Fintech apps have proliferated over the last decade. It is now commonplace to use these services to track your spending and set your budget for the coming month, to help you apply for a loan, split a bill with friends, or manage your investments. According to a 2018 survey by the Clearing House, one in three U.S. banking consumers now uses at least one fintech app.

These apps rely on establishing connections with traditional financial institutions. Data aggregators, in particular, play a major role in this ecosystem. These companies access financial account data with consumers’ permission and facilitate the underlying service the consumer has requested.

Increasingly, this consumer-permissioned data sharing is enabled by APIs – short for “application programming interfaces.” APIs may allow financial data to flow between fintech companies and traditional financial institutions with improved accuracy, increased control over data, and enhanced data security. But when companies use APIs for these purposes, they also need to consider a wide range of legal issues.

APIs and the Fintech Ecosystem

An API is a collection of tools, computer routines, and technology protocols that acts as a conduit for data to flow between systems in a controlled fashion. APIs have been used for years, both among financial institutions and in other industries, to share data within closely restricted environments. Increasingly, they are being used to connect previously detached aspects of the financial services industry.

APIs help address a number of challenges posed by the development of fintech. For example, many fintech apps have traditionally relied on “screen-scrapping” to retrieve account information, which requires consumers to provide their login credentials to a third party. This practice may create security risks. In contrast, where financial institutions and fintech companies partner to use a secure API, they can achieve this data transfer with less risk and increased data accuracy. APIs can also facilitate safe and quick payments and transfers of account relationships between institutions.

Initial Regulatory Responses

Beginning in 2016, European authorities made a strong push in support of open banking through APIs. Specifically, the U.K.’s Competition and Market Authority (“CMA”) announced its “Open Banking” initiative, and the European Union issued its second Payments Systems Directive (“PSD2”). Open Banking requires the largest U.K. banks to use open-access APIs so that consumers can access transaction and payment data. Similarly, PSD2 requires institutions to allow licensed third parties to access consumer financial data through APIs.

The regulatory framework in the U.S. is more muddled. Section 1033 of the Dodd-Frank Act requires financial institutions to make available to consumers their financial data in an easily useable format. It also grants authority to the Consumer Financial Protection Bureau (“CFPB” or “Bureau”) to create rules to govern these interactions. Consistent with its section 1033 authority, the Bureau issued a request for information (“RFI”) regarding data aggregators in November 2016. Following the RFI, the Bureau issued non-binding principles for “Consumer Authorized Financial Data Sharing and Aggregation” in October 2017. These principles
advocat[ed] strongly for consumer control of the consumer’s data” while emphasizing the need for privacy and data security protections.

Other U.S. regulators have also discussed the benefits and risks associated with data aggregation, APIs, and increasing connectivity within the banking system. For example, in July 2018, the Treasury Department issued a report strongly supportive of data aggregation. This report also “identified the need to remove legal and regulatory uncertainties currently holding back . . . data-sharing agreements that would effectively move firms away from screen-scraping to more secure and efficient methods of data access,” like APIs. In contrast, the Financial Industry Regulatory Authority (“FINRA”) issued a March 2018 Investor Alert that sounded a more cautious note, warning customers to “be mindful of data aggregation risks,” while acknowledging that APIs offer “a safer option than [screen] scraping.”

Despite these various regulatory publications, U.S. policymakers have not yet created binding rules focused specifically on open APIs or data aggregation generally. This has created its own challenges, as discussed further below.

**Legal Issues To Consider**

These services implicate a wide variety of legal issues, and in many cases further clarity is needed to both encourage continued innovation and protect consumers. Below are a few of the issues that financial services companies that use APIs for fintech partnerships should consider:

**Data Privacy**

When using APIs to exchange financial data, companies must ensure personal information remains subject to appropriate privacy protections. A central premise of account aggregation is that the data is shared with consumer consent. Companies should therefore use robust consent mechanisms to ensure consumers understand the terms to which they are agreeing.

This is critical under several legal frameworks. First, clear and conspicuous disclosures reduce the risk that a regulator could consider the practices “deceptive” under the Federal Trade Commission (“FTC”) Act, the Dodd-Frank Act, or relevant state laws. Second, the Gramm-Leach-Bliley Act (“GLBA”) and California Consumer Protection Act (“CCPA”) both recognize exceptions to their data sharing restrictions when the consumer intentionally directs the sharing. In negotiating agreements governing the use of APIs, the parties should consider specific provisions governing appropriate consumer disclosures.

**Data Security**

As noted previously, APIs are generally considered more secure than screen scraping. Nonetheless, maintaining the security of data retrieved by APIs is critical from both a commercial and regulatory perspective, and requires ongoing investment.

All financial institutions are subject to data security requirements under GLBA. Generally, nonbank fintech companies are subject to the FTC’s GLBA Safeguards Rule, which has historically created very general obligations. In March 2019, however, the FTC proposed to make these requirements much more detailed.

Banks supervised by the prudential banking regulators are subject to even more stringent cybersecurity oversight through regulatory supervision, including through the Federal
Financial Institutions Examination Council’s information technology standards. In addition, these regulators have exercised their authority under the Bank Service Company Act to supervise directly the data security practices of certain bank service providers, including at least one of the major data aggregators. Finally, as part of their obligations under GLBA, as well as general third-party risk management guidance, banks are responsible for conducting stringent diligence of the data security practices of third parties with whom they share personal information.

These legal frameworks highlight the need for companies to maintain robust security standards, and also often shape negotiations around data aggregation. Points of contention may include audit rights and the allocation of risk for potential data breaches.

Other Issues

While these data protection questions are central to these services, a wide range of other topics may be implicated. For example:

- **Data Rights.** The legal ownership of this consumer data as between the various participants in the ecosystem (including customers, banks and fintech companies) is not always clear. For now, these questions are typically resolved through contract.

- **Unauthorized Transactions.** Under the Electronic Funds Transfer Act (“EFTA”) and Regulation E, financial institutions generally may not hold a consumer liable for an unauthorized transaction. These institutions have long protested that this rule should not apply if a data aggregator is responsible for the unauthorized transaction.

- **Fair Credit Reporting.** The Fair Credit Reporting Act (“FCRA”) imposes certain obligations on “furnishers” of consumer report information. When a financial institution agrees to provide a fintech company consumer data through an API, is it acting as a “furnisher?” Such a conclusion would be inconsistent with the purposes of the FCRA, but also is not clearly foreclosed by the statutory or regulatory text.

- **CFPB Supervision.** The CFPB has authority under Dodd-Frank to designate certain financial companies as “larger participants” subject to Bureau supervision. Some traditional financial institutions have argued that the Bureau should exercise this authority to supervise the major data aggregators.

- **Third-Party Risk Management.** The federal banking agencies have issued guidance describing their supervisory expectations for banks’ oversight of third-party service providers. These expectations are risk-based and may include due diligence, contractual protections, and monitoring. Data services companies such as data aggregators should be subject to these risk management programs when they enter into API agreements with financial institutions.

Conclusion

Interconnected banking is helping consumers access innovative services and increasing competition in the financial services industry. More and more, these connections are facilitated by APIs. Along with significant benefits, such relationships between market participants also raise a variety of legal questions. At least until the U.S. develops a clearer framework for
interconnected banking, companies will need to remain vigilant to make sure they have thought through and addressed all the relevant legal risks.
Where Do Banks Fit in the Fintech Stack?

Remarks by
Lael Brainard
Member
Board of Governors of the Federal Reserve System
at the
Northwestern Kellogg Public-Private Interface Conference on
“New Developments in Consumer Finance: Research & Practice”

April 28, 2017
We can learn a lot from the evolution of smartphones as we try to envisage where the fintech ecosystem--and banks’ role within it--might be heading in the future. Smartphones have ushered in an age when different companies can easily work with each other’s products to seamlessly provide services to consumers. Today I want to reflect on what we might learn from that model about the increasingly interconnected world of financial services.

On the 10th anniversary of the iPhone, a Wired.com article revealed that even Steve Jobs hadn’t predicted the smartphone’s potential as a platform.1 Apple was just trying to design an iPod that made phone calls. Today, the average American spends five hours a day on their phone, unlocking it an average of 80 times daily.2 Even the Supreme Court has noted that smartphones are now “such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.”3

Of course, we aren’t using these appendages primarily to make phone calls. Instead, we mainly use our smartphones to access applications (apps).4 In June of last year, Apple announced that over 2 million apps were available on its App Store.5 For the most part, these

---

I am grateful to Kelvin Chen for his assistance in preparing this text.

apps were not created *or even envisaged* by Apple. These apps have been downloaded 130 billion times, generating over $50 billion in revenue for third-party developers.\(^6\)

The iPhone is a key platform on which that app ecosystem operates. How did that happen? Apple essentially made the smartphone a toolkit for third-party developers to experiment, innovate, build, and scale new apps. It did so by investing heavily in developing open application programming interfaces (APIs) that provided third-party developers clear instructions and open access to the iPhone platform. This strategy enabled those outside developers to build new applications that delivered Apple’s customers additional value by taking advantage of the existing functionality of the iPhone. Specifically, this open architecture makes available to outside developers clear instructions that enable them to use the iPhone’s various sensors, processors, displays, and other interfaces in combination with their own code to develop new products.

On top of that, a robust secondary layer of developers use the APIs of *other* developers in their technology stacks to quickly assemble new business models. Take ride-sharing services, for instance. They have built multibillion-dollar businesses that are, in large part, dependent on combinations of APIs from different companies. They may use Google Maps’ APIs for location services, Stripe or Braintree’s APIs for payments, Twilio’s APIs for text messaging, and Amazon Web Services’ or IBM’s APIs for computing power. All of these products, and more, work seamlessly together in real time to provide products that are so ubiquitous that we now use them as verbs for how we navigate the world. We “Uber” to the store or “Snapchat” a friend.

Risks and Opportunities in an Increasingly Interconnected World

There is every reason to expect financial services to make a similar transition to an increasingly interconnected digital world. By now, we’ve all heard estimates of the thousands of fintech companies that have launched in the past few years and the billions of investment dollars that are flooding into this sector. But for all of the talk of “disruption,” I want to underscore an important point: More often than not, there is a banking organization somewhere in the fintech stack. Just as third-party app developers rely on smartphone sensors, processors, and interfaces, fintech developers need banks somewhere in the stack for such things as: (a) access to consumer deposits or related account data, (b) access to payment systems, (c) credit origination, or (d) compliance management. For instance, account comparison services rely on access to data from consumers’ bank accounts. Savings and investment apps analyze transactions data from bank accounts to understand how to optimize performance and manage the funds consumers hold in those accounts. Digital wallets draw funds from payment cards or bank accounts. Marketplace loans most often depend on loan origination by a bank partner. And payment innovations often “settle up” over legacy payment rails, like the automated clearinghouse.

---


In short, the software stacks of almost all fintech apps point to a bank at one layer or another.

So as fintech companies and banks are catching up to the interconnected world, the various players are sorting out how best to do the connecting. Much of the work so far has been focused on the technical challenges, which are notable. Most banks’ core systems are amalgams of computing mainframes built decades ago before the Internet or cloud computing were widely available and, in many cases, stitched together over the course of mergers and consolidations. It takes a lot of investment to securely convert that infrastructure to platforms that can operate in real-time with ready access for Internet-native third-party developers.

But important policy, regulatory, and legal questions also demand attention. And that is where the smartphone analogy loses its power. On balance, bank activities are much more highly regulated than smartphones. Those regulations enable consumers to trust their banks to secure their funds and maintain the integrity of their transactions. While “run fast and break things” may be a popular mantra in the technology field, it is ill suited to an arena where a serious breach could undermine confidence in the payments system. Indeed, some of the key underpinnings of consumer protection and safety and soundness in the banking world--that consumers should be exceptionally careful in granting account access, that in certain conditions banks could be presumed to bear liability for unauthorized charges, and that banks can be held responsible for ensuring that service providers and vendors do right by their customers--sit

---

9 While Bitcoin is a notable exception, many consumers still rely on connecting their bank accounts with Bitcoin exchanges to convert their fiat currency to virtual currency and vice-versa.

uneasily alongside the requisites of openness, connectivity, and data access that enable today’s app ecosystem.\textsuperscript{11} For instance, before entering an outsourcing arrangement, a bank is expected to consider whether the service provider’s internal processes or systems (or even human error at the outside party) could expose the bank and its customers to potential losses or expose the bank’s customers to fraud and the bank to litigation; whether the service provider complies with applicable laws and regulation; and whether poor performance by that outside party could materially harm the bank’s public reputation.

The smartphone app ecosystem developed without the regulations or associated guardrails pertaining to institutions that people trust to hold their life savings. For instance, when Pokémon Go was first launched, its creator, Niantic, used an outdated Google API to verify consumer identities. This created confusion about whether millions of consumers had unwittingly granted Niantic full access to their e-mails, contact lists, and calendars.\textsuperscript{12} However, it did not stand in the way of Pokémon Go subsequently being downloaded a half billion times.\textsuperscript{13} In contrast, these kinds of mistakes in the banking sector could raise grave concerns about consumer data privacy and security and the integrity of consumer transactions data. That’s why banks are expected to conduct extensive risk assessments and due diligence of their service

\textsuperscript{11} See, e.g., 12 CFR §1005.1(b); appendix C to 12 CFR part 1005, comment 2(m)-2 (“If a consumer furnishes an access device and grants authority to make transfers to a person (such as a family member or co-worker) who exceeds the authority given, the consumer is fully liable for the transfers unless the consumer has notified the financial institution that transfers by that person are no longer authorized.”); Division of Banking Supervision and Regulation and Division of Consumer and Community Affairs, Board of Governors of the Federal Reserve System, “Guidance on Managing Outsourcing Risk,” \url{https://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf}, December 5, 2013.

\textsuperscript{12} See, e.g., Olivia Solon, “Have You Given Pokémon Go Full Access to Everything in Your Google Account?” Guardian, July 12, 2016, \url{www.theguardian.com/technology/2016/jul/11/pokemon-go-privacy-security-full-access-google-account} ("The discovery sparked a wave of fear that playing the game might allow its developers, Niantic Labs, to read and send email, access, edit and delete documents in Google Drive and Google Photos, and access browser and maps histories. In fact, both Google and Niantic Labs, say that ‘full access’ counterintuitively means nothing of the sort, a claim backed up by independent security researchers. The issue appears to stem from the fact that Niantic Labs uses an outdated version of Google’s shared sign-on service.")

\textsuperscript{13} See, e.g., Ben Gilbert, “Pokémon Go Has Been Downloaded over 500 Million Times,” Business Insider, September 7, 2016, \url{www.businessinsider.com/pokemon-go-500-million-downloads-2016-9}. 
providers, extending even to operations and internal controls, among other requirements.\footnote{See, e.g., Division of Banking Supervision and Regulation and Division of Consumer and Community Affairs, Board of Governors of the Federal Reserve System, “Guidance on Managing Outsourcing Risk,” www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf, December 5, 2013.}

While that helps ensure a safe and sound banking system, that also makes it more challenging for both the banks and fintech companies to harness safely the interconnectivity that has powered other parts of the digital world.

**Different Approaches to the Fintech Stack**

Because of the high stakes, fintech firms, banks, data aggregators, consumer groups, and regulators are all still figuring out how best to do the connecting. There are a few alternative approaches in operation today, with various advantages and drawbacks.

smartphone world. If a developer wants to use a Google Maps API to embed a map in her application, she first must create a developer account with Google, agreeing to Google’s terms and conditions. This means she will have entered a contract with the owner of the API, and the terms and conditions may differ depending on how sensitive the particular API is. Google may require only a minimum amount of information for a developer that wants to use an API to display a map. Google may, however, require more information about a developer that wants to use a different API to monitor the history of a consumer’s physical locations over the previous week. And in some cases, the competitive interests of Google and a third-party app developer may diverge over time, such that the original terms of access are no longer acceptable.16

The fact that it is possible and indeed relatively common for the API provider—the platform—to require specific controls and protections over the use of that API raises complicated issues when imported to the banking world. As banks have considered how to facilitate connectivity, the considerations include not only technical issues and the associated investment, but also the important legal questions associated with operating in a highly regulated sector. The banks’ terms of access may be determined in third-party service provider agreements that may offer different degrees of access. These may affect not only what types of protections and vetting are appropriate for different types of access over consumers’ funds and data held at a bank in order to enable the bank to fulfill its obligations for data security and other consumer protections, but also the competitive position of the bank relative to third-party developers.

There is a second broad type of approach in which many banks have entered into agreements with specialized companies that essentially act as middlemen, frequently described

---

16 The Financial Times reported that Uber will invest half a billion dollars into developing its own mapping software as it continues its push into driverless cars, thereby reducing its reliance on Google Maps. Leslie Hook, “Uber to Pour $500m into Global Mapping Project,” Financial Times, July 31, 2016, www.ft.com/cms/s/0%2Fe0dfa45e-5522-11e6-befd-2fe0c26b3c60.html?ft_site=falcon&desktop=true#axzz4G0M5oyu8.
as “data aggregators.” These banks may lack the budgets and expertise to create their own open APIs or may not see that as a key element in their business strategies. Data aggregators collect consumer financial account data from banks, on the one hand, and then provide access to that data to fintech developers, on the other hand.  

Data aggregators organize the data they collect from banks and other data sources and then offer their own suite of open APIs to outside developers. By partnering with data aggregators, banks can open their systems to thousands of developers, without having to invest in creating and maintaining their own open APIs. This also allows fintech developers to build their products around the APIs of two or three data aggregators, rather than 15,000 different banks and other data sources. And, if agreements between data aggregators and banks are structured as data aggregators performing outsourced services to banks, the bank should be able to conduct the appropriate due diligence of its vendors, whose services to those banks may be subject to examination by safety and soundness regulators.

Some banks have opted for a more “closed” approach to fintech developers by entering into individual agreements with specific technology providers or data aggregators. These

---

17 For example, one major data aggregator reports that about 70 percent of the data it collects from over 15,000 sources is collected via “structured feeds” under contractual agreements with financial institutions. See Envestnet, Inc., 2016 Annual Report, at 28, March 24, 2016.


agreements often impose specific requirements rather than simply facilitating structured data feeds. These banks negotiate for greater control over their systems by limiting who is accessing their data—often to a specific third party’s suite of products. Likewise, many banks use these agreements to limit what types of data will be shared. For instance, banks may share information about the balances in consumers’ accounts but decline to share information about fees or other pricing. While recognizing the legitimate need for vetting of third parties for purposes of the banks fulfilling their responsibilities, including for data privacy and security, some consumer groups have suggested that the standards for vetting should be commonly agreed to and transparent to ensure that banks do not restrict access for competitive reasons and that consumers should be able to decide what data to make available to third-party fintech applications.20

A third set of banks may be unable or unwilling to provide permissioned access, for reasons ranging from fears about increased competition to concerns about the cost and complexity of ensuring compliance with underlying laws and regulations. At the very least, banks may have reasonable concerns about being able to see, if not control, which third-party developers will have access to the banking data that is provided by the data aggregators. Accordingly, even banks that have previously provided structured data feeds to data aggregators may decide to limit or block access.21 In such cases, however, data aggregators can still move


21 See, e.g., Envestnet, Inc., 2016 Annual Report, March 24, 2016. (“[O]ne or more of our current customers could decide to limit or block our access to the data feeds we currently have in place with these customers due to factors outside of our control such as more burdensome regulation of our or our customers’ industry, increased compliance requirements or changes in business strategy. If the sources from which we obtain information that is important to
forward to collect consumer data for use by fintech developers without the permission or even potentially without the knowledge of the bank. Instead, data aggregators and fintech developers directly ask consumers to give them their online banking logins and passwords. Then, in a process commonly called “screen scraping,” data aggregators log onto banks’ online consumer websites, as if they were the actual consumers, and extract information. Some banks report that as much as 20 to 40 percent of online banking logins is attributable to data aggregators. They even assert that they have trouble distinguishing whether a computer system that is logging in multiple times a day is a consumer, a data aggregator, or a cyber attack.

For community banks with limited resources, the necessary investments in API technology and in negotiating and overseeing data-sharing agreements with data aggregators and third-party providers may be beyond their reach, especially as they usually rely on service providers for their core technology. Some fintech firms argue that screen scraping—which has drawn the most complaints about data security—may be the most effective tool for the customers of small community banks to access the financial apps they prefer—and thereby necessary to remain competitive until more effective broader industry solutions are developed.

Clearly, getting these connectivity questions right, including the need to manage the consumer protection risks, is critically important. It could make the difference between a world in which the fintech wave helps community banks become the platforms of the future, on the one hand, or, on the other hand, a world in which fintech instead further widens the gulf between community banks and the largest banks.

---

our solutions limit or restrict our ability to access or use such information, we may be required to attempt to obtain the information, if at all, through end user-permissioned data scraping or other means that could be more costly and time-consuming, and less effective or efficient. . . . The legal environment surrounding data scraping and similar means of obtaining access to information on third-party websites is not completely clear and is evolving, and one or more third parties could assert claims against us seeking damages or to prevent us from accessing information in that manner.”}
Tradeoffs

The different approaches to integrating banks into the fintech stack represent different risks and tradeoffs. Connectivity solutions that require intermediaries such as data aggregators and rely on screen scraping potentially create repositories of consumer credentials for hackers to target. Banks argue that if such a repository is breached, thousands of banks could be impacted.22 Further complicating things, because screen scrapers operate without contractual relationships with the banks from which they pull information, banks have little leverage or ability to vet the security of the screen scrapers’ systems and methods or their overall risk. In these circumstances, some commentators have noted that if a data aggregator or third-party developer is breached, it may not be clear who would bear responsibility for any losses—the bank, the data aggregator, the fintech developer, or the consumer. Some third-party developers have included terms and conditions that specifically limit their liability to consumers.23 It is not clear the extent to which many consumers understand the risks involved with sharing their banking credentials, the more limited liability accepted by many third-party developers relative to their bank or credit card issuer, and the fact that the third-party developers may in turn provide those credentials to others in some instances.


23 See, e.g, “Personal Capital Terms of Use” (last updated February 22, 2017), www.personalcapital.com/content/terms-of-use/ (last visited April 16, 2017). (“TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE LIABILITY OF PERSONAL CAPITAL, ITS AFFILIATES, LICENSORS AND AGENTS TO YOU SHALL NOT EXCEED ONE HUNDRED U.S. DOLLARS ($100).” Further, Personal Capital requires that consumers submit to pre-dispute arbitration agreements and waive any rights to pursue relief in a class action proceeding as part of its terms of use. This would mean that if a data breach were to occur, each affected consumer would have to seek relief on his own, with a maximum possible recovery of $100. In addition, Personal Capital’s terms and conditions specify that the arbitrator can require that the consumer pay Personal Capital’s legal fees, if Personal Capital is to prevail.
On the other side of the debate, fintech companies are concerned that banks could use their control over consumer data access in the context of bilateral contracts with data aggregators to leverage their position in order to impede competition elsewhere in the stack. This argument about access and competition echoes similar concerns in the smartphone arena.24

Further, third-party developers argue that open standards for data access can help banks meet consumers’ expectations for mobile banking by providing access to the fintech apps that best serve their needs. The relatively open architecture of the iPhone platform means that Apple profits from outside developers’ products without having to design or invest in them directly. For instance, Apple didn’t include a home-grown mapping app during the first few years of the iPhone.25 Instead, it relied on Google to provide that important function for its smartphones before trying to build its own mapping tool—a process that took a number of iterations before getting it right. Open platform strategies may mean that banks can essentially outsource product development to fintech firms.26 This could be a boon—particularly for small community banks.

24 When the iPhone first launched, for instance, one phone provider paid a premium for exclusive access to the smartphone. This meant that, for several years, consumers that wanted the iPhone also had to enter relationships with the only Internet service provider platform that offered the phone. See, e.g., Saul Hansell, “Why AT&T Wants to Keep the iPhone Away from Verizon,” New York Times, April 22, 2009, https://bits.blogs.nytimes.com/2009/04/22/why-att-wants-to-keep-the-iphone-away-from-verizon/ (“AT&T is paying Apple an unusually high subsidy on top of the $199 and $299 paid by iPhone buyers. But it appears to be getting quite a return on that investment.”) At the same time, Apple has used its own iPhone platform to affect the development of products further up the stack. While much of the iPhone is an open platform for third-party developers, developers do not have access to the iPhone’s secure element and Near Field Communication (NFC) antenna—key components of digital wallet technologies. This means that Apple Pay is the only “tap-to-pay” NFC digital wallet available for iPhones—and that Apple Pay competitors, like Android Pay and Samsung Pay, are unable to access 40 percent of the smartphones in the United States. See, e.g., Philip Elmer-DeWitt, “About Apple’s 40% Share of the U.S. Smartphone Market,” Fortune, February 11, 2016, http://fortune.com/2016/02/11/apple-iphone-ios-share/. When a group of Australia’s largest banks recently petitioned the country’s antitrust authority to allow them to band together to require Apple to unlock access to the NFC antenna, for use by their digital wallets, their request was denied. See, e.g., Simon Sharwood, “Banking Group Denied Access to iPhones’ NFC Chips for alt.Apple.Pay,” Register, April 3, 2017, www.theregister.co.uk/2017/04/03/banking_group_denied_access_to_iphones_nfc_chips_for_altapplepay/
25 See, e.g., Chance Miller, Apple Maps Now Used 3x as Often as Google Maps on iOS, Serving 5B Requests per Week, 9to5Mac, December 7, 2015, https://9to5mac.com/2015/12/07/apple-maps-usage-numbers/.
26 For example, small business lender Kabbage, Inc. has entered agreements with large banks, where Kabbage licenses its data analysis-heavy customer acquisition platform to banking partners who then go on to originate, fund, and service the underlying loans. See, e.g., Kabbage Inc., “Kabbage and Santander UK Partner to Accelerate SMB
that would not have to worry about developing the best consumer interface, mobile app, digital wallet, or lending product. The bank would only have to worry about getting the connections to an open API right and then reap the benefits of the innovation by third parties.

**Regulatory Developments**

As regulators, 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. More broadly, we have a strong interest in permitting socially beneficial innovations to flourish, while ensuring the risks that they may present are appropriately managed, consistent with the legal requirements. We do not want to unnecessarily restrict innovations that can benefit consumers and small businesses through expanded access to financial services or greater efficiency, convenience, and reduced transaction costs. Nor do we want to drive these activities away from regulated banks and toward less governed spaces in the financial system.

Regulators in the United Kingdom and continental Europe have recently outlined new approaches to facilitate connectivity in financial services, while attempting to mitigate the associated risks. In August 2016, the UK Competition & Markets Authority (CMA) released a package of mandates aimed at increasing competition for consumer and small business current accounts (akin to U.S. checking accounts).27 This year nine of the country’s largest banks were

---

27 UK Competition & Markets Authority, “CMA Paves the Way for Open Banking Revolution,” press release, August 9, 2016, [www.gov.uk/government/news/cma-paves-the-way-for-open-banking-revolution](http://www.gov.uk/government/news/cma-paves-the-way-for-open-banking-revolution). ("[O]lder and larger banks do not have to compete hard enough for customers’ business, and smaller and newer banks find it difficult to grow. This means that many people are paying more than they should and are not benefiting from new services. To tackle these problems, the CMA is implementing a wide-reaching package of reforms. Central to the CMA’s remedies are measures to ensure that customers benefit from technological advances and that new entrants and smaller providers are able to compete more fairly."); UK Competition & Markets Authority, Retail Banking Market Investigation: Final Report," August 9, 2016,
required to create open APIs to share nonsensitive, non-consumer-specific information, like pricing, fees, terms, and conditions as well as branch and automated teller machine locations.\textsuperscript{28} This initial limited sharing of information has started communication and collaboration across the industry on areas like data standards and organizational governance, which will facilitate work on more contentious questions. Before March 2018, the CMA is scheduled to enforce a broader package of reforms, including mandating that the nine banks create APIs that allow third-party banks and nonbanks to access consumer accounts for reading transaction data and payment initiation.

In the European Union, beginning in 2018, member states will be required to start implementing the European Parliament’s revised Payment Services Directive (PSD2).\textsuperscript{29} Among other elements, PSD2 created licensing regimes for third parties that access bank accounts for purposes of initiating payment orders or consolidating information with consumers’ consent.\textsuperscript{30} The directive mandates that banks allow these licensed third parties to access their consumer accounts (with consumer permission) without premising such access on contractual agreements with the banks. Indeed, PSD2 requires that credit institutions not block or hinder access to payment accounts and that licensed third parties have access to credit institutions’ payment accounts services in an objective, nondiscriminatory, and proportionate manner. When credit

\textsuperscript{28} The nine banks include the five largest banks in Great Britain (Lloyd’s Banking Group, Royal Bank of Scotland, HSBC Group, Barclays, and Santander UK plc); three leading banks in Northern Ireland (Allied Irish Bank, Bank of Ireland, and Danske Bank) and the largest UK building society, Nationwide Building Society.  
\textsuperscript{30} Specifically, Payment Initiation Service Providers (PISPs) initiate payment orders at the request of a user with respect to funds held in another entity’s bank account; Account Information Service Providers (AISPs) are online services that consolidate information, with consumers’ consent, from those consumers’ accounts at other entities.
institutions do reject access, they are required to provide the relevant authorities detailed reasoning for the rejection.

The directive attempts to mitigate the attendant data-security and consumer-protection risks with a number of measures that, by and large, are not readily available policy options in the United States. Importantly, third parties that access bank accounts will be subject to licensing and registration requirements, as well as associated capital and insurance requirements. Moreover, the directive envisions that electronic payments will be authorized by two-factor authentication—for example “something you know” and “something you are.”

The United States is likely to address these issues in a different way, at least initially, given that regulatory authorities are more broadly distributed, and the relevant statutory language predates these technological developments. The Consumer Financial Protection Bureau (CFPB) issued a Request for Information last fall to explore issues surrounding consumers’ granting access to account information to third parties. Of course, safety and soundness regulation—and with it, concerns about data security, cyber security, and vendor risk management—is distributed among a number of regulators. For instance, there may be value to examining the vendor risk management guidance so that it facilitates banks connecting more securely and efficiently with the fintech apps that consumers prefer. Similarly, it could be useful to periodically assess whether and how authority under the Bank Service Company Act might pertain to developments

31 With limited exceptions, such as for de minimis transactions.
in the fast evolving fintech sector. In addition, the private sector is continuing to actively experiment with a variety of different approaches to the connectivity question and may itself move toward one or more widely accepted standards. Accordingly, efforts to craft approaches that enhance connectivity while mitigating the associated risks will likely benefit from the engagement of multiple agencies, along with input from the private sector and other stakeholders.

Separately, the Office of the Comptroller of the Currency (OCC), which is responsible for administering national bank charters, has announced that it is exploring offering “special purpose national bank charters” to fintech companies. As envisioned by the OCC, obtaining a special purpose charter would have the practical effect of allowing certain fintech companies (companies that make loans, make payments, or accept deposits) to potentially bypass the need for connecting to a bank for certain purposes in favor of becoming licensed as banks themselves. The OCC’s proposal raises interpretive and policy issues for the Federal Reserve regarding whether charter recipients would become Federal Reserve members or have access to Federal Reserve accounts and services, such as direct access to payment systems. If the OCC proposal is finalized, the Federal Reserve would have to closely analyze these issues with respect to any fintech firms that express an interest in moving forward with an application.

When Apple launched the iPhone in 2007, who could have predicted that it would net billions from a game like Pokémon Go, which involved no investment, development, or advertising on Apple’s part beyond opening its platform to developers? It is still too early to have any confidence that we know which fintech innovations will prove to be the most long-

lasting or widely adopted. By the same token, the fintech industry is still figuring out the fundamental questions of the best ways to make the necessary connections to the banking platforms to facilitate consumers’ ability to better monitor and manage their financial lives, while providing the level of data security and protection they have come to rely on from their banks.\textsuperscript{35} Change is surely coming, as financial products and services move onto interconnected platforms. As the sector evolves, it’s important that all parties involved pay close attention not only to the technical questions, but to the requisite regulatory, policy, and legal considerations to ensure continued trust and confidence in the financial system.

Where Do Consumers Fit in the Fintech Stack?

Remarks by

Lael Brainard

Member

Board of Governors of the Federal Reserve System

at

“FinTech Risks and Opportunities: An Interdisciplinary Approach”
a conference sponsored by the University of Michigan

Ann Arbor, Michigan

November 16, 2017
The new generation of fintech tools offers the potential to help consumers manage their increasingly complicated financial lives, but also poses risks that will need to be managed as the marketplace matures.¹

In many ways, the new generation of fintech tools can be seen as the financial equivalent of an autopilot. The powerful new fintech tools represent the convergence of numerous advances in research and technology--ranging from new insights into consumer decisionmaking to a revolution in available data, cloud computing, and artificial intelligence (AI). They operate by guiding consumers through complex decisions by offering new ways of looking at a consumer’s overall financial picture or simplifying choices, for example with behavioral nudges.

As consumers start to rely on financial autopilots, however, it is important that they remain in the driver’s seat and have a good handle on what is happening under the hood. Consumers need to know and decide who they are contracting with, what data of theirs is being used by whom and for what purpose, how to revoke data access and delete stored data, and how to seek relief if things go wrong. In short, consumers should remain in control of the data they provide. In addition, consumers should receive clear disclosure of the factors that are reflected in the recommendations they receive. If these issues can be appropriately addressed, the new fintech capabilities have enormous potential to deliver analytically grounded financial services and simplified choices, tailored to the consumers’ needs and preferences, and accessible via their smartphones.²

¹ I am grateful to Kelvin Chen for his assistance in preparing this text. The remarks represent my own views, which do not necessarily represent those of the Federal Reserve Board or the Federal Open Market Committee.
Consumers Face Complex Financial Choices

When the first major “credit card,” the Diner’s Club Card, was introduced in 1949, consumers could only use the cardboard card at restaurants and, importantly, only if they paid the entire amount due each month. Today, the average cardholder has about four credit cards, and the Federal Reserve Bank of New York estimates that American consumers collectively carry $785 billion in credit card debt.

When signing up for a credit card, consumers face a bewildering array of choices. Half of consumers report that they select new cards based on reward programs, weighing “cash back” offers against “points” with their credit card provider that may convert into airline or hotel “miles,” which may have varying values depending on how they are redeemed. In some cases, rewards may apply to specific spending categories that rotate by quarter and require that consumers re-register each term, and the rewards may expire or be forfeited under complicated terms.

In some cases, the choices may be confusing. Let’s take the example of zero percent interest credit card promotions. A consumer may choose a zero percent interest credit card promotion and expect to pay no interest on balances during a promotional period, after which any balances are assessed at a higher rate of interest going forward. But if a consumer instead

---

chooses a zero percent interest private-label credit card with deferred interest and has a positive balance when the promotional period expires, interest could be retroactively assessed for the full time they held a balance during the promotional period. Even sophisticated consumers could be excused for confusing these products.

As it turns out, it is often the most vulnerable consumers who have to navigate the most complicated products. For instance, one recent study of the credit card market found that the average length of agreements for products offered to subprime consumers was 70 percent longer than agreements for other products.

The complexity multiplies when we go beyond credit cards and consider other dimensions of consumers’ financial lives. The Federal Deposit Insurance Corporation has found that nearly a quarter of the Americans that don’t maintain bank accounts are concerned that bank fees are too unpredictable. Even though mortgage debt is over two-thirds of household debt, nearly half of consumers don’t comparison shop before taking out a mortgage. Student loans now make up 11 percent of total household debt, more than twice its share in

---

8 Id at section 5.1.2.
2008. Over 11 percent of student debt is more than 90 days delinquent or in default—and researchers at the Federal Reserve Bank of New York estimate that this figure may understate the problem by as much as half.

Today, consumers navigate numerous weighty financial responsibilities for themselves and their dependents. It seems fair to assume they could use some help managing this complexity. In the Federal Reserve Board’s annual Survey of Household Economics and Decisionmaking (SHED), more than half of respondents reported that their spending exceeded their income in the prior year. Indeed, 44 percent of SHED respondents reported that they could not cover an emergency expense costing $400 without selling something or borrowing money.

New Tools to Help Consumers Manage Their Finances

Given the complexity and importance of these decisions, it is encouraging to see the fast-growing development of advanced, technology-enabled tools to help consumers navigate the

---


13 Federal Reserve Bank of New York, Quarterly Report on Household Debt and Credit, August 2017, www.newyorkfed.org/medialibrary/interactives/householdcredit/data/pdf/HHDC_2017Q2.pdf. (“[D]elinquency rates for student loans are likely to understate effective delinquency rates because about half of these loans are currently in deferment, in grace periods or in forbearance and therefore temporarily not in the repayment cycle. This implies that among loans in the repayment cycle delinquency rates are roughly twice as high.” Id. n.2.)


16 Id.
complex issues in their financial lives. These tools build on important advances in our understanding of consumer financial behavior and the applications, or “app,” ecosystem.

Researchers have invested decades of work exploring how consumers actually make decisions. We all tend to use shortcuts to simplify financial decisions, and it turns out many of these can prove faulty, particularly when dealing with complex problems.\(^{17}\) For example, empirical evidence consistently shows that consumers overvalue the present and undervalue the future.\(^{18}\) Researchers have documented that consumers make better savings decisions when they are presented with fewer options.\(^{19}\) They have shown the importance of “anchoring” bias—the tendency to place disproportionate weight on the first piece of information presented. This bias can lead consumers either to make poor financial choices or instead to tip the scales in favor of beneficial choices, as with automatic savings defaults.\(^{20}\) Similarly, “nudges” can help consumers

---

\(^{17}\) See, e.g., Krista Tippett, *On Being*, radio interview with Daniel Kahneman, October 5, 2017, https://onbeing.org/programs/daniel-kahneman-why-we-contradict-ourselves-and-confound-each-other-oct2017/. (“…[I]t is actually completely not possible for a finite human mind to be rational or to obey the axioms of rationality. You’d have to know too much . . . [T]he cognitive rules are, to a large extent, simplifying rules. They are shortcuts.”)


in the right circumstances or instead backfire in surprising ways.\textsuperscript{21}

These behavioral insights are especially powerful when paired with the remarkable advances we have seen in the technological tools available to the average consumer, especially through their smartphones.\textsuperscript{22} Smartphones are ubiquitous. The 2016 Federal Reserve Survey of Consumer and Mobile Financial Services (SCMF) found that 87 percent of the U.S. adult population had a mobile phone, the vast majority of which were smartphones.\textsuperscript{23} Smartphone use is prevalent even among the unbanked and underbanked populations. Survey evidence suggests we are three times more likely to reach for our phone than our significant other when we first wake up in the morning.\textsuperscript{24}

Some evidence suggests that smartphones are already helping consumers make better financial decisions. The 2016 SCMF found that 62 percent of mobile banking users checked their account balances on their phones before making a large purchase, and half of those that did


\textsuperscript{24} See Bank of America, Trends in Consumer Mobility Report, 2015, http://newsroom.bankofamerica.com/files/doc_library/additional/2015_BAC_Trends_in_Consumer_Mobility_Report.pdf. (Finding that 35 percent of survey respondents reported that they reach for their mobile devices first thing, as compared to 10 percent for their significant other.)
so decided not to purchase an item as a result. In addition, 41 percent of smartphone owners checked product reviews or searched product information online while shopping in a retail store, and 79 percent of those respondents reported changing their purchase decision based on the information they accessed on their smartphone.

And those use cases just scratch the surface of what is possible. First of all, the smartphone platform has become a launch pad for a whole ecosystem of apps created by outside developers for a wide variety of services, including helping consumers manage their financial lives.

Second, the smartphone ecosystem puts the enormous computing power of the cloud at the fingertips of consumers. Interfacing with smartphone platforms and other apps, outside developers can tap the computing power of the leading cloud computing providers in building their apps. Importantly, cloud computing offers not only the power to process and store data, but also powerful algorithms to make sense of it. Due to early commitment to open-source principles, app developers have open access to many of the same machine-learning and artificial intelligence tools that power the world’s largest internet companies. Further, the major cloud computing providers have now taken these free building blocks and created different machine-learning and artificial intelligence stacks on their cloud platforms. A developer that wants to incorporate artificial intelligence into their financial management app can access off-the-shelf

_____________________

26 Id.
models of cloud computing providers, potentially getting to market faster than by taking the traditional route of finding training data and building out models in-house from scratch.

Third, fintech developers can also draw from enormous pools of data that were previously unavailable outside of banking institutions. Consumer financial data are increasingly available to developers via a new breed of business-to-business suppliers, called data aggregators. These companies enable outside developers to access consumer account and transactional information typically stored by banks. But aggregators do more than just provide access to raw data. They facilitate its use by developers, by cleaning the data, standardizing it across institutions, and offering their own application programming interfaces for easy integration. Further, similar to cloud computing providers, data aggregators are also beginning to provide off-the-shelf product stacks on their own platforms. This means that developers can quickly and easily incorporate product features, such as predicting creditworthiness, determining how much a consumer can save each month, or creating alerts for potential overdraft charges.

Researchers have documented the benefits of tailored one-on-one financial coaching. Until recently, though, it has been hard to deliver that kind of service affordably and at scale, due to differences in consumers’ circumstances. Let’s again consider the example of deferred interest credit cards. It turns out only a small minority of consumers miss the deadlines for repaying promotional balances and are charged retroactive interest payments, and they typically

---

have deep subprime scores. Similarly, for consumers that opt into overdraft products on their checking accounts, 8 percent of consumers pay 75 percent of the fees. Up until now, it has been hard for consumers to understand those odds and objectively assess whether they are likely to be in the group of customers that will face challenges with a particular financial product. The convergence of smartphone ubiquity, cloud computing, data aggregation, and off-the-shelf AI products offer the potential to make tailored financial advice scalable. For instance, a fintech developer could pair historical data about how different types of consumers fare with a specific product, on the one hand, with a consumer’s particular financial profile, on the other hand, to make a prediction about how that consumer is likely to fare with the product.

The Evolution of Financial Autopilots

Since the early days of internet commerce, developers have tried to move beyond simple price comparison tools to offer tailored “agents” for consumers that can recommend products based on analyses of individual behavior and preferences. Today, a new generation of personal financial management tools seems poised to make that leap. When a consumer wishes to select a new financial product, he or she can now solicit options from a number of websites and mobile apps. These new comparison sites can walk the consumer through a wide array of financial products, offering to compare features like rewards, fees, and rates, or tailoring to a consumer’s stated goals. Some fintech advisors ask consumers to provide access to their bank accounts,

retirement accounts, college savings accounts, and other investment platforms in order to enable a fintech advisor to offer a consumer a single, near complete picture of his balances and cash flows across different institutions.

In reviewing the advertising, terms and conditions, and apps of an array of fintech advisors, it appears that many of these tools offer advanced data analysis, machine learning, and even artificial intelligence to help consumers cut down on unnecessary spending, set aside money for savings, and use healthy nudges to improve their financial decisions. For instance, a fintech advisor may help a consumer automate savings “rules,” like rounding up charges and putting the difference into savings, enabling these small balances to accumulate over time or setting a small amount of money aside every time a consumer spends money on little splurges.

The early stages of innovation inevitably feature a lot of learning from trial and error. Fortunately, as the fintech ecosystem advances, there are useful experiences and good practices to draw upon from the evolution of the commercial internet. To begin with, one internet adage is that if a product is free, “you are the product.”34 In this vein, fintech advisors frequently offer free services to consumers and earn their revenue from the credit cards and other financial products that they recommend through lead generation.

Of course, many fintech advisors are not lead generators. Some companies offer fee-for-service models, with consumers paying a monthly fee for the product. Other companies are paid by employers, who then provide the products free of charge to their employees as an employee benefit. In these cases, they likely have quite different business models.

---

But for those services that do act as lead generators, there are important considerations about whether and how best to communicate information to the consumer about the nature of the recommendations being made. For instance, according to some reports, fintech advisors can make between $100 and $700 in lead generation fees for every customer that signs up for a credit card they recommend.35

In many cases, a fintech advisor may describe their service as providing tailored advice or making recommendations as they would to friends and family. In such cases, a consumer might not know whether the order in which products are presented by a fintech assistant is based on the product’s alignment with his or her needs or different considerations. Different fintech advisors may order the lists they show consumers using different criteria. A product may be at the top of the advisor’s recommendations because the sponsoring company has paid the advisor to list it at the top, or the sponsoring company may pay the fintech assistant a high fee, contingent upon the consumer signing up for the product. Alternatively, a fintech advisor may change the order of the loan offers or credit cards based on the likelihood that the consumer will be approved. Moreover, in some cases, the absence of lead generation fees for a particular product may impact whether that product is on the list shown to consumers at all.

There appears to be a wide variety of practices regarding the prominence and placement of advertising and other disclosures relative to the advice and recommendations such firms

provide. Overall, fintech assistants have increasingly improved the disclosures that explain to consumers how they get paid, but this is still a work in progress.

The good news is that these challenges are not new. The experience with internet search engines outside of financial products, such as Google, Bing, and Yahoo!, as well as with other product comparison sites, such as Travelocity and Yelp, may provide useful guidance. As consumers and businesses have adapted to the internet, we have, collectively, adopted norms and standards for how we can expect search and recommendation engines to operate. In particular, we generally expect that search results will be included and ranked based on what’s organically most responsive to the search—unless it is clearly labeled otherwise. According to a Federal Trade Commission staff letter, search results will be included and ranked based on what’s organically most responsive to the search—unless it is clearly labeled otherwise. Accordingly, when we search for a product, we now know to look for visual cues that identify paid search results, usually in the form of a text label like “Sponsored” or “Ad”, different formatting, and visually separating advertising from natural search results. Even when an endorsement is made in a brief Twitter update, we now expect disclosures to be clear and conspicuous.

As fintech advisors evolve to engage consumers in new ways, disclosure methodologies will no doubt be expected to adapt as well. For instance, some personal financial management

---


tools now interact with consumers via text message. If consumers move to a world in which most of their interactions with their advisors occur via text-messaging “chatbots”--or voice communication--I am hopeful that industry, regulators, consumers, and other stakeholders will work together to adapt the norms to distinguish between advice and sponsored recommendations.

The Data Relationship

While the lead generation revenue model presents some familiar issues that are readily apparent, under the hood, fintech relationships raise even more complex issues for consumers in knowing who they are providing their data to, how their data will be used, for how long, and what to expect in the case of a breach or fraud. Let me briefly touch on each issue in turn.

Often, when a consumer signs up with a fintech advisor or other fintech app, they are asked to log into their bank account in order to link the fintech app with their bank account data. In reviewing apps’ enrollment processes, it appears that consumers are often shown log-in screens featuring bank logos and branding, prompting consumers to enter their online banking logins and passwords. In many cases, the apps note that they do not store the consumers’ banking credentials.

When the consumer logs on, he or she is often not interfacing with a banks’ computer systems, but rather, providing the bank account login and password to a data aggregator that provides services to the fintech app. In many cases, the data aggregator may store the password and login and then use those credentials to periodically log into the consumer’s bank account and copy available data, ranging from transaction data, to account numbers, to personally identifiable information. In other cases, things work differently under the hood. Some banks and data aggregators have agreed to work together to facilitate the ability to share data with outside
developers in authorized ways. These agreements may delineate what types of data will be shared, and authorization credentials may be tokenized so that passwords are never stored by the aggregator.39

It is often hard for the consumer to know what is actually happening under the hood of the financial app they are accessing. In most cases, the log in process does not do much to educate the consumer on the precise nature of the data relationship. Screen scraping usually invokes the bank’s logo and branding but infrequently shows the logo or name of the data aggregator. In reviewing many apps, it appears that the name of the data aggregator is frequently not disclosed in the fintech app’s terms and conditions, and a consumer generally would not easily see what data is held by a data aggregator or how it is used. The apps, websites, and terms and conditions of fintech advisors and data aggregators often do not explain how frequently data aggregators will access a consumer’s data or how long they will store that data.40

Recognizing this is a relatively young field, but one that is growing fast, there are a myriad of questions about the consumer’s ability to opt out and control over data that will need to be addressed appropriately. In examining the terms and conditions for a number of fintech apps, it appears that consumers are rarely provided information explaining how they can


terminate the collection and storage of their data. For instance, when a consumer deletes a fintech app from his or her phone, it is not clear this would guarantee that a data aggregator would delete the consumer’s bank login and password, nor discontinue accessing transaction information. If a consumer severs the data access, for instance by changing banks or bank account passwords, it is also not clear how he or she can instruct the data aggregator to delete the information that has already been collected. Given that data aggregators often don’t have consumer interfaces, consumers may be left to find an email address for the data aggregator, send in a deletion request, and hope for the best.

If things go wrong, consumers may have limited remedies. In reviewing terms, it appears that many fintech advisors include contractual waivers that purport to limit consumers’ ability to seek redress from the advisor or an underlying data aggregator. In some cases, the terms and conditions assert that the fintech developer and its third-party service providers will not be liable to consumers for the performance of or inability to use the services. It is not uncommon to see terms and conditions that limit the fintech adviser’s liability to the consumer to $100.

Traditionally, under the Electronic Funds Transfer Act and its implementing Regulation E, consumers have had protections to mitigate their losses in the event of erroneous or fraudulent transactions that would otherwise impact their credit and debit cards, such as data breaches. Those protections are not absolute, however.41 In particular, if a consumer gives another person an “access device” to their account and grants them authority to make transfers, then the consumer is “fully liable” for transfers made by that person, even if that person exceeds his or

41 See 12 CFR section 1005.2(m) (1). (Excluding from the definition of “unauthorized electronic fund transfer” any “electronic fund transfer initiated… [by] a person who was furnished the access device to the consumer’s account by the consumer…..”)
her authority, until the consumer notifies the bank. As the industry matures, the various stakeholders will need to develop a shared understanding of who bears responsibility in the event of a breach.

Shared Responsibility and Shared Benefit Moving Forward

So what can be done to make sure consumers have the requisite information and control to remain squarely in the driver’s seat? Establishing and implementing new norms is in the shared interest of all of the participants in the fintech stack. For instance, in the case of credit cards, mortgages, and many other products, it is often banks or parties closely affiliated with banks that pay fees to fintech advisors to generate leads for their products, pursuant to a contract. Through these contractual relationships with fintech advisors, banks have considerable influence in the lead generation relationship, including through provisions describing how a sponsored product should be described or displayed. Banks have a stake in ensuring that their vendors and third-party service providers act appropriately, that consumers are protected and treated fairly, and that the banks’ reputations aren’t exposed to unnecessary risk. Likewise, some of the leading speech-only financial products are currently credit card and bank products.
Accordingly, banks have incentives to invest in innovating the way they disclose information to consumers, as they also invest in new ways of interacting with them.

As for consumers’ relationships with data aggregators, there’s an increasing recognition that consumers need better information about the terms of their relationships with aggregators, more control over what is shared, and the ability to terminate the relationship.46 We have spoken to data aggregators who recognize the importance of finding solutions to many of the complex issues involved with the important work of unlocking the potential of the banking stack to developers. And while there are some difficult issues in this space, other issues seem relatively straightforward. It shouldn’t be hard for a consumer to be informed who they are providing their credentials to. Consumers should have relatively simple means of being able to consent to what data are being shared and at what frequency. And consumers should be able to stop data sharing and request the deletion of data that have been stored.

Responsibility for establishing appropriate norms in the data aggregation space should be shared, with banks, data aggregators, fintech developers, consumers, and regulators all having a role.47 Banks and data aggregators are negotiating new relationships to determine how they can work together to provide consumers access to their data, while also ensuring that the process is


secure and leaves consumers in the driver’s seat. In many cases, banks themselves were often the original customers of data aggregators, and many continue to use these services. According to public filings, more than half of the 20 largest banks are customers of data aggregators. The banks have an opportunity as customers of data aggregation services to ensure that the terms of data provision protect consumers’ data and handle it appropriately.

Regulators also recognize that there may be opportunities to provide more clarity about how the expectations about third-party risk management would work in this sector, as well as other areas experiencing significant technological change. Through external outreach and internal analysis, we are working to determine how best to encourage socially beneficial innovation in the marketplace, while ensuring that consumers’ interests are protected. We recognize the importance of working together and the potential to draw upon existing policies, norms, and principles from other spaces. Consumers may not fully understand the differences in regulations across financial products or types of financial institutions, or whether the rules change when they move from familiar search and e-commerce platforms to the fintech stack. Consumers, as well as the market as a whole, will benefit if regulators coordinate to provide more unified messages and support the development of standards that serve as a natural extension of the common-sense norms that consumers have come to expect in other areas of the commercial internet.


Conclusion

The combination of technologies that put vast computing power, rich data sets, and artificial intelligence onto simple smartphone apps together with important research into consumer financial behaviors has great potential to help consumers navigate their complex financial lives more effectively, but there are also important risks. I am hopeful that fintech developers, data aggregators, bank partners, consumers, and regulators will work together to keep consumers in the driver’s seat as we move forward with these new technologies. If we work together effectively toward this goal, the fintech stack may be able to offer enormous benefits to the consumers they aim to serve, while appropriately identifying and managing the risks.
**October 18, 2017**

**Consumer Protection Principles:**

**Consumer-Authorized Financial Data Sharing and Aggregation**

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

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

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

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

---

² 12 U.S.C. 5511(b)(5).
The Bureau recognizes that many consumer protections apply to this market under existing statutes and regulations. These Principles are not intended to alter, interpret, or otherwise provide guidance on—although they may accord with—the scope of those existing protections. Thus, the Principles do not themselves establish binding requirements or obligations relevant to the Bureau’s exercise of its rulemaking, supervisory, or enforcement authority. In addition, the Principles are not intended as a statement of the Bureau’s future enforcement or supervisory priorities.

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

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

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

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

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

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

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

5) **Security**

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

6) **Access Transparency**

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

7) **Accuracy**

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

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

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

9) **Efficient and Effective Accountability Mechanisms**

The goals and incentives of parties that grant access to, access, use, store, redistribute, and dispose of consumer data align to enable safe consumer access and deter misuse. Commercial participants are accountable for the risks, harms, and costs they introduce to consumers. Commercial participants are likewise incentivized and empowered effectively to prevent, detect, and resolve unauthorized access and data sharing, unauthorized payments conducted in connection with or as a result of either authorized or unauthorized
data sharing access, data inaccuracies, insecurity of data, and failures to comply with other obligations, including the terms of consumer authorizations.
Connect America Fund\textsuperscript{37} will be implemented and will provide additional funding for rural fixed broadband over the next decade.\textsuperscript{38} Additional support for these efforts is reflected in Executive Order 13821, which states that “it shall therefore be the policy of the executive branch to use all viable tools to accelerate the deployment and adoption of affordable, reliable, modern, high-speed broadband connectivity in rural America.”\textsuperscript{39} Concurrently, the President instructed the Secretary of the Interior to develop a plan to increase access to tower facilities and other infrastructure managed by the Department of the Interior in rural America for broadband deployment.\textsuperscript{40}

Deployment of more infrastructure to support broadband in rural areas will help to close the digital divide and assist more Americans in underserved communities to participate in the digital economy and overcome geographic isolation.

**Consumer Financial Data**

As a result of digitization, vast amounts of data now exist in forms that can be readily aggregated and analyzed with computing power. Online and mobile applications that draw on these data make it possible for consumers to view banking and other financial account information, often held at different financial institutions, on a single platform, monitor the performance of their investments in real-time, compare financial and investment products, and even make payments or execute transactions. Applications can also assist with automatic savings, budget advice, credit decisions, and fraud and identity theft detection in real-time.\textsuperscript{41}

In short, digitized record-keeping and these applications have exponentially improved a consumer’s ability to make financial decisions. It has given rise to a new sector of nonbank financial institutions focused on products and services utilizing data aggregation, based on data obtained with the consumer’s consent. The rise of such financial institutions presents questions regarding the way in which they operate and are currently regulated.

\textsuperscript{37} The Connect America Fund, also known as the Universal Service High-Cost Fund, is the FCC’s program to expand voice and broadband services for areas where they are unavailable.


\textsuperscript{39} Executive Order 13821, Streamlining and Expediting Requests to Locate Broadband Facilities in Rural America (Jan. 8, 2018) [83 Fed. Reg. 1507 (Jan. 11, 2018)].

\textsuperscript{40} Executive Office of the President, Supporting Broadband Tower Facilities in Rural America on Federal Properties Managed by the Department of the Interior (Jan. 8, 2018) [83 Fed. Reg. 1511 (Jan. 12, 2018)].

Data Aggregation

Data aggregation generally refers to any process in which information from one or more sources is compiled and standardized into a summary form. Often data are aggregated for specific business or research purposes such as statistical analysis, performance tracking, or recordkeeping. As of the end of June 2018, five of the largest publicly-traded U.S. companies by market capitalization are integral drivers of the digital economy and use data aggregation for telecommunications, logistics, marketing, social media, and other purposes.

How Data Aggregation Works

At the most basic level, data aggregation in the financial services sector necessarily involves consumers, financial services firms, data aggregators, and consumer financial technology (fintech) application providers. “Consumers” are the individuals who are users of financial services and the principal providers of the information collected by financial service companies. In the consumer financial services data aggregation framework, consumers decide which applications to use in order to access their data, give consent for that access, and provide necessary authentication (i.e., login) information.

“Financial services companies” or “financial services firms” include banks, mutual funds, insurance companies, broker-dealers, wealth management firms, and other financial institutions that provide traditional retail banking, depository, credit, brokerage, investment, and other account management services to consumers. These companies are the sources of consumer financial account and transaction data.

“Data aggregators” are the firms that access, aggregate, share, and store consumer financial account and transaction data they acquire through connections to financial services companies. Aggregators are intermediaries between the fintech applications that consumers use to access their data, on the one hand, and the sources of data at financial services companies on the other. An aggregator may be a generic provider of data to consumer fintech application providers and other third parties, or it may be part of a company providing branded and direct services to consumers.

Finally, “consumer fintech application providers” are the firms that access consumer financial account and transaction data, either from data aggregators or financial services companies, in order to provide value-added products and services to consumers. Consumers access these services through “fintech applications” — i.e., the websites or mobile apps — created by these firms. Consumer fintech application providers may also have direct links to financial services companies in order to, for example, provide direct services to a bank’s customers, access payments systems, or facilitate credit origination.

Operationally, the key data aggregation processes involve acquiring, compiling, standardizing, and disseminating consumer financial data. Data aggregators may differ in the breadth and sophistication of the aggregation services they offer, and may specialize in different types of data or target a


43. These companies are Apple, Amazon, Alphabet [Google], Microsoft, and Facebook, based on Treasury analysis of Bloomberg data.
Some data aggregators may focus on aggregating financial account balances, transactions data, or credit card activity, for example, or they may primarily support consumer fintech application providers geared toward offering specific products (such as auto loans or mortgages) or services (such as peer-to-peer payments or budget tracking).

In general, data aggregators make data available by providing a platform on or through which consumer fintech application providers can build and run their applications and provide an interface with consumers. Because data aggregators are few in number compared to financial services companies — a relative handful versus thousands — and because they have generally sunk the costs of connecting to financial services companies, consumer fintech application providers only have to “build” to the data aggregators’ specifications and not to hundreds or thousands of platforms run by individual financial institutions.45

Before these processes and interfaces can commence, however, a data aggregator requires access to consumers’ data housed at financial services companies. At present, there are two primary methods through which data aggregators gain access to consumer financial data: “screen-scraping” and application programming interfaces (APIs).

Screen-Scraping

When data aggregators and consumer fintech application providers lack a direct connection to run fintech applications using data housed at financial services companies, they often rely on screen-scraping. In screen-scraping, consumers provide their account login credentials — usernames and passwords — in order to use the fintech application.46 Consumers may or may not appreciate that they are providing their credentials to a third-party, and not logging in directly to their financial services company. Using these login credentials, data aggregators access consumers’ financial

---

45. By one data aggregator’s account, there are eight major aggregators of consumer-authorized data in the United States. See MX Technologies Inc., A List of Financial Data Aggregators in the United States, blog post (Mar. 5, 2018), available at: https://www.mx.com/moneysummit/a-list-of-financial-data-aggregators-in-the-united-states. The listed data aggregators were Intuit, Quovo, Plaid, Envestnet/Yodlee, Morningstar/ByAllAccounts, Fiserv/CashEdge, Finicity, and MX.

accounts, and then, either manually or through specialized software, acquire the financial account and transaction data and even process data requests or execute transactions. Equally concerning, financial services companies are not always aware when screen-scraping methods are being used to access their customers’ data.

Although screen-scraping can be an effective method of obtaining data, it is generally considered to have certain vulnerabilities and drawbacks. Many of the risks and concerns associated with data aggregation described in this report — whether for consumers, financial services companies, consumer fintech application providers, or data aggregators themselves — stem from the practice of screen-scraping.

**Application Programming Interfaces**

The second method of accessing consumer financial account and transaction data is through an API or similar form of direct feed. For purposes of this report, an API can be loosely described as a clearly specified program that links two or more systems and that enables a well-defined communication and data exchange between them in order to run applications and other software. An API is not a specific technology, but rather a technology-enabled agreement or protocol that enables a computer system or source of data to interact with or be used by other software. Unlike in the case of screen-scraping, data aggregation through an API generally means that financial services companies are knowingly participating in the sharing of data. As such, financial services companies can potentially deploy APIs that allow for the inclusion of robust security features, greater transparency and access controls for consumers, improved data accuracy, and more predictable and manageable information technology costs. APIs, however, cost money to develop, which could raise particular hurdles for smaller financial institutions with fewer information technology resources.

APIs may be designed to be open or they may be restricted to selected partners. In an open API, any third-party data aggregator or consumer fintech application provider that meets certain predetermined and published standards (e.g., security, licensing, etc.) can gain access to consumer data and build consumer-facing applications. In contrast, partnered APIs entail bilateral and exclusive agreements between financial services companies and data aggregators or consumer fintech application providers. In either case, the API method of access is generally enabled through consumer consent provided to the financial services company or at the API access point rather than through giving consumer login credentials to third-parties.

---

47. To illustrate how this works, think for example of nearly any app or website — for example, for ride-sharing services, retail stores, special events, etc. — that includes a map or the ability to provide point-to-point (or turn-by-turn) directions. These apps and websites generally do not create their own maps and navigation software. Instead, they would incorporate the maps and navigation software of an internet-based provider that specializes in aggregating mapping and navigation data. This provider makes its mapping and navigation products available for use by third-parties by establishing an API that includes instructions, tools, and other resources that enable software developers to incorporate such products into their own apps and websites.
Efforts to Improve Data Aggregation

Data aggregators, consumer fintech application providers, and financial services companies generally agree that consumers should have secure and reliable access to their financial account and transaction data, and that, in principle, consumers, if they opt-in, should be able to utilize fintech applications and other innovations that make use of their data. However, there is a lack of consensus on what secure and reliable access entails. As described by one observer, “the U.S. debate seems stuck at the yet-to-be resolved issue of migrating account aggregators from screen scraping-based to more secure and efficient API-based data-sharing methodologies.”\(^48\) As long as this impasse remains unresolved, consumers will be caught in the middle.

Consequently, data aggregators, consumer fintech application providers, and financial services companies in the United States are looking for better approaches to data aggregation. Despite the recognized advantages of using APIs as opposed to screen-scraping methods for data aggregation, current APIs have their limitations. Some data aggregators have entered into bilateral agreements to obtain data through an API, but this approach can be difficult to scale given the large number of U.S. financial services companies. In addition, data aggregators told Treasury that access through APIs was frequently and

unilaterally restricted, interrupted, or terminated by financial services companies.\textsuperscript{49} Hence, Treasury’s understanding is that a significant amount of data is still obtained through screen-scraping.

Much of the focus is on improving API methods to resolve issues such as standardizing data elements and fair and proportional allocation of liability and accountability in the event of a data breach. In some cases, participants from across the data aggregation framework are collaborating to develop robust open APIs that serve the needs of all stakeholders.\textsuperscript{50} Further, trade groups are also starting to solidify views and have developed principles with respect to data aggregation.\textsuperscript{51}

**Open Banking in the United Kingdom**

In considering regulatory approaches for data aggregation, the efforts in other countries that have created their own regulatory regimes for consumer access to financial account and transaction data can provide a useful comparison point. In August 2016, the United Kingdom’s Competition and Markets Authority (CMA) issued a report, which concluded that the market for retail banking was not sufficiently competitive and was dominated by large banks. The CMA outlined a package of remedies called Open Banking, which required the nine largest U.K. banks to adopt “open API banking standards… [and] to make data available using these standards.”\textsuperscript{52} Other banks can opt-in on a voluntary basis.

\begin{itemize}
\item \textsuperscript{49} See also Robin Sidel, *Big Banks Lock Horns with Personal-Finance Web Portals*, The Wall Street Journal (Nov. 4, 2015).
\item \textsuperscript{50} One such effort is being carried out through the OFX Consortium, the origins of which date back to 1997. The OFX specification is one of original standards for the exchange of financial information between consumers and financial services providers. In April 2016, the OFX Consortium released OFX 2.2, which introduced new standards including data tags and tokenized authentication solutions for sharing consumer financial data. See OFX Consortium, *OFX 2.2 Released with OAuth-Token based Authentication*, Business Wire (Apr. 7, 2016), available at: https://www.businesswire.com/news/home/20160407006078/en/OFX-2.2-Released-OAuth-Token-based-Authentication. A more recent effort is that of the Aggregation Services Working Group of the FS-ISAC. The Working Group, which consists of representatives from financial services companies, data aggregators, and fintech developers, recently issued the second version of its API for secure, tokenized data transfer. See Financial Services Information Sharing and Analysis Center, *Press Release – FS-ISAC Enables Safer Financial Data Sharing with API* (Feb. 13, 2018), available at: https://www.fsisac.com/article/fs-isac-enables-safer-financial-data-sharing-api.
\item \textsuperscript{51} See, e.g., Securities Industry and Financial Markets Association, *SIFMA Data Aggregation Principles* (Apr. 2018), available at: https://www.sifma.org/wp-content/uploads/2018/04/sifma-data-aggregation-principles.pdf. The SIFMA principles affirm that consumers “may use third-parties to access their financial account data” and “such access should be safe and secure.” See also Renee Hobbs, Envestnet|Yodlee, Envestnet|Yodlee, Quovo and Morningstar ByAllAccounts: Statement of Joint Principles for Ensuring Consumer Access to Financial Data, blog post (May 11, 2018), available at: https://www.yodlee.com/blog/envestnet-yodlee-quovo-and-morningstar-byallaccounts-statement-of-joint-principles-for-ensuring-consumer-access-to-financial-data. These three data aggregators proposed a “Secure Open Data Access” framework, which includes the following four components: (1) consumers must be able to access their financial account data for purposes of using any legitimate application; (2) consumers must provide affirmative consent on the basis of clear and conspicuous disclosure regarding the use of their data; (3) all entities who handle consumer account information must adhere to best practices for security standards and implement traceability/visibility; and (4) the entity responsible for a consumer’s financial loss must make the consumer whole.
\item \textsuperscript{52} See Competition and Markets Authority, *Retail Banking Market Investigation: Final Report* (Aug. 9, 2016), at 441-461, available at: https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf.
\end{itemize}
These remedies are aimed at increasing competition, including lowering costs for consumers switching between financial institutions.

The first stage of Open Banking went live in March 2017, when the covered banks were required to make certain “open data” — i.e., public information such as the location of branches and automated teller machines as well as the terms of certain banking products — widely available online. The full Open Banking standard came into effect in January 2018. The CMA established the nonprofit Open Banking Implementation Entity (OBIE) to work with banks and third-party fintech developers to help integrate with Open Banking and to test their products and services based on the data. Fintech developers enrolled in Open Banking must be regulated by the U.K. Financial Conduct Authority.53

Open Banking uses “read/write” APIs with standards and specifications defined by OBIE. To securely access and share data, the participating banks develop API “endpoints” on which fintech developers can build applications. The use of APIs permits consumers to retain full control over their account information. Consumers must give explicit consent before using any fintech applications and are redirected to their bank’s login screen to enter their login credentials. Consumers determine which information can be accessed, for how long and for what purpose, and can revoke their consent at any time. Shared data is encrypted and its usage is tracked, and only regulated persons can access it.

There are significant differences between the United States and the United Kingdom with respect to the size, nature, and diversity of the financial services sector and regulatory mandates. Given those differences, an equivalent Open Banking regime for the U.S. market is not readily applicable. Nonetheless, as Open Banking matures in the United Kingdom, U.S. financial regulators should observe developments and learn from the British experience.

Issues and Recommendations

Consumers’ ability to realize the benefits of data aggregation is limited, in part due to the lack of agreement between data aggregators and financial services companies over access to consumer financial account and transaction data. However, Treasury recognizes that significant strides have been made in recent years to bridge these disagreements. As information and data technology advances, and with sustained commitment to the principle that consumers should be able to freely access and use their financial account and transaction data, Treasury believes that improved approaches to data aggregation that will benefit consumers and financial institutions alike are surely attainable.

Consumer Access to Financial Account and Transaction Data

The only express statutory provision regarding access to a consumer’s own financial account and transaction data is Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank).54 It states that, subject to rules prescribed by the Bureau, financial services

53. As of July 2018, there were 33 regulated third-party providers enrolled in Open Banking. See https://www.openbanking.org.uk/regulated-providers/.

companies subject to the Bureau’s jurisdiction as covered persons are required to make available to a consumer, upon request, certain financial account and transaction data concerning any product or service obtained by the consumer from that financial services company. This data must be made available in an electronic form usable by the consumer.

In November 2016, the Bureau issued a request for information to better understand the benefits and risks associated with market developments that rely upon data aggregation. Subsequently, the Bureau published nonbinding principles in October 2017 expressing a vision for a “robust, safe, and workable data aggregation market,” although it noted that “few, if any, individual stakeholders” enumerated all of the consumer protection concerns presented in the principles.

As described by the Bureau, financial data subject to consumer and consumer-authorized access may include any transaction, series of transactions, or other aspect of consumer usage, the terms of any account, such as a fee schedule, realized consumer costs, such as fees or interest paid, and realized consumer benefits, such as interest earned or rewards. The principles underscore the role of companies that access consumers’ financial data, with their permission, in order to provide services that hold the promise of “improved and innovative consumer financial products and services.”

In addition to the Bureau, other groups have developed their own principles for data aggregation, including the Securities Industry and Financial Markets Association, the Consumer Financial Data Rights Coalition, and the Center for Financial Services Innovation. While Treasury is not endorsing any particular set of principles, they contain common themes on topics such as security, access, and consumer consent, which can form the basis for consensus on consumer-authorized data aggregation.

---

55. Under Section 1002(6) of Dodd-Frank [12 U.S.C. § 5481(6)], a “covered person” is defined as “any person that engages in offering or providing a consumer financial product or service,” and any affiliate of such a person, if the affiliate acts as a service provider to that person. Notwithstanding the broad definition of “covered person,” other provisions place limits on the Bureau’s jurisdiction for certain entities. See, e.g., 12 U.S.C. § 5517.

56. 12 U.S.C. § 5533(a). Section 1033, however, applies only to information that the covered person can retrieve in the ordinary course of its business with respect to that information. 12 U.S.C. § 5533(b)(4).


58. Data Aggregation RFI.


62. Id. at 1.

Direct Consumer Access Versus Consumer-Authorized Access

In response to the Bureau’s request for information, conflicting views were expressed on whether data aggregators are covered by Section 1033. Some financial services companies argued that access rights apply only to direct consumer access to their data but not to consumer-authored access through a data aggregator or a fintech application. In contrast, consumer groups, data aggregators, and consumer fintech application providers asserted that consumers are entitled to access their financial account and transaction data via fintech applications.

The definition of “consumer” in Title X of Dodd-Frank includes not only an individual, but “an agent, trustee, or representative acting on behalf of an individual.” This definition is best interpreted to cover circumstances in which consumers affirmatively authorize, with adequate disclosure, third parties such as data aggregators and consumer fintech application providers to access their financial account and transaction data from financial services companies. Otherwise, narrowly interpreting Section 1033 as applying only to direct consumer access would do little to advance consumer interests by eliminating many of the benefits they derive from data aggregation and the innovations that flow through from fintech applications.

Recommendation

Treasury recommends that the Bureau affirm that for purposes of Section 1033, third parties properly authorized by consumers, including data aggregators and consumer fintech application providers, fall within the definition of “consumer” under Section 1002(4) of Dodd-Frank for the purpose of obtaining access to financial account and transaction data.

Entities Covered by Data Access Requirements

Section 1033 applies only to “covered persons” under Dodd-Frank, which includes a subset of financial services companies. Furthermore, the Bureau’s jurisdiction is subject to limitations for some financial services companies subject to regulation by other federal or state regulators, including: persons regulated by a state securities commission, to the extent that such persons act in a regulated capacity, or by the Securities and Exchange Commission (SEC); persons regulated by the Department of Labor (DOL) that are offering 401(k) plans or employee benefit plans; and persons regulated by state insurance regulators that are offering insurance products.

Financial services companies primarily regulated by regulators other than the Bureau play important roles in the retirement savings plans of many Americans. While one approach is to expand the scope of Section 1033 to expressly include these companies, Treasury does not believe that step is necessary. Treasury has not identified evidence of market failure with respect to electronic access to data held by financial services companies not subject to Section 1033. In outreach meetings, financial planners and investment advisers advised Treasury that many broker-dealers and their

64. See Bureau Stakeholder Insights, at 4-5.
custodians have been providing financial account and transaction data in a usable electronic format for a long time.\textsuperscript{69} Such data, for instance, is needed to produce performance reports and monitor asset allocations. However, in outreach meetings with Treasury, financial planners and investment advisers indicated that the current data feeds from broker-dealers were generally reliable.

\textit{Recommendations}

Treasury recommends that regulators such as the SEC, Financial Industry Regulatory Authority, DOL, and state insurance regulators recognize the benefits of consumer access to financial account and transaction data in electronic form and consider what measures, if any, may be needed to facilitate such access for entities under their jurisdiction.\textsuperscript{70} However, Treasury recommends against further legislative action to expand the scope of Section 1033 at this time.

\textit{Consumer Disclosure, Consent, and Termination}

The products and services discussed in this section require consumer authorization as the legal basis for accessing the financial account and transaction data. But consumers cannot make informed choices without transparent, comprehensible, and readily accessible disclosure. Without adequate disclosure, consumers will be unable to clearly understand and weigh the risks and benefits of using fintech applications and letting third-parties access and use their personal and financial data.

Some fintech applications and data aggregators make hard-to-follow disclosures as to which financial account and transaction data will be obtained and how that data will be utilized and stored. In other cases, the disclosures, terms, and conditions may be hard to find or they may be written in dense legalistic language that induces the consumer to head straight to the “accept” button, or else forgo usage of the service.

Disclosures may not be fully effective to the extent that consumers remain unaware of the data relationships underlying the services they are using. For example, for fintech applications that rely on a data aggregator to obtain or process the consumer’s financial account and transaction data, the role of the data aggregator may be opaque to the consumer. As consumers increasingly access fintech applications through their mobile devices, the likelihood that they will read and understand long and meticulous disclosures diminishes.

While complex disclosures designed to protect service providers rather than inform consumers are a problem, consumers should make every effort to read disclosures so that they understand their rights and obligations. It is not enough to assert that measures are needed to ensure that consumers understand what they are agreeing to when they use third-party applications. As one observer wrote, “[d]isclosures written in plain language might increase consumer awareness, but

\begin{itemize}
\item \textsuperscript{69} A number of the financial planners and investment advisers indicated that it was more difficult to obtain data from 401(k) plans, particularly the smaller ones, than from traditional broker-dealers.
\item \textsuperscript{70} See, e.g., General Instruction C.(3).g of Form N-1A under the Securities Act and Investment Company Act (requiring electronic machine-readable information about mutual funds).
\end{itemize}
that only works if consumers actually read the ‘Terms and Conditions’ before downloading the latest financial app.”

While consumers have to some extent become conditioned to opt for convenience over security, they nevertheless continue to look to their primary financial institutions for protection of their personal and financial data. This raises issues of importance for these financial institutions, including how to verify that their customers have in fact authorized a third party to access their account or initiate a transaction. Further, data aggregators may obtain significantly more consumer financial data than necessary to provide the service that the customer requested, often unknown to the customer. The implications of these features give rise to a potentially wide cascade of issues regarding downstream use of the data, including broader issues related to data privacy that are beyond the scope of this report.

Finally, consumers should have an easy way to revoke their consent to data aggregator access to their financial account and transaction data. Otherwise, data aggregators may retain and continue to use the data and, in some circumstances, may even be able to acquire additional data. It is important that requirements regarding customer authorization be improved to allow customers to exercise control over the scope and duration of data being obtained, how the data is used, and to whom it may be provided.

**Recommendations**

Treasury recommends that the Bureau work with the private sector to develop best practices on disclosures and terms and conditions regarding consumers’ use of products and services powered by consumer financial account and transaction data provided by data aggregators and financial services companies. The goal should be to provide disclosures and terms and conditions that are written in plain language, readily accessible, readable through the preferred device used by consumers to access services, and presented in a reasonably simple and intuitive format so that consumers can give informed and affirmative consent regarding to whom they are granting access, what data is being accessed and shared, and for what purposes. If necessary, the Bureau should consider issuing principles-based disclosure rules pursuant to its authority under Section 1032 of Dodd-Frank.

Treasury also believes that consumers should have the ability to revoke their prior authorization that permits data aggregators and fintech applications to access their financial account and transaction data. Data aggregators and fintech applications should provide adequate means for consumers to easily and effectively revoke their consent to access to their financial account and transaction data.

---


to readily revoke the prior authorization. If necessary, banking regulators and the SEC should consider issuing rules that require financial services companies to comply with a consumer request to limit, suspend, or terminate access to the consumer’s financial account and transaction data by data aggregators and fintech applications.

Moving Away from Screen-Scraping to More Secure Access Methods

The practice of using login credentials for screen-scraping poses significant security risks, which have been recognized for nearly two decades. Screen-scraping increases cybersecurity and fraud risks as consumers provide their login credentials to access fintech applications. During outreach meetings with Treasury, there was universal agreement among financial services companies, data aggregators, consumer fintech application providers, consumer advocates, and regulators that the sharing of login credentials constitutes a highly risky practice.

APIs are a potentially more secure method of accessing financial account and transaction data than screen-scraping. A number of foreign jurisdictions have opted to promote access through APIs, in part due to security concerns. The United Kingdom, through its open banking initiative, has specified regulatory standards for data sharing through APIs. The European Union has adopted the Revised Payment Service Directive (PSD2), which requires banks to grant licensed third-party payment service providers access to bank infrastructure and account data. PSD2 also contemplates the standardization of APIs. Singapore has encouraged the use of bank APIs but has not made it a regulatory mandate.

Data aggregators and consumer fintech application providers have expressed reservations with an API approach. They claim, for example, that their efforts to work with financial services companies to do away with screen-scraping have for the most part been met with resistance, and that financial services companies have largely refused to enable direct access to their data or to set up open APIs. There are concerns that without some sort of industry standard or regulatory guidance, API access could be restricted to certain types of data dictated by the financial services company, as opposed to the consumer, susceptible to unexpected interruptions and terminations, and subject to unreasonable and disproportionate liability.

Recommendations

Treasury sees a need to remove legal and regulatory uncertainties currently holding back financial services companies and data aggregators from establishing data sharing agreements that effectively

74. See footnote 46.
move firms away from screen-scraping to more secure and efficient methods of data access. Treasury believes that the U.S. market would be best served by a solution developed by the private sector, with appropriate involvement of federal and state financial regulators.

A potential solution should address data sharing, security, and liability. Any solution should explore efforts to mitigate implementation costs for community banks and smaller financial services companies with more limited resources to invest in technology.

**Liability for Unauthorized Access**

Screen-scraping also appears tied to the issue of liability. Financial services companies have expressed concerns that they may bear the burden of any losses arising from a breach at the data aggregator or a downstream fintech application. Even if the consumer’s losses are not limited by Regulation E,79 such as when a consumer authorized a person other than the consumer to initiate an electronic funds transfer by providing login credentials to such third party, the consumer may nonetheless expect the bank or other financial institution to make him or her whole for any losses.

Providing login credentials to a data aggregator creates opportunities for bad actors to illicitly obtain such highly sensitive credentials and allow assets to be transferred out of the account. Screen-scraping also can allow a data aggregator to obtain significantly more data than needed by the underlying fintech application, including sensitive personally identifiable information, which could be subsequently stolen.80 Moving away from screen-scraping can facilitate resolution of the liability issue by eliminating the need for login credentials, reducing the amount and sensitivity of unnecessary data being acquired by data aggregators and decreasing the possibility of an unauthorized transaction.

Some data aggregators have entered into agreements with financial services companies to access the financial account and transaction data through an API but conditioned on contractual liability and indemnification of the financial services company. Other data aggregators have been unable or unwilling to reach agreement on such terms. In such circumstances, data aggregators usually continue to obtain data through screen-scraping.

As the U.S. Government Accountability Office (GAO) has observed, the issue of financial responsibility for consumer losses and access to consumer financial transaction data has been discussed at meetings of federal banking regulators and the Bureau under the auspices of the Federal Financial Institutions Examination Council (FFIEC). However, these discussions have not resulted in any specific policy outcomes to guide market participants.81 Without resolution of liability and other

---

79. 12 C.F.R. Part 205. Regulation E implements the Electronic Fund Transfer Act, which establishes a framework of the rights, liabilities, and responsibilities of participants in the electronic fund and remittance transfer systems.

80. The sensitivity of consumer financial transaction data can vary. For example, data indicating that a bank account is a checking account may be less sensitive than the associated ABA routing and account numbers. If a fintech application only needs to know the account type, then it would be unnecessary to obtain the more sensitive ABA routing and account numbers.

issues, “consumers could have to choose between facing potential losses or not using what they may find to be an otherwise valuable financial service, and fintech firms providing useful services to consumers will face barriers to providing their offerings more broadly.”

Recommendations
Treasury recommends that any potential solution discussed in the prior recommendation also address resolution of liability for data access. If necessary, Congress and financial regulators should evaluate whether federal standards are appropriate to address these issues.

Standardization of Data Elements
There are other areas in which collaboration among market participants could improve consumers’ ability to use their data. Collaborative attempts have been made among financial services companies, data aggregators, and consumer fintech application providers to create standardized data elements, including efforts by Open Financial Exchange (OFX) and Financial Services Information Sharing and Analysis Center (FS-ISAC). However, these efforts have not achieved full consensus to date. A standardized set of data elements and formats would help to foster innovation in services and products that use financial account and transaction data, because it may be more efficient to develop a single agreed-upon taxonomy. Data elements would need to be developed for a broad range of products and services related to banking, investments, retirement, loans, insurance, and taxes. Standardization could improve the market efficiency for financial products and services by making it easier to engage in comparative analysis.

Data currently obtained by aggregators from separate financial services companies can be incompatible and must be cleaned and standardized before it can be used. Financial services companies often use “disparate and customized formats to send and share information, employing different nomenclature for [otherwise] common terms.”

Recommendations
Treasury recommends that any potential solution discussed in the prior recommendation address the standardization of data elements as part of improving consumers’ access to their data. Any solution should draw upon existing efforts that have made progress on this issue to date. If necessary, Congress and financial regulators should evaluate whether federal standards are appropriate to address these issues.

Clarifying When Data Aggregators Are Subject to Third-Party Guidance
Some banks have raised concerns over whether third-party guidance may apply if a bank enters into an API agreement with a data aggregator that establishes terms of access, because the bank has

82. Id. at 57.
83. See footnote 50.
entered into a contract. Third party guidance clearly applies when a bank itself is providing data aggregation as a service to its customers and has hired a data aggregator to collect the data with its customer’s authorization because the data aggregator becomes a service provider to the bank. But when the data aggregator has entered into an API agreement with the bank where it is not providing a service to the bank, it is unclear whether third party guidance may still apply.

Data aggregators would not consider themselves service providers to banks when, for example, they rely on screen-scraping to access financial account and transaction data that has been authorized by a consumer. However, if data aggregators were to instead enter into an API agreement with a bank, it may become subject to third-party guidance because of the contractual relationship, which can increase compliance costs.

This regulatory uncertainty over the application of third-party guidance may, therefore, be inadvertently discouraging more API agreements between banks and data aggregators.

Recommendation
Treasury recommends that the banking regulators remove ambiguity stemming from the third-party guidance that discourages banks from moving to more secure methods of data access such as APIs. Further discussion of bank regulatory oversight of third-party relationships is addressed in the following chapter on Aligning the Regulatory Framework to Promote Innovation.

Current Regulation of Data Aggregators
The greater the amount of consumer financial account and transaction data that is retained by data aggregators, the greater is the possible harm to consumers that could result from a data breach. Although data aggregators do not have a specific regulatory scheme similar to banks or other depository institutions, they are currently subject to regulation under the federal consumer protection laws administered by the FTC as well as state consumer protection laws. Some financial services companies have suggested that the absence of the same level of regulatory oversight of data aggregators and downstream consumer fintech application providers raises significant risks for consumers. In particular, they have argued that the security practices of data aggregators are not comparable to the standards applied at banks and the security practices of consumer fintech application providers are even weaker.

85. Banking regulators have issued guidance for assessing and managing risks in third-party relationships. The guidance views a third-party relationship as “any business arrangement between a bank and another entity, by contract or otherwise.”

86. Treasury is aware that some data aggregators have entered into agreements with banks, sometimes on an informal basis, while engaging in screen-scraping. For example, a data aggregator may agree to pull the data during the night in order to minimize disruption to the bank’s computer systems.

87. In outreach meetings with Treasury, data aggregators have asserted that they mitigate data breach risk by only retaining aggregated and anonymized data that is not associated with any personally identifiable information of the consumer.

88. To the extent that a data aggregator or consumer fintech application provider is providing services to a bank, the services provided are subject to the third-party oversight framework imposed by banking regulators under the Bank Services Company Act.

Data aggregators and consumer fintech application providers are subject to the Gramm-Leach-Bliley Act (GLBA), which is a federal law specifying the ways that financial institutions, including some nonbank financial institutions, protect the security and confidentiality of nonpublic personal information of individuals. The provisions in GLBA govern how financial institutions, as defined under the statute, implement administrative, technical, and physical safeguards to insure the security and confidentiality of customer records, protect against any anticipated threats or hazards, and protect against unauthorized access. Financial institutions must explain their policies to their customers that are designed to safeguard sensitive data. These provisions of GLBA are enforced by the FTC, the federal banking agencies, the SEC, and the Commodity Futures Trading Commission (CFTC). To be compliant with GLBA, financial institutions must apply specific protections to customers’ private data in accordance with the institution’s data security plan.

To implement GLBA, the FTC set forth the primary information security provisions in its Safeguards Rule. The FTC’s Safeguards Rule requires financial institutions to assess and develop a documented security plan that describes the company’s program to protect customer information, including the following areas particularly important to information security: employee management and training, information systems, and detecting and managing system failures. The intent of the GLBA information security requirements in the Safeguards Rule is to protect consumers and reduce reputational damage caused by unauthorized sharing or loss of private customer data. The FTC has indicated that data aggregators and consumer fintech application providers significantly engaged in financial services and products are financial institutions under GLBA and therefore subject to the Safeguards Rule.

In addition, there are efforts underway to regulate consumer-authorized data aggregation, including potential legislation, at the state level. However, Treasury believes that state-by-state regulation, which would be more cumbersome and costly to comply with as compared with regulation by a single federal regulator, would not be workable given the complexity of data issues at hand.

Recommendation
Moving away from screen-scraping and eliminating the sharing of login credentials will address the most significant concerns raised about the need to increase regulation of data aggregators and

---

92. Financial institutions include companies that offer consumer financial products or services like loans, financial or investment advice, or insurance.
94. Id. § 6803(c)(3).
96. 16 C.F.R. §§ 314.3 and 314.4.
consumer fintech application providers. While data security concerns will remain an important issue, the Safeguards Rule appropriately addresses such concerns.98

To the extent that any additional regulation of data aggregation is necessary, Treasury recommends that it occur at the federal level by regulators that have significant experience in data security and privacy, and that will have, through legislation if necessary, broad jurisdiction to ensure equivalent treatment in the nonfinancial sector.

Data Security and Breach Notification

Data Security Standards

The data security provisions of GLBA are enforced by the federal banking agencies for depository institutions,99 the SEC and the CFTC for entities under their jurisdiction, and the FTC for all other financial institutions.100 With the exception of the FTC, these federal agencies are authorized to routinely supervise and examine for compliance with these provisions of GLBA and their implementing regulations. These agencies all maintain authority to implement regulations for GLBA.

Data security standards are significantly different between nonfinancial companies, such as retailers and manufacturers, and financial institutions. Vast amounts of consumer payment credentials and financial data are routinely stored on a nonfinancial company’s internal or third-party systems, used for marketing purposes, or simply used to complete transactions instantly. Yet, nonfinancial companies are not subject to comprehensive federal data security standards under GLBA and are not subject to routine examination for compliance with data security standards. The only heightened obligation to protect data comes from the exercise of the FTC’s authority under Section 5 of the Federal Trade Commission Act101 to bring enforcement actions against nonfinancial companies for unfair or deceptive practices. The FTC has exercised this authority more than 60 times since 2002; however, this authority is limited to enforcement action and does not give the FTC supervision and examination rights over these nonfinancial companies.102

In addition to federal standards, nonfinancial companies and financial institutions subject to the FTC’s jurisdiction under GLBA must comply with applicable state laws that impose heightened or specific data security standards. To date, only 13 states have imposed data security standards for protection of consumer financial data, which have different requirements. For instance, Florida requires a business to take “reasonable measures” to protect and secure personal information data

---

98. In addition to the information security requirements, GLBA also contains privacy requirements as to how financial institutions collect, use, and maintain nonpublic personal information and under what circumstances that information can be shared. These provisions are applicable to financial institutions under the Bureau’s Regulation P [12 C.F.R. Part 1016].


100. Insurance data security was examined in the Asset Management and Insurance Report.


that is stored in “electronic form,” but Utah does not differentiate between personal information stored electronically or on paper.\textsuperscript{103}

Over the last several years, many nonfinancial companies have been subject to significant data breaches of consumer financial data. For example, in 2013, Target announced that payment card information of 41 million consumers was compromised.\textsuperscript{104} In 2014, Home Depot announced that the payment card information of more than 50 million customers was stolen in a data breach.\textsuperscript{105} More recently, the retailer Hudson’s Bay Co. advised roughly 5 million customers of its subsidiary stores Lord & Taylor and Saks Fifth Avenue that their payment credentials had been compromised.\textsuperscript{106} Data breaches are not unique to nonfinancial companies and have affected financial institutions as well.\textsuperscript{107}

\textbf{Data Breach Notification}

The United States does not have a national law establishing uniform national standards for notifying consumers of data breaches, or for providing them a clear and straightforward mechanism for resolving disputes.\textsuperscript{108} In the absence of uniform national standards, states have been aggressive in developing their own data breach notification laws. Each state law may apply to any company located in that state or that does business with residents of that state. In practice, this means that in the event of a data breach companies could be subject to the data breach notification laws of 50 states as well as of the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands.\textsuperscript{109} State laws for data breach notification often include specific provisions regarding the number of affected individuals that will trigger notification requirements, the timing of notification, and form of notification, among other requirements. Unsurprisingly, state data breach notification laws are far from uniform. Indeed, they vary in a number of significant ways, including with respect to the most fundamental aspect, namely the scope of data covered under the definition of personal

\begin{itemize}
\item \textsuperscript{103} Compare Fla. Stat. § 501.171(2) with Utah Code § 13-44-201.
\item \textsuperscript{107} For example, JPMorgan Chase was subject to a data breach in 2014 and Equifax suffered a data breach in 2017.
\item \textsuperscript{108} Federal banking regulators have adopted guidance for depository institutions in the event of unauthorized access to customer information. See Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice [70 Fed. Reg. 15736 (Mar. 29, 2005)].
\end{itemize}
information.\textsuperscript{110} Other inconsistencies among states’ breach notification laws can make compliance difficult for firms and entail disparate treatment for consumers. The lack of uniformity and efficiency affects both nonfinancial companies and financial institutions.

\textit{Recommendation}

Congress has considered establishing a federal data security standard and breach notification standard on several occasions. For example, during the 114\textsuperscript{th} Congress, two separate bills, sharing many common principles, successfully passed their respective committees.\textsuperscript{111} During this Congress, legislation has again been considered to establish these federal standards.

Treasury recommends that Congress enact a federal data security and breach notification law to protect consumer financial data and notify consumers of a breach in a timely manner. Such a law should be based on the following principles:

- Protect consumer financial data
- Ensure technology-neutral and scalable standards based on the size of an entity and type of activity in which the entity engages
- Recognize existing federal data security requirements for financial institutions
- Employ uniform national standards that preempt state laws

\textbf{Digital Legal Identity}

Digital identity products and services hold promise for improving the trustworthiness, security, privacy, and convenience of identifying individuals and entities, thereby strengthening the processes critical to the movement of funds, goods, and data as the global economy races deeper into the digital age. Digital identity systems also have the potential to generate cost savings and efficiencies for financial services firms. For instance, trustworthy digital identity systems could improve customer identification and verification for onboarding and authorizing account access, general risk management, and antifraud measures.

\textbf{Legal Identity}

Legal identity is distinct from broader concepts of personal and social identity. Legal identity is the specification of a unique natural or legal person that (1) is based on certain pre-specified characteristics or attributes of the person that are intended to establish the person’s uniqueness, (2) is recognized by the state under national law, and (3) ascribes legal rights and duties to that person. Proof of legal identity is required to open a bank, brokerage, or other account at a regulated financial institution. Digital legal identity uses electronic means to unambiguously assert and authenticate a real person’s unique legal identity.

\textsuperscript{110} For example, Maryland specifically includes biometric data of an individual such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristics, while other states do not. Compare Md. Code Com. Law § 14-3501(d) [as amended by House Bill 974 (May 4, 2017)] with Nevada Rev. Stat. § 603A.040.

Portability

Digital identity systems potentially allow legal identity to be portable. Portable legal identity means the individual’s verified identity credentials can be used to establish legal identity for new customer relationships at unrelated financial institutions or government entities, without each financial institution’s having to obtain and verify personally identifiable information (PII) to meet regulatory requirements. Portability requires developing interoperable digital identification products, systems, and processes. While not permitted in the private sector under current regulations, trustworthy portable third-party digital identity services could potentially save relying parties time and resources in identifying, verifying, and managing customer identities, including for account opening and access. Portability could also potentially save customers the inconvenience of having to prove and authenticate identity for each unrelated financial institution or government service, and reduce the risk of identity-theft stemming from the repeated exposure of PII.

Components of a Digital Identity System

Digital identity systems may rely on various types of technology and use digital technology in several ways, but generally involve two essential components: (1) identity proofing, enrollment, and credentialing; and (2) authentication. They may also involve a third component, federation, which is optional, but allows identity to be portable. Identity proofing and enrollment may be digital or documentary, remote, or in-person. Credentialing, authentication, and federation are always digital. Different identity service providers can provide some or all of the components of a digital identity system.

Identity proofing establishes that a subject is who they claim to be. It involves obtaining and verifying that attribute evidence is genuine and accurate, and issuing a digital credential to bind the verified identity to a real-life person. Identity proofing depends on official government registration and documentation/certification, or at least on governmentally recognized registration and certification, for verification.

Authentication establishes that the person asserting identity is who he or she claims to be. It involves confirming, through a secure digital authentication protocol, that the individual asserting identity is in control of the technologies and credentials that bind the validated identity to a real person. Successful authentication provides reasonable, risk-based assurances to the relying party that the subject asserting identity today is the same person who previously

112. For example, digital identity systems may use electronic databases to obtain and confirm attribute information and/or store and manage records; digital credentials to authenticate identity for accessing mobile, online, and offline financial activities; and digital biometrics to provide attributes to identify and/or a credential to authenticate individuals.

asserted identity and accessed a financial service, and is in fact a given identified customer. Trustworthy authentication is key for combating account-access identity fraud.114

Federation involves the use of federated identity architecture and assertions to convey the results of an authentication process and, if requested or required, attribute information to relying parties across a set of networked systems.115

The National Institutes of Standards and Technology (NIST) of the U.S. Department of Commerce has recently established risk-based technical standards for each of the component processes of a digital identity system (enrollment and identity proofing; authentication and lifecycle management; and federation),116 which are mandatory for the federal government, but only voluntary for the private sector.

Public-Private Roles

Both the government and the private sector have important roles in establishing a trustworthy U.S. digital identity ecosystem. In the United States, the private sector is generally relied upon to develop innovative identity products, services, and business models, while the federal government is ultimately responsible for establishing the minimum substantive requirements for proving legal identity, including core attributes and acceptable attribute evidence. Federal and state government authorities also provide the official government registration and the related official root identity evidence (e.g., birth certificates, passports) on which legal identity currently depends.

Public and private sector stakeholders need to work together to develop trustworthy digital legal identity products and services for use in the financial sector and elsewhere. To facilitate this objective, stakeholders should address a number of issues, including:

- How to leverage the NIST guidelines to establish flexible, risk-based standards for digital customer identification and verification, keyed to the risk levels associated with specific customers and/or types of financial products and services
- How to ensure the trustworthiness, privacy, and cybersecurity of identity service providers, such as government or industry certification and supervision
- Business models and liability allocation appropriate for establishing portable legal identity
- Ways the public and private sectors can effectively work together to reduce regulatory burden and catalyze the market for trustworthy digital identity products and services


116. See NIST 800-63A, 800-63B, and NIST 800-63-3. The NIST digital identity guidelines set requirements for three different levels of trustworthiness, called levels of assurance (LOAs), for each of these component processes, based on the LOA’s degree of trustworthiness.
Treasury recommends that financial regulators work with Treasury to enhance public-private partnerships to identify ways government can eliminate unintended or unnecessary regulatory and other barriers and facilitate the adoption of trustworthy digital legal identity products and services in the financial services sector. This would include engaging the private sector to help the financial regulators adopt regulation in the legal identity space that is flexible, risk-, principles-, and performance-based, future-proofed, and technology-neutral. Treasury also recognizes that the development of digital legal identity products and services in the financial services sector should be implemented in a manner that is compatible with solutions developed across other sectors of the U.S. economy and government.

Treasury also supports the efforts of the Office of Management and Budget to fully implement the long-delayed U.S. government federated digital identity system. Treasury recommends policies that would restore a public-private partnership model to create an interoperable digital identity infrastructure and identity solutions that comply with NIST guidelines and would reinvigorate the role of U.S. government-certified private sector identity providers, promoting consumer choice and supporting a competitive digital identity marketplace. Treasury also seeks to leverage the U.S. government federated identity system — in particular, its certification and auditing regime for digital identity providers — to permit financial institutions to use digital identity services provided by certified providers to conduct customer identification and verification for onboarding.

Finally, Treasury encourages public and private stakeholders to explore ways to leverage the REAL ID Act\textsuperscript{117} driver's license regime — particularly, robust state REAL ID license identity-proofing processes — to provide trustworthy digital identity products and services for the financial sector.

The Potential of Scale

The ongoing digital transformation of the financial services system is being driven not only by developments in computing power, the expanding ubiquity and interconnection of computers and mobile devices, and the exponential growth in digitized financial data, but also by technologies that can benefit from advances in data and computing capacity at greater scale and with greater efficiency. Scalable technologies such as cloud computing enable financial services companies to store and process vast amounts of data and to quickly add new computing capacity to meet changing needs. At the same time, advances in big data analytics, machine learning, and artificial intelligence are expanding the frontiers of financial services firms’ abilities to glean new and valuable business insights from vast datasets.

Cloud Technology and Financial Services

Cloud technology is enabling organizations across the economy to more rapidly innovate by reducing barriers to entry to acquire high quality computing resources. Cloud computing, more specifically, enables more convenient, on-demand access to computing resources (e.g., networks, servers,