of highly sensitive data like Social Security numbers and bank account numbers. Plaintiffs brought this securities action after Capitol One shares lost value as a result of the breach.
  - In February 2020, Capital One filed a motion to dismiss, arguing that plaintiffs failed to adequately plead facts sufficient to show that bank executives made the at-issue statements with the required level of scienter.
  - In their March 2020 opposition memorandum, plaintiffs counter that Capital One executives falsely stated that the bank encrypted data, made misleading statements about its compliance with relevant industry standards and regulations, and suggested that cybersecurity was one of its top priorities.

# Commercial Litigation – Permissions

- ***JPMorgan Chase, N.A. v. The Federal Republic of Nigeria*** [2019] EWAC Civ 1641.
  - A UK appeals court refused to strike Nigeria's claim of gross negligence against JPMorgan for the bank's release of $875.7 million to a shell company controlled by a former government minister suspected of corruption.
  - The key issue in the case is whether JPMorgan owes Nigeria a "Quincecare" duty to refuse to dispense a client's funds if a reasonable banker would not do so under circumstances that raise suspicions about misappropriation.
  - Nigeria argues that JPMorgan was on notice of possible suspicious conduct based on past suspicious activity reporting.
  - JPMorgan argues that its account agreement contracted away any Quincecare liability.

# CONSUMER LITIGATION

## DATA BREACH DISCLOSURE

# Consumer Litigation – Data Breach

- ***Barnes v. Hanna Andersson, LLC,*** No. 3:20-cv-00812-DMR (N.D. Cal. Mar. 3, 2020).
  - Customers of Hanna Andersson, a high-end children's apparel brand, filed a class action lawsuit against the company and Salesforce—Andersson's customer relationship management software—following a data breach. Hackers obtained customers' personal and payment information, which is now for sale on the dark web.
  - Plaintiffs allege that Andersson and Salesforce did not have reasonable security policies and procedures in place to protect the sensitive, personally identifiable information and billing information that Andersson collected.
  - Allegations in support of plaintiffs' negligence and California Unfair Competition Law claims include the fact that the hacking went unnoticed for months; Andersson informed its customers more than a month after it learned of the breach; and Andersson provided less detailed notice to consumers than it did to state Attorneys General.
  - On March 3, 2020, plaintiffs amended their complaint to add a count alleging that the defendants' failure to implement reasonable security systems violated the California Consumer Privacy Act.

# Consumer Litigation – Data Breach

- ***In re Equifax Inc. Customer Data Sec. Breach Litig.***, No. 1:17-md-02800 (N.D. Ga. Feb. 10, 2019).
  - In December 2019, a district court approved a settlement to resolve the claims of about 147 million individuals whose personal information was disclosed as the result of a data breach at Equifax, one of the nation's three consumer reporting agencies.
  - The settlement obligated Equifax to spend up to $425 million compensating consumers, $77.5 million in attorneys fees, and $1 billion invested in improving its own data security.
  - Equifax alerted the public to the hack and disclosure of PII more than a month after it learned of the breach.
  - This case is particularly noteworthy because of sensitivity of the data disclosed—often including Social Security numbers—the large size of the impacted population, and the fact that victims were not necessarily customers of Equifax.
  - The settlement provided class members with free credit monitoring services or, in the alternative, a cash option. This cash option garnered press attention because of confusion over whether the whole class was entitled to $125 even as the pool of funds set aside for such compensation quickly dwindled.
  - In February 2020, several class members who objected to the settlement filed notice of appeal in the Court of Appeals for the Eleventh Circuit, where they are expected to challenge the fairness of the settlement and the size of the attorneys fees award.

# Consumer Litigation – Disclosure

- ***Reyes v. Experian Info. Sols., Inc.***, No. 8:16-cv-563-AG-AFMx (C.D. Cal. Jan. 27, 2020).
  - Experian and the plaintiff class reached a $24 million settlement to resolve claims that Experian's practice of reporting disputed loans on credit reports was "unduly misleading" in violation of the Fair Credit Reporting Act (FCRA).
  - The lead plaintiff brought the case after Experian persisted in including on her credit report a past-due loan from an out-of-business pay-day lender. When that company closed, it requested that Experian remove any of its accounts from consumers' credit reports—which took Experian over a year to do.
  - The certified class includes more than 50,000 individuals whose Experian credit reports noted a delinquent loan from that lender. Under the terms of the settlement, each class member will receive $270 automatically.
  - The court granted preliminary approval to the settlement and set a hearing on the settlement for May 18, 2020.

# KEY TAKEAWAYS

# Key Takeaways

1. Disputes can arise in an environment where consumers and companies rely on technology to facilitate financial services while also misunderstanding the extent to which their data is secure.
2. Regulators are emptying their toolbox in search of ways to more actively police financial institutions' use of technology and data.
3. Data breaches, data access, and ransomware are the subject of commercial and consumer litigation.

# Biography

**Richard S. Taffet**
**New York**
T +1.212.309.6795
F +1.212.309.6001

Richard S. Taffet serves as lead counsel in a wide range of antitrust, intellectual property, and other domestic and international litigation and counselling matters. He represents clients in technology, financial, industrial products, and consumer goods industries.

For close to 40 years Richard has tried cases in state and federal courts, as well as in arbitration proceedings; represented clients' interests in appeals to numerous Federal Courts of Appeal and the Supreme Court of the United States; and has advised clients in connection with a broad range of competition and intellectual property matters. Richard also regularly assists clients in matters before the United States Department of Justice and Federal Trade Commission, as well as foreign competition and other regulatory bodies, including in European and Asian jurisdictions. Richard is also recognized as a leading counsel and thought leader in connection with matters involving technology standards development.

Richard is noted in *Chambers USA* "as a proficient and respected antitrust and IP lawyer," and for his "excellent strategic views and his ability to always think one step ahead."

# Biography

**Bryan R. Woll**
**New York**
T +1.212.309.6047
F +1.212.309.6001

Bryan R. Woll is part of a team of lawyers that advises businesses and individual clients in commercial and securities litigation, government and self-regulatory organization investigations, complex civil litigation, and regulatory enforcement actions. Bryan maintains an active pro bono practice focused on housing, public education funding, and public benefits for families experiencing homelessness.

While in law school, Bryan served as an intern for Commissioner Terrell McSweeny of the Federal Trade Commission. He also worked on federal and state housing regulation at the Legal Aid Society's Law Reform Unit and was part of a team litigating class actions at the New York Legal Assistance Group's Special Litigation Unit.

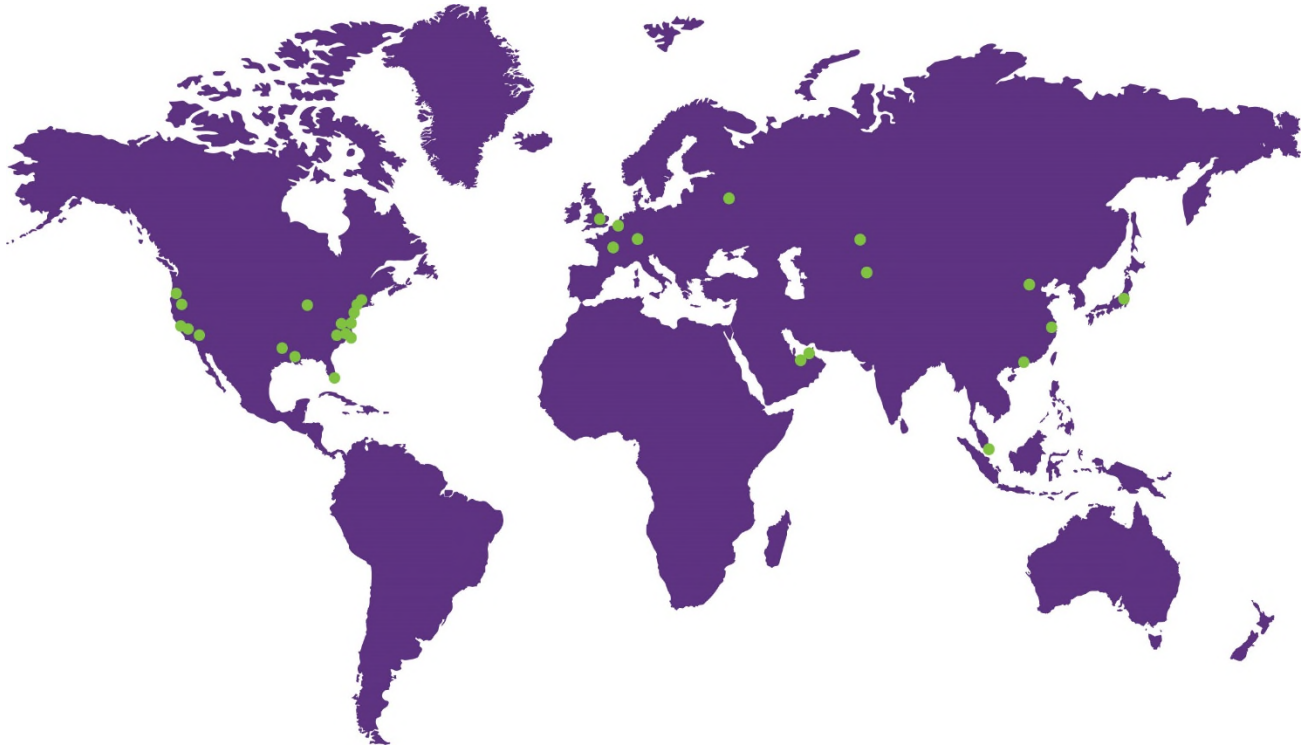
Prior to becoming a lawyer, Bryan worked as an analyst on legislative and regulatory issues at the New York City Mayor's Office of Management and Budget. He also spent several years managing an eviction prevention program at the Brownsville Partnership, a non-profit organization in Brooklyn.

## Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

## Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

*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. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

# THANK YOU