For release on delivery
1:15 p.m. EDT (12:15 p.m. CDT)
April 28, 2017

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 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]

---

[1] David Pierce, "Even Steve Jobs Didn't Predict the iPhone Decade," Wired, January 9, 2017, www.wired.com/2017/01/apple-iphone-10th-anniversary/.

[2] Mary Meeker, Internet Trends 2016—Code Conference, June 1, 2016, www.slideshare.net/kleinerperkins/2016-internet-trends-report/109-KPCB_INTERNET_TRENDS_2016_PAGE109Average (slide 109); and Ben Bajarin, "Apple's Penchant for Consumer Security," TechOpinions, April 18, 2016, https://techpinions.com/apples-penchant-for-consumer-security/45122.

[3] See Riley v. California, 134 S. Ct.2473, 2484 (2014), www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.

[4] For instance, the average American now spends nearly an hour a day on Facebook's mobile platforms alone. See, e.g., James B. Stewart, "Facebook Has 50 Minutes of Your Time Each Day. It Wants More," New York Times, May 5, 2016, www.nytimes.com/2016/05/06/business/facebook-bends-the-rules-of-audience-engagement-to-its-advantage.html. This count includes Facebook, Messenger, and Instagram, but not WhatsApp.

[5] See, e.g., Jordan Golson, "Apple's App Store Now Has over 2 Million Apps," The Verge, June 13, 2016, www.theverge.com/2016/6/13/11922926/apple-apps-2-million-wwdc-2016.

[6] See, e.g., Sarah Perez, "Apple's App Store hits 2M apps, 130B downloads, $50B paid to developers," TechCrunch June 13, 2016, https://techcrunch.com/2016/06/13/apples-app-store-hits-2m-apps-130b-downloads-50b-paid-to-developers/. On August 3, 2016, Apple CEO Tim Cook noted on Twitter that the $50 billion figure had been

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

---

surpassed. Tim Cook, Twitter, Aug. 3, 2016, https://twitter.com/tim_cook/status/760929629226041345 (last accessed April 4, 2017).

that are flooding into this sector.[7] 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.[8] 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 system.[9] 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

---

[7] In 2015 KPMG estimated that global investment in fintech had risen six-fold in the prior three years. KPMG, "'Fintech 100'--Announcing the World's Leading Fintech Innovators for 2015," December 2015, https://home.kpmg.com/xx/en/home/media/press-releases/2015/12/fintech-announcing-the-world-leading.html. In the lending sector alone, Goldman Sachs estimates that $11 billion of annual profit is at risk of leaving the banking system. Ryan M. Nash and Eric Beardsley, The Future of Finance Part 1: The Rise of the New Shadow Bank (New York: Goldman Sachs, March 3, 2015), www.betandbetter.com/photos_forum/1425585417.pdf. McKinsey & Company estimates that there are over 2,000 fintech startups, which have attracted nearly $23 billion of venture capital and growth equity over the past five years. See Miklos Dietz, Somesh Khanna, Tunde Olanrewaju, and Kausik Rajgopal, "Cutting Through the Noise around Financial Technology," McKinsey & Company, February, 2016, www.mckinsey.com/industries/financial-services/our-insights/cutting-through-the-noise-around-financial-technology.

[8] See Miklos Dietz, Somesh Khanna, Tunde Olanrewaju, and Kausik Rajgopal, "Cutting Through the Noise around Financial Technology," McKinsey & Company, February, 2016, www.mckinsey.com/industries/financial-services/our-insights/cutting-through-the-noise-around-financial-technology.

[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.

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.[10] 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 uneasily alongside the requisites of openness, connectivity, and data access that enable today's app ecosystem.[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

---

[10] See, e.g., Bryan Yurcan, "Is a Turning Point Near for Core Systems?" American Banker, April 20, 2016, www.americanbanker.com/news/is-a-turning-point-near-for-core-systems (noting survey findings that 70 percent of U.S. bankers do not feel that their current processes can quickly adapt to market changes, and that 53 percent of survey respondents identified new products/innovation as the top benefit of investing in new core systems); Tom Groenfeldt, "Updating, Replacing, Surrounding Core Banking System," Forbes, July 21, 2015, www.forbes.com/sites/tomgroenfeldt/2015/07/21/updating-replacing-surrounding-core-banking-system/#2e019cd61282.

[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," https://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf, December 5, 2013.

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.[12] However, it did not stand in the way of Pokémon Go subsequently being downloaded a half billion times.[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 providers, extending even to operations and internal controls, among other requirements.[14] 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.

---

[12] See, e.g., Olivia Solon, "Have You Given Pokémon Go Full Access to Everything in Your Google Account?" Guardian, July 12, 2016, 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.")

[13] See, e.g., Ben Gilbert, "Pokémon Go Has Been Downloaded over 500 Million Times," Business Insider, September 7, 2016, www.businessinsider.com/pokemon-go-500-million-downloads-2016-9.

[14] 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.

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.

A number of large banks have developed or are in the process of developing interfaces to allow outside developers access to their platforms under controlled conditions. Similar to Apple opening the APIs of its phones and operating systems, these financial companies are working to provide APIs to outside developers, who can then build new products on the banks' platforms.[15] It is worth highlighting that platform APIs generally vary in their degree of openness, even in the 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

[15] See, e.g., Citigroup, "Citi Launches Global API Developer Hub to Enable Open Banking," press release, November 10, 2016, www.citigroup.com/citi/news/2016/161110b.htm; BBVA, "BBVA API Market, the Platform for Financial Innovators," press release, May 4, 2016, www.bbva.com/en/news/general/bbva-api-market-platform-financial-innovators/; Mark Boyd, "Capital One Launches First True Open Banking Platform in U.S., Programmable Web," March 11, 2016, www.programmableweb.com/news/capital-one-launches-first-true-open-banking-platform-us/2016/03/11; Penny Crosman, "Fintech Glasnost: Why U.S. Banks are Opening Up APIs to Outsiders," American Banker, July 8, 2015, www.americanbanker.com/news/fintech-glasnost-why-us-banks-are-opening-up-apis-to-outsiders; see also Pymnts.com, "Mastercard Turns Up the API Volume," September 28, 2016, www.pymnts.com/mastercard/2016/mastercard-turns-up-the-api-volume/; Visa Inc., "Visa Opens its Global Network with Launch of Visa Developer," press release, February 4, 2016, www.businesswire.com/news/home/20160204006175/en/Visa-Opens-Global-Network-Launch-Visa-Developer. Indeed, over five years ago, French bank Credit Agricole used open APIs to launch an app store of its own. The bank even connects its customers with developers, using message boards so that customers (or even other banks) can post ideas for developers to build. See, e.g., Karen Epper Hoffman, "Open API for Bank Apps: Can Credit Agricole's Model Work Here?" American Banker, July 29, 2013; CA Store, www.creditagricolestore.fr/catalogue-d-applications.html (last visited April 4, 2017) (as of April 2017, the site features 47 apps and 62 ideas); Mary Wisniewski, "Will Banks Become App Stores? This De Novo Wants To," American Banker, February 18, 2016, www.americanbanker.com/news/will-banks-become-app-stores-this-de-novo-wants-to.

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 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.[17] Data aggregators organize the data they collect

---

[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-2fc0c26b3c60.html?ft_site=falcon&desktop=true#axzz4G0M5oyu8.

[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.

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.[18]

Some banks have opted for a more "closed" approach to fintech developers by entering into individual agreements with specific technology providers or data aggregators.[19] These 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

---

[18] See, e.g., 12 USC §§ 1861-67; Division of Banking Supervision and Regulation and Division of Consumer and Community Affairs Federal Reserve System, Guidance on Managing Outsourcing Risk, www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf, December 5, 2013; Steven Boms, "Yodlee Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records," Docket No. CFPB 2016-0048, February 21, 2017, www.regulations.gov/document?D=CFPB-2016-0048-0033. ("Yodlee . . . has complied with hundreds of bank audits and with examinations by the Office of the Comptroller of the Currency throughout its history.")

[19] See, e.g., "Finicity and Wells Fargo Ink Data Exchange Deal," press release, April 4, 2017, www.finicity.com/press-release-finicity-wells-fargo-ink-data-exchange-deal/; Wells Fargo & Co., "Intuit Signs New Data-Exchange Agreement with Wells Fargo," press release, February 3, 2017, www.wellsfargo.com/about/press/2017/intuit-agreement_0203/; Intuit, "Chase, Intuit to Give Customers Greater Control of Their Information," press release, January 25, 2017, www.intuit.com/company/press-room/press-releases/2017/Chase-Intuit-to-Give-Customers-Greater-Control-of-Their-Information/; Wells Fargo & Co., "Wells Fargo, Xero Agree on New Data-Exchange Method," press release, June 7, 2016, www.wellsfargo.com/about/press/2016/new-dataexchange-method_0607/; Silicon Valley Bank, "Xero and Silicon Valley Bank Partner to Offer Innovative Companies Next-Generation Financial Management," press release, July 16, 2014, www.svb.com/News/Company-News/Xero-and-Silicon-Valley-Bank-Partner-to-Offer-Innovative-Companies-Next-Generation-Financial-Management/.

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 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

---

[20] See, e.g., Center for Financial Services Innovation, "Consumer Data Sharing Principles: A Brief on the Framework for Industry-Wide Collaboration," October 20, 2016, http://cfsinnovation.org/research/consumer-data-sharing-principles-a-brief-on-the-framework-for-industry-wide-collaboration/. Indeed, many of the developers that make use of the bank data obtained by data aggregators are actually *other* banks. Steven Boms, "Yodlee Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records," Docket No. CFPB 2016-0048, February 21, 2017, www.regulations.gov/document?D=CFPB-2016-0048-0033. ("Over our almost two-decade history, Yodlee has built a client base that includes 12 of the 20 largest banks in the United States and the largest banks in more than 20 countries.")

[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 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.")

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.

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.

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]

---

[22] According to one banking trade organization, "[t]his is a rich reward for a single hack, either of an aggregated database of personally identifiable information or of a single consumer's multiple accounts, makes data aggregators an attractive target for criminals. [Hackers would] obtain the key not to just a single room, but the key ring with keys to all the rooms." The Clearing House, "Comment Letter to Bureau-2016-0048 Request for Information Regarding Consumer Access to Financial Records," February 21, 2017, http://files.consumerfinance.gov/f/documents/112016_cfpb_Request_for_Information_Regarding_Consumer_Access_to_Financial_Records.pdf.

[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.

[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

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 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.

---

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 Growth," press release, April 3, 2016, www.kabbage.com/blog/kabbage-santander-uk-partner-accelerate-smb-growth/.

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 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.[28]

[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. ("[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, https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf.

[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.

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).[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.[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 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

[29] Directive (EU) 2015/2366 of the European Parliament and of the Council, November 25, 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366 (last visited Feb. 1, 2017).
[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.

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."[31]

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.[32] 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.[33] Similarly, it could be useful to periodically assess whether and how authority under the Bank Service Company Act might pertain to developments 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

[31] With limited exceptions, such as for de minimis transactions.
[32] Richard Cordray, "Prepared Remarks of CFPB Director Richard Cordray" at the Lendit USA Conference, March 6, 2017, www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-richard-cordray-lendit-usa-conference/; Richard Cordray, "Prepared Remarks of CFPB Director Richard Cordray" at Money 20/20, October 23, 2016, www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-richard-cordray-money-2020/; Consumer Financial Protection Bureau, "Request for Information Regarding Consumer Access to Financial Records," Federal Register, November 22, 2016, www.federalregister.gov/documents/2016/11/22/2016-28086/request-for-information-regarding-consumer-access-to-financial-records.
[33] See, e.g., Lael Brainard, "The Opportunities and Challenges of Fintech" at the Conference on Financial Innovation at the Board of Governors of the Federal Reserve System, December 2, 2016, https://www.federalreserve.gov/newsevents/speech/brainard20161202a.htm.

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.[34] 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

[34] See Office of the Comptroller of the Currency, Exploring Special Purpose National Bank Charters for Fintech Companies, December 2016, www.occ.treas.gov/topics/bank-operations/innovation/comments/special-purpose-national-bank-charters-for-fintech.pdf.

providing the level of data security and protection they have come to rely on from their banks.[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.

[35] See, e.g., Jennifer Booton, "Apple Will Make $3 Billion Playing Pokémon Go," MarketWatch, July 21, 2016, www.marketwatch.com/story/apple-stands-to-make-billions-from-pokemon-go-2016-07-20 (citing report by analyst Lauren Martin).