United States Government Accountability Office
Report to Congressional Requesters

March 2018

FINANCIAL TECHNOLOGY

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

GAO-18-254

GAO Highlights

Highlights of GAO-18-254, a report to congressional requesters

March 2018

FINANCIAL TECHNOLOGY

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

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 Lawrance L. Evans, Jr. at (202) 512-8678 or Evansl@gao.gov.

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

Tables

Figures

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

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

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.[1] 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.[2]

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

[1]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.

[2]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.[3] 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.[4] A variety of fintech firms provide mobile wallets, including Apple, Google, and Samsung.[5]

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.[6]

---

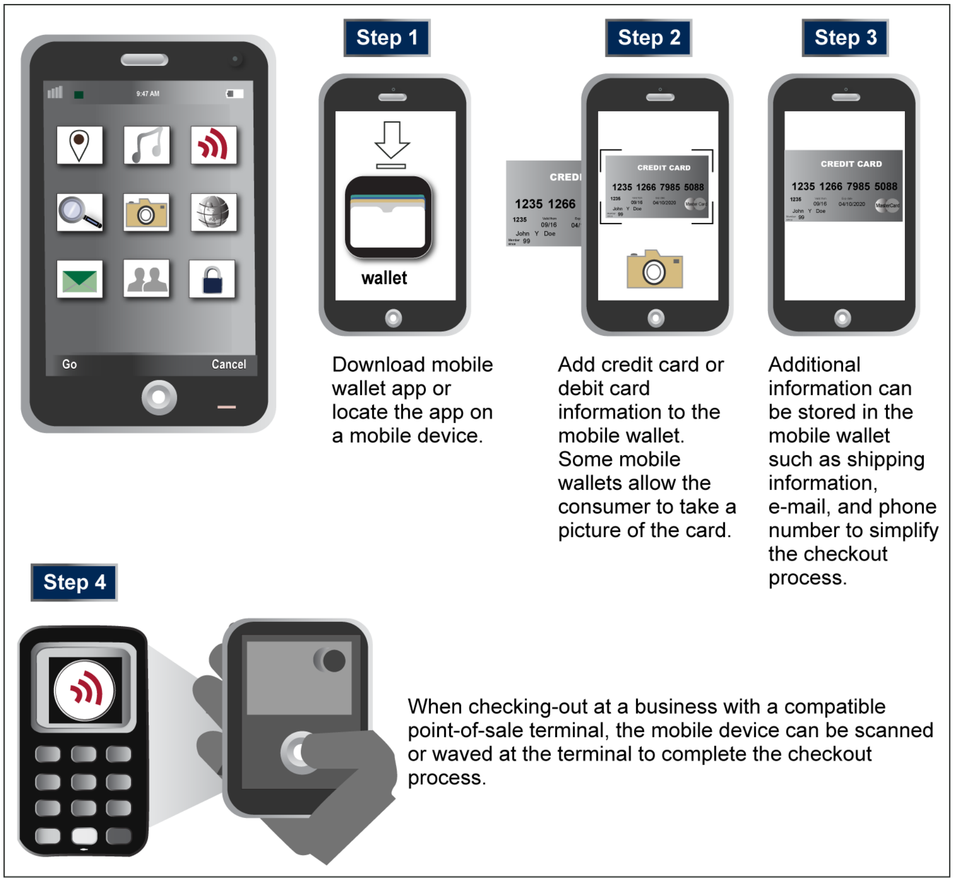
[3] In a mobile wallet, consumers can enter payment information from debit and credit cards, gift cards, and prepaid cards. Consumers can also store other information often needed to complete a transaction, such as shipping address, e-mail, and phone number.

[4] 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 Pandy 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 Pandy, 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.

[5] 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.

[6] 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.[7] According to a report by the Smart Payment Association, 200,000 locations accepted Apple Pay when it was

[7]Board of Governors of the Federal Reserve, *Consumers and Mobile Financial Services 2016* (Washington, D.C.: March 2016).

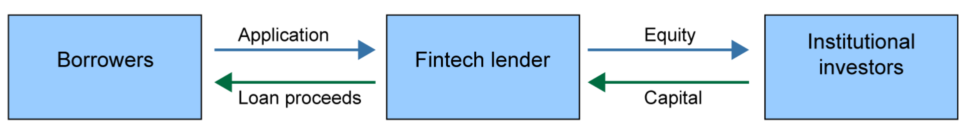
launched in September 2014, but by February 2016, this number had reached 2 million.[8] According to Paypal, it had 218 million active customer accounts at the end of the third quarter of 2017 and processed over 6 billion payments valued at more than $354 billion in 2016.

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



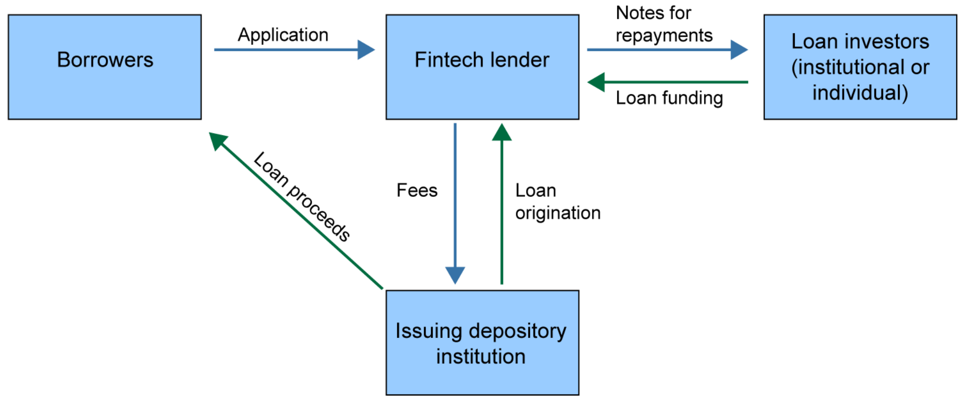
Sources: GAO analysis of Congressional Research Service and Department of the Treasury information. | GAO-18-254

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,

[8]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,[9] and other market monitors estimate that fintech lending volumes could grow to as much as $90 billion to $122 billion by 2020.[10]

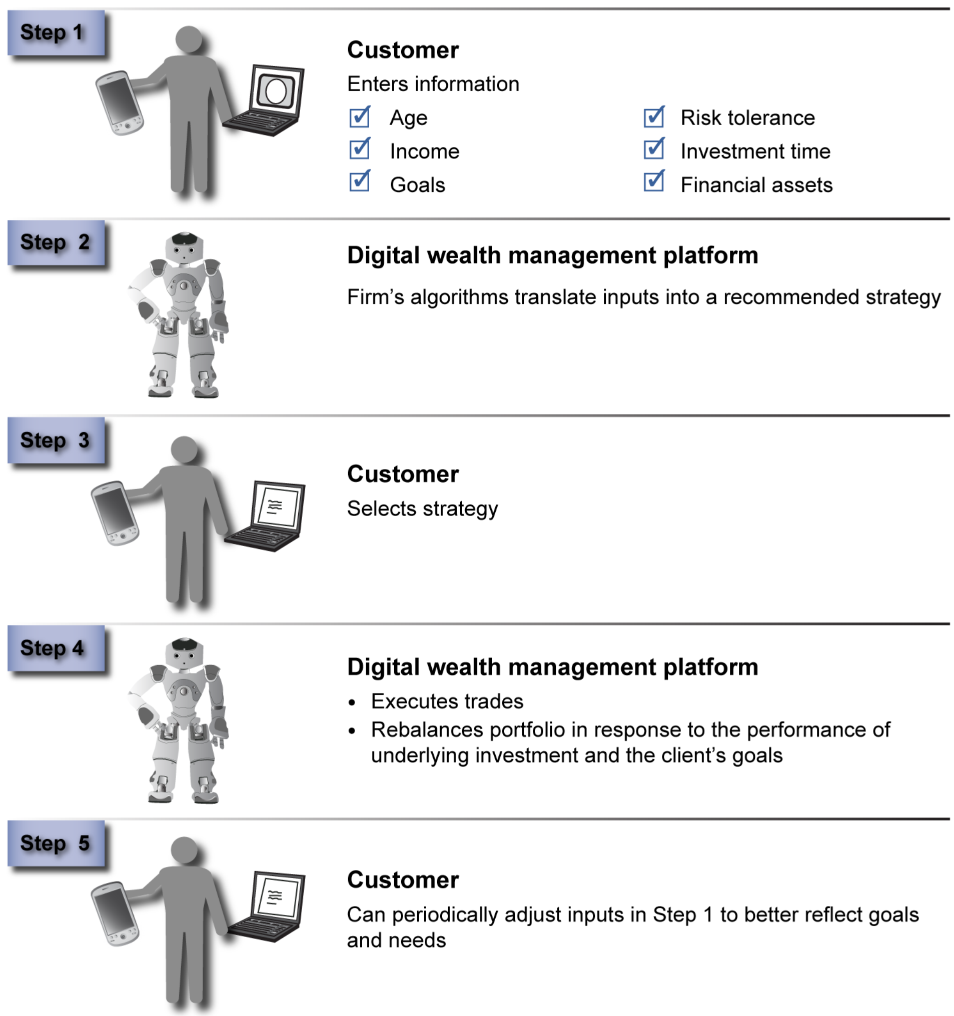
Fintech Wealth Management and Financial Advice

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.

[9]See S&P Global Market Intelligence December 2016 *U.S. Digital Lending Landscape* (Charlottesville, Va: December 2016).

[10]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.[11]

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

[11]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[12] 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.[13]

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

[12]See GAO-14-496. As we previously reported, virtual currencies can be used to make payments and transfer funds.

[13]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.[14] 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.

[14] 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 promoted 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.[15]

[15] 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.[16]

- **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.[17] 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.[18] 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.

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

[17] 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.

[18] 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.[19] 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.[20] 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.[21] 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

[19]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.

[20]Consumer Financial Protection Bureau, *Data Point: Credit Invisibles* (Washington, D.C.: May 2015).

[21]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.[22] 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

[22]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.[23]

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.[24] 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.

[23]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.

[24]*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.[25] 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.[26] 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.[27] In addition, FCC and FTC have issued tips for consumers and firms publicizing practices that help avoid cramming.[28]

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.[29] Other fintech firms voluntarily disclose to consumers in their terms and conditions that any mobile wallet balances they hold are not

[25]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*.

[26]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).

[27]Protecting Consumers From Unauthorized Carrier Charges and Related Unauthorized Charges, 82 Fed. Reg. 37830 (Aug. 14, 2017).

[28]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).

[29]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,[30] holding investments against funds held or transmitted,[31] and meeting minimum net worth requirements.[32]

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.[33] 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

[30]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.

[31]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.

[32]CSBS reports that all states have net worth requirements, with the exception of Montana. The most common minimum net worth requirement is $100,000.

[33]*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.[34] 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.[35]

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

[34] *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.

[35] 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.[36] As with traditional lenders, federal fair lending laws, such as the Equal Credit Opportunity Act, apply to fintech lenders.[37] 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.[38] However, the Equal Credit Opportunity Act requires lenders, including fintech lenders, that deny credit to applicants to disclose the specific reasons for denial.[39] Alternatively, if the fintech lender's underwriting is too lax, loans could be made to borrowers who lack the ability to repay them.[40] Borrowers who default under these circumstances then face limited access to and higher prices for credit in the future.

[36]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.

[37]*See* 15 U.S.C. § 1691c.

[38]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.

[39]*See* 15 U.S.C. § 1691(d)(3).

[40]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.[41] 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.[42] 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.[43] 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.[44]

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

[41]Robo-advisers can be investment advisers or broker dealers. FINRA rules govern broker dealers and SEC rules govern investment advisers.

[42]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).

[43]For more information, see GAO-17-361.

[44]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).[45]

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.[46] 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.[47] Whereas traditional transactions can be reversed to correct fraud or errors, many virtual currency transactions are designed to be irreversible.[48] 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.[49] However, firms that transmit,

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

[46]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.

[47]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).

[48]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.

[49]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.[50]

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.[51] 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.[52]

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.[53] 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.[54] Fraud and theft are risks of other securities offerings, and investors receive

[50]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.

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

[52]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).

[53]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).

[54]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.[55] 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.[56] 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.[57] To help investors address these risks, SEC and FINRA have issued documents publicizing risks of token sale investment.[58]

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

[55]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).

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

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

[58]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.[59]

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.[60] 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.

[59]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, 1016); 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).

[60]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.[61] Like traditional financial institutions, rules and guidelines implementing the Gramm-Leach-Bliley Act (GLBA) generally require fintech firms to secure customer information.[62] In addition, some regulators have issued guidance to consumers publicizing practices that help avoid security problems when using fintech products.[63] 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.[64] For example, the New York State Department of Financial

[61]For example, firms may use data encryption, secure elements of mobile hardware, and tokenization to help protect the transmission of consumer data.

[62]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.

[63]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*.

[64]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.[65]

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.[66] 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.[67] 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.[68]

[65]New York State Department of Financial Services, *Cybersecurity Requirements for Financial Services Companies*, 23 NYCRR 500 (March 2017).

[66]GLBA restricts, with some exceptions, the disclosure of nonpublic information by companies defined as "financial institutions." *See* 15 U.S.C. § 6801.

[67]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).

[68]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.[69] 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.[70] 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.[71]

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

[69]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.

[70]Financial Action Task Force, *Emerging Terrorist Financing Risks* (Paris, France: October 2015).

[71]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.[72] 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.[73] 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.[74]

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.[75] 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

[72]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).

[73]Bank for International Settlements and Financial Stability Board, *FinTech Credit*.

[74]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).

[75]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.[76] 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

[76]*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.[77] 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.[78]

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 intuition 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

[77]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.

[78]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.[79] 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.[80] 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.[81] 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.

[79]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.

[80]Office of the Comptroller of the Currency, *Third-Party Relationships: Risk Management Guidance,* OCC Bulletin 2013-29, Oct. 30, 2013.

[81]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.[82] 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.[83] 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.[84] CFPB may also conduct examinations of individual companies that it determines

[82]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 $10billion 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.

[83]*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.

[84]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.[85] In addition, all states and the District of Columbia required lending licenses for consumer lenders operating in their states, according to CSBS staff.[86]

[85]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.

[86]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.[87] For example, in 2015 New York finalized a new license for virtual currency businesses under New York's financial services law.[88]

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.[89] 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.[90] For example, Money Transmitters Regulators

[87]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.

[88]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.

[89]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-charted, 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.

[90]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.[91] 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.[92] 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.[93] 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.[94] For example, in 2015, FTC took action against the providers

[91]According to CSBS, Montana, New Jersey, and Wisconsin do not have licensing requirements related to anti-money laundering.

[92] *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).

[93]*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.

[94]*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.[95] It can also bring enforcement action against non-bank service providers that maintain or process customer information under its GLBA authority.[96]

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.[97] 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.[98] 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

[95]*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.

[96]*See* 15 U.S.C. § 6805; *see also* 16 C.F.R. pt. 234.

[97]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).

[98]*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.[99]

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.[100]

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.

[99] *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).

[100] 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.[101] 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.[102] 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.[103]

[101]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.

[102]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.

[103]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.[104]

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

[104] *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.[105] 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.[106] 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.[107] For example, the newsletter listed laws and regulations related to

[105]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).

[106]Federal Reserve System, *Consumer Compliance Outlook*, 2nd ed. (Philadelphia, Pa.: December 2017).

[107]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.[108] 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.[109]
- 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.[110] 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.[111]
- 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

[108] *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).

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

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

[111] 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.[112]

- 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.[113]
- 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.[114] 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.[115]
- 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.[116] For example, the

[112] *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.

[113] Commodity Futures Trading Commission, LabCFTC, *A CFTC Primer on Virtual Currencies* (Washington, D.C.: October 2017).

[114] *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).

[115] Financial Industry Regulatory Authority, *Initial Coin Offerings: Know Before You Invest* (Washington, D.C.; August 2017).

[116] 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.[117] 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.

[117]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.[118] 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

[118]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.[119] 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.[120] 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

[119]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.

[120]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.[121] 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.[122] 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.[123] Additionally, in 2013, state regulators established the Multi-State MSB Examination Taskforce, which coordinates and facilitates multistate supervision of MSBs. [124] CSBS staff told us that multistate exams have made the state MSB exam process more efficient for state regulators and MSBs.

[121] *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).

[122] 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.

[123] The seven states include Georgia, Illinois, Kansas, Massachusetts, Tennessee, Texas and Washington.

[124] 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.[125] 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.[126]

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

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

[126] 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.[127]

- **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.[128]
- **Differing regulatory interpretation of consumer protection requirements.** As discussed above, fintech firms may be subject to

[127]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.

[128]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.[129]

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

[129]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.[130] 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.[131]
- 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

[130]Treasury staff we interviewed told us in October 2017 that they did not have plans to reconvene the group.

[131]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.[132]

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

[132]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.[133] 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.[134]

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.[135] 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

---

[133] GAO-12-1022.

[134] GAO, *Managing for Results: Implementation Approaches Used to Enhance Collaboration in Interagency Groups*, GAO-14-220 (Washington, D.C.: Feb. 14, 2014).

[135] 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.[136] Similarly, the Financial Stability Board has suggested that responsible agencies further open lines of communication to address cross-cutting fintech issues.[137]

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.[138] 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

[136]Bank for International Settlements, *Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors,* August 2017.

[137]Financial Stability Board, *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention*, June 2017.

[138]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.[139] 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.[140] 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

[139]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).

[140]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.[141]

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.[142] 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

[141]Federal Financial Institutions Examination Council, *Information Technology Examination Handbook, E-Banking Booklet Appendix D: Aggregation Services* (Washington, D.C.: August 2003).

[142]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.[143] 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.[144]

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

[143]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.

[144]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.[145] 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

[145]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.[146] 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.

[146]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											
	CFPB	CFTC	FDIC	Federal Reserve	FINRA	FTC	NCUA	OCC	SEC	United Kingdom	Singapore	Hong Kong
Innovation office	●	●	--	●[a]	●	●	--	●	●	●	●	●
Dedicated webpage	●	●	--	●[a]	●	●	--	●	●	●	●	●
Dedicated e-mail address	●	●	--	●[a]	●	--	--	●	●	●	●	●
Dedicated phone number	--	●	--	--	--	--	--	●	--	●	--	--
Office hours	●	●	--	●[a]	●	--	--	●	--	●	●	●
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.

[a]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											
	CFPB	CFTC	FDIC	Federal Reserve	FINRA	FTC	NCUA	OCC	SEC	United Kingdom	Singapore	Hong Kong
Sandbox	--	--	--	--	--	--	--	--	--	●	●	●
Regulatory relief tool[a]	●	●	--	--	--	--	--	--	●	●	●	●
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.

[a]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.[147] 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.[148] 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

[147]Consumer Financial Protection Bureau, *No-Action Letter to Upstart Network, Inc. (Washington, D.C.: September 2017).*

[148]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.[149] 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

[149]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.[150] 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.[151]

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

[150]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).

[151]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											
	CFPB	CFTC	FDIC	Federal Reserve	FINRA	FTC	NCUA	OCC	SEC	United Kingdom	Singapore	Hong Kong
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 regulators 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. 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.

Lawrance L. Evans, Jr.

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.[1] 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

[1]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.

Table 2: Domestic Interagency Fintech Collaboration Efforts

Name of group	Participating agencies	Mission/goals	Ways in which group addresses fintech
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.

Name of group	Participating agencies	Mission/goals	Ways in which group addresses fintech
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

Table 3: International Interagency Fintech Collaboration Efforts

Name of group	Participating agencies	Mission / goals	Ways in which group addresses 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. 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.

Name of group	Participating agencies	Mission / goals	Ways in which group addresses fintech
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

cfpb 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.[1] 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.[2] 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

---

[1] The Bureau's consumer protection principles are available at http://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.
[2] *See* 81 Fed. Reg. 83,806 (Nov. 22, 2016).

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

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

J. Christopher Giancarlo
Chairman

(202) 418-5030
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 21st 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 rick transfer markets.

Sincerely,

J. Christopher Giancarlo

Appendix VI: Comments from the Conference of State Bank Supervisors

CSBS SINCE 1902
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 20th 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.[1] 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.

[1] 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[2] – on the internet or in person – requires state licensure as a consumer credit provider.[3] Though state product requirements may vary,[4] 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.[5] 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

---

[2] 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.nationwidelicensingsystem.org/slr/PublishedStateDocuments/ND-MB-License-Description.pdf.

[3] *See, e.g.* Oregon Consumer Finance License, *available at* https://mortgage.nationwidelicensingsystem.org/slr/PublishedStateDocuments/OR-Consumer-Finance-License-Company-Description.pdf; New Hampshire Small Loan Lender Company License, *available at* https://mortgage.nationwidelicensingsystem.org/slr/PublishedStateDocuments/NH-Small-Loan-Lender-Company-Description.pdf.

[4] Typically, state thresholds vary for interest rate, principal, and term.

[5] Licensing records for SoFi, LendingClub, Prosper, and UpStart can all be found on NMLS Consumer Access at 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.[6] 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.[7]

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.[8] 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.[9] Through the MMET, in 2017, the

[6] 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.

[7] *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.

[8] *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-Protocoll010512.pdf.

[9] 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.[10] 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.[11] 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.[12] 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.

[10] *See* MMET 2016 Annual Report, *available at* https://www.mtraweb.org/exams/multi-state-msb-examination-taskforce-mmet/.

[11] *See* https://www.csbs.org/model-regulatory-framework-virtual-currencies.

[12] 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.[13] 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;

[13] 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).[14]

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,[15] large multi-state companies that engage in physical money transfer,[16] and specialty MSBs that serve local communities.[17]

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.[18] The table below shows the market share of fintech payments companies in different MSB markets as of the second quarter of 2017.

[14] For more information, see the SRR Annual Report. *Available at* http://mortgage.nationwidelicensingsystem.org/about/Documents/2016%20SRR%20AR%20Report%20Web%20Version.pdf.
[15] Large multi-state companies engaged in electronic money transfer are likely licensed in 10 or more states without agents.
[16] 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.
[17] Specialty MSBs are likely licensed in 1-state, often providing services to a particular community.
[18] 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.[19] The Senators stated, "[s]ince many fintech companies are

[19] 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.[20]

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.

[20] 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.[21] 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

[21] 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.[22]

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.[23]

More recently, seven states have agreed to a multi-state agreement that seeks to standardizes key elements of the licensing process for money services businesses.[24] 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 for 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

[22] For more information on NMLS 2.0, *see* http://mortgage.nationwidelicensingsystem.org/Pages/NMLS20Information.aspx.
[23] For more information on SES, *see* https://new.nmls.org/ses.
[24] *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.[25]

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,

[25] 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.

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,

G. Patrick Webre
Acting Chief
Consumer and Governmental Affairs Bureau

Appendix VIII: Comments from the Federal Deposit Insurance Corporation

FDIC
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. Lawrance L. 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

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.

3

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,

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

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,

Mark Treichel

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. Lawrance 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.[1] 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

[1] "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.[2] It has also conducted significant outreach to establish a more open and continuous dialogue regarding innovation.[3]

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

Grace E. Dailey
Senior Deputy Comptroller and Chief National Bank Examiner

[2] See "Responsible Innovation" on occ.gov (https://www.occ.gov/topics/responsible-innovation/index-innovation.html).

[3] 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.

2

Appendix XII: Comments from the Securities and Exchange Commission

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

OFFICE OF
THE CHAIRMAN

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.

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, (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, (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, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548