Utah Law Review

Volume 2020 | Number 5 Article 4

1-2021

Show Me the (Data About the) Money!

Nizan Geslevich Packin
Barusch College

SHOW ME THE (DATA ABOUT THE) MONEY!

Nizan Geslevich Packin*

Abstract

Information about consumers, their money, and what they do with it is the lifeblood of the flourishing financial technology ("FinTech") sector. Historically, highly regulated banks jealously protected this data. However, consumers themselves now share their data with businesses more than ever before. These businesses monetize and use the data for countless prospects, often without the consumers' actual consent. Understanding the dimensions of this recent phenomenon, more and more consumer groups, scholars, and lawmakers have started advocating for consumers to have the ability to control their data as a modern imperative. This ability is tightly linked to the concept of open banking—an initiative that allows consumers to control and share their banking data with service providers as they see fit. But in the U.S., banks have threatened to block the servers of tech companies and data aggregators—business entities that serve as the middlemen connecting FinTech companies and banks, enabling consumers to get more financial services—from accessing their customers' data even if the customers agree to it. With no regulation or accepted standards for the ethical gathering and use of data, banks argue that limiting access helps them protect their clients' privacy, improve their accounts' safety, and promote consumer protection principles. Banks claim that FinTech apps collect more data than needed, store it insecurely, and sell it to others.

But the motivation of the big banks in advocating for such limitations may not be so pure. Banks do not want to relinquish competitive advantages, lose customers, or be held liable for data or fund losses. Witnessing resistance, tech companies are not sitting idly by waiting for banks to limit their data access. Instead, they are working on ways to outsmart banks' blocking technology and use data aggregation services as a middleman. They also extended the fight into Washington, where regulators such as the Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB) are noticing how technology impacts consumer data flows and credit reporting issues. Advocating for consumers' rights to control data, tech companies lobby for open banking.

 Associate Professor of Law at Baruch College, City University of New York, and an Affiliated Faculty at Indiana University Bloomington's Program on Governance of the Internet & Cybersecurity. A special thanks to the participants of the 2020 PLSC, as well as the 2020 National Business Law Scholars Conference, for their helpful comments. Thanks also to Peter Kim for the invaluable input.

The legal status of third-parties' right to access consumers' financial data is anchored in the EU's recently adopted Payment Services Directive II. In the U.S., however, the approach to open banking is market-based, in which data aggregators have become key players without the notice of consumers. Realizing this, in 2018, the Financial Industry Regulatory Authority (FINRA) issued a warning about the dangers of consumers sharing their account data with data aggregators to access apps, and in 2019, the Federal Deposit Insurance Corporation (FDIC) inspector general released a report expressing concerns about data aggregators.

The status-quo could change. The previously ignored Section 1033 of the Dodd-Frank Act "provides for consumer rights to access financial account and account-related data in usable electronic forms." Yet, the section's applicability to third-parties, which access consumer data with consumers' permission as opposed to consumers directly accessing their own data, is not clear. Similarly, regulation must address data aggregators' business operations, including issues such as anti-competition, obtaining consumers' informed consent to data sharing, and data security, given the credit card companies' recent attempts to acquire the biggest data aggregators. This Article is the first to direct attention to data aggregators—an overlooked category within the financial services industry. By analyzing financial regulation and privacy law, this Article examines data aggregators' relationships with banks, tech companies, and consumers. It provides a comparative lens between top-down and bottom-up regulatory approaches to data sharing, and draws from an Australian law that creates a singular consumer right that enables all institutions to connect to other data systems. It also suggests regulating data aggregators as gatekeepers in ways analogous to credit rating agencies.

TABLE OF CONTENTS

I. INTRODUCTION

When a consumer downloads a FinTech app, such as Venmo[1] or RobinHood,[2] on her smartphone then logs into it, she is likely not interfacing with her bank but providing her bank account login and password to a data aggregator. Frequently, the data aggregator stores the login credentials and uses them to continually log into the consumer's bank account to copy all personally identifiable data, ranging from transaction information to account numbers. Additionally, once it has accessed consumer data, the data aggregator can share, sell, or even carelessly dispose of her information with or without the consumer's knowledge.

These open banking practices of accessing, sharing, transferring, and selling data raise many concerns as they entail great risk. Data is valuable. The more data a company has about an individual, the more power it has over that individual's decision-making. In today's big data-driven economy, the companies with the most data have the most power. Consequently, people's ability to maintain control over their data has become a modern imperative, especially in consumer finance, where technological advances impact consumers' transfer of data and affect credit scoring issues.[3] In particular, such technological advances enable American consumers, who

[1] Venmo is a non-banking business entity that offers peer-to-peer payment services and a digital money transfer network, accessible via a smartphone app. *See generally* Kelly McNulty, *How Venmo Works and What You Need to Know Before You Use It*, MARKETWATCH (Apr. 17, 2019, 10:54 AM), https://www.marketwatch.com/story/how-venmo-works-and-what-to-know-before-you-use-it-2019-04-09 [https://perma.cc/XY89-79MB].

[2] RobinHood is a FinTech investment app that helped introduce a "generation of investors to the market, but without much in the way of additional education." *See* Matthew J. Razzano, *An Unsafe Sandbox: Fintech Innovation at the Expense of Consumer Protection?*, 2019 U. ILL. L. REV. ONLINE 132, 136 (2019).

[3] *See generally* Nizan Geslevich Packin & Yafit Lev-Aretz, *On Social Credit and the Right to be Unnetworked*, 2016 COLUM. BUS. L. REV. 339 (2016) (explaining the consequences of implementing a social credit system in finance).

spend on average five hours a day on their smartphones,[4] to allow third-parties to access their personal financial data by using different technologies.[5] But the problem is beyond the scope of certain defined contexts, such as those protected by privacy or data protection laws, which hardly reflects issues discussed in current privacy theories.[6] The rights and duties of various parties interested in individuals' personal data in computer databases are unclear.[7]

Despite the ambiguity surrounding third-party rights over individuals' personal information, and even more so since the COVID-19 pandemic has pushed more individuals to use FinTech services on their smartphones,[8] consumers continue to transact with FinTech companies as they offer innovative services and products. For example, according to a report by the World Bank's Global Financial Inclusion Database, three-quarters of the world's poor in 2011 did not have a bank account for a variety of reasons, such as costs, travel distances, and difficulties associated with opening an account,[9] but can use their mobile-phones for financial services. Even in

---

[4] Eileen Brown, *Americans Spend Far More Time on Their Smartphones than They Think*, ZDNET (Apr. 28, 2019, 1:15 PM), https://www.zdnet.com/article/americans-spend-far-more-time-on-their-smartphones-than-they-think/ [https://perma.cc/7FFF-3EES] (reporting that "[t]he average American spends 5.4 hours a day on their phone").

[5] Third-parties typically access personal financial data using (i) an application programming interface ("API"), or (ii) screen scrapers. APIs—sets of code that give third-parties secure access to their back-end data—serve as channels for developers to get to the data and build their own products and services around it. Put differently, a screen scraper is a "software capable of automatically contacting various web sites and extracting relevant information." *See* Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act,* 24 B.U. J. SCI. & TECH. L. 372, 383 (2018) (quoting Shea *ex rel.* The Am. Reporter v. Reno, 930 F. Supp. 916, 929 (S.D.N.Y. 1996)). In banking, the terms refer to a non-bank that offers services and obtains secure credentials of bank customers to access their accounts, gets their financial data, and saves it in an app via an automated process. *See id.* at 373–74.

[6] JANE K. WINN & BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE § 7.09 (4th ed. 2020).

[7] Jane K. Winn & James Wrathall, *Who Owns the Customer—The Emerging Law of Commercial Transactions in Electronic Customer Data*, 56 BUS. LAW. 213, 214–15 (2000).

[8] *See, e.g.*, *New Data: More than Forty Percent of U.S. Consumers Shop Through Digital Channels . . . And Stay There*, PYMNTS (Nov. 9, 2020), https://www.pymnts.com/news/merchant-innovation/2020/new-data-more-than-forty-percent-of-u-s-consumers-shop-through-digital-channels-and-stay-there/ [https://perma.cc/Y9DU-FLGY]; *FSB: Outsourcing Banking Technology Could Pose 'Systemic Risk,'* PYMNTS (Nov. 9, 2020), https://www.pymnts.com/news/banking/2020/fsb-risk-of-outsourcing-bank-technology/ [https://perma.cc/WQD6-R4C3] ("The pandemic may have also accelerated the trend towards greater reliance on certain third-party technologies." (quoting the Financial Stability Board)).

[9] Asli Demirguc-Kunt & Leora Klapper, *Measuring Financial Inclusion: The Global Findex Database* 11–18 (World Bank Dev. Research Grp., Working Paper No. 6025, 2012); *see also* Matthew B. Gross, Jeanne M. Hogarth & Maximilian D. Schmeiser, *Use of*

the U.S., a relatively large number of households live at least partially outside the mainstream financial system.[10] Such households' lack of access to the financial system contributes to financial disparity, tragically impacts consumers' ability to navigate the twists and turns of life, and prevents economic recovery.[11] But, thanks to the emergence of new innovative technologies that facilitate connectivity and mobile financial transactions, tech companies and social networks have successfully set their foot on the market for underserved populations and offer services to these individuals.[12] Moreover, even consumers that are part of the traditional financial service system, have started to rely more and more on FinTech services. Research shows that in the U.S., twenty percent of families with traditional bank accounts rely on alternative financial services.[13]

Similarly, FinTech solutions enable "data portability," which refers to consumers' ability to transfer digital information from one place to another quickly and easily. However, in the absence of legislation, companies might not facilitate it, and the consumers will not have the ability to transfer their data.[14] Aside from

---

Financial Services by the Unbanked and Underbanked and the Potential for Mobile Financial Services Adoption, 98 FED. RES. BULL. 1 (2012), http://www.federalreserve.gov/pubs/bulletin/2012/pdf/mobile_financial_services_201209.pdf [https://perma.cc/8CCF-D9M3].

[10] CONSUMER & CMTY. DEV. RSCH. SECTION, FED. RSRV. BD., CONSUMERS AND MOBILE FINANCIAL SERVICES 5 (2014), http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201403.pdf [https://perma.cc/WMR8-DGKX].

[11] *See* Sarah Bloom Raskin, Governor, Fed. Rsrv. Bd., Remarks at The New America Foundation Forum: Economic and Financial Inclusion in 2011: What It Means for Americans and Our Economic Recovery (June 29, 2011) (detailing why broad inclusion matters to economic recovery, and stating that "effective inclusion in the financial marketplace depends upon a strong regulatory framework, active market participation, and an expansion in public financial literacy").

[12] *See generally* Nizan Geslevich Packin & Yafit Lev-Aretz, *Big Data and Social Netbanks: Are You Ready to Replace Your Bank?*, 53 HOUS. L. REV. 1211 (2016) [hereinafter Packin & Lev-Aretz, *Big Data and Social Netbanks*] (discussing the rise of non-bank FinTech start-ups); *Fintech: Examining Digitization, Data, and Technology*: *Hearing Before the S. Comm. on Banking, Hous., & Urb. Affs.,* 115th Cong. 4 (2018) (Steven Boms, President, Allon Advocacy, LLC, on behalf of the Consumer Fin. Data Rights Grp.), https://www.banking.senate.gov/imo/media/doc/Boms%20Testimony%209-18-18.pdf [https://perma.cc/8XR4-48J4] ("Twenty percent of adult Americans are underbanked by the traditional financial services system and almost nine million American households are entirely unbanked. For these consumers, third party, technology-based tools can provide vital, affordable access to a financial system that has left them behind.").

[13] Jason Furman, *Financial Inclusion in the United States*, WHITE HOUSE BLOG (June 10, 2016, 8:00 AM), https://obamawhitehouse.archives.gov/blog/2016/06/10/financial-inclusion-united-states [https://perma.cc/RCA9-RBTQ]. People use FinTech services for, *inter alia*, things like faster payments, robo-advisers, and wealth management tools. *See* CONSUMER & CMTY. DEV. RSCH. SECTION, *supra* note 10, at 21.

[14] Rory Van Loo, *Technology Regulation by Default: Platforms, Privacy, and the CFPB*, 2 GEO. L. TECH. REV. 531, 534 (2018) (discussing data portability). The EU Payment

promoting goals such as financial inclusion, internet connectivity, data portability, and enhancement of other information-related rights, FinTech companies are successful because they make things easier for consumers. They offer user-friendly products and services and enable consumers to save and spend efficiently, improving their customer experience.[15] This is important because we live in an era where customers demand top-notch experiences.[16] But since banks are not technology companies and have traditionally not focused on offering more custom-tailored experiences,[17] a third of all banking customers in 2019 used external custom-tailored

---

Account Directive grants the right of bank account data portability to EU consumers. Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the Comparability of Fees Related to Payment Accounts, Payment Account Switching and Access to Payment Accounts with Basic Features, 2014 O.J. (L 257) 214. Similarly, the General Data Protection Regulation ("GDPR") grants consumers the right to get a copy of the information they have provided. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1. Likewise, under the second Payment Services Directive ("PSDII"), banks must share access to their customer account data with their competitors. Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC, 2015 O.J. (L 337) 35.

[15] *See* LAUREN SAUNDERS, NAT'L CONSUMER LAW CTR., FINTECH AND CONSUMER PROTECTION: A SNAPSHOT 2 (2019), https://www.nclc.org/images/pdf/cons-protection/rpt-fintech-and-consumer-protection-a-snapshot-march2019.pdf [https://perma.cc/Y94E-5L7J] ("Fintech products and services have the potential to provide important benefits to consumers. They promise to lower costs, promote financial inclusion, help people avoid fees and comparison shop, improve personal financial management, and build assets and wealth.").

[16] The majority of consumers in the financial services industry would likely cease to buy from or transact with a business—specifically a bank—if a competitor, such as a FinTech company, offers a better experience. *See Customer Expectations Hit All-Time Highs*, SALESFORCE RESEARCH, https://www.salesforce.com/research/customer-expectations/ [https://perma.cc/Q2VR-KQN4] (last visited July 6, 2020) (finding that 76% of customers thought it was easier than ever to take their business elsewhere, as disruptive companies leverage technology to offer the personalized, valuable, immediate, and superior experience customers have grown to expect from businesses they engage with).

[17] Consumer expectations for customization are important. A study showed that 70% of customers say understanding how they use products and services is very important to winning their business, 59% of customers say tailored engagement based on prior interactions is very important to winning their business, and customers are more than twice as likely to view personalized offers as significant versus insignificant. *Id.*; *see also* Sam Stewart, Philippe Soussan, Pierre Roussel, Muriel Dupas, Juan Uribe & Frédérique Brugère, *Retail Banking Distribution 2025: Up Close and Personal*, BOS. CONSULTING GRP. (Sept. 26, 2019), https://www.bcg.com/publications/2019/retail-banking-distribution-2025-up-close-personal.aspx [https://perma.cc/TK6L-7J65] (explaining how personalization of

FinTech apps.[18] Likewise, nearly two-thirds of millennials would share their data in return for more personalized service.[19]

In noticing this trend in consumer preferences early on, technology companies and banks have started jockeying over who controls—and has access to—consumer financial data. This conflict is particularly noticeable in the U.S., where some banks threaten to block technology companies' servers from accessing their customers' financial data. The banks argue that access limits are how they can best look out for their clients' interests, protect their privacy, improve account safety,[20] and promote consumer protection principles.[21] The banks claim FinTech companies do not protect consumer privacy, or prevent potential discrimination that can stem from using, sharing, and selling data that is then analyzed for various purposes, and that they collect more data than needed, store it insecurely, and sell it to third-parties.[22]

Between 2016 to 2020, the power struggle over consumer financial data has escalated. After several banks, such as JPMorgan Chase and Capital One, made it clear that they intend to control FinTech companies' access to data, global media outlets started covering the tension.[23] Serving as a poster child for this tension in

---

customer service can help banks increase profitability by up to 25% and how customers expect smart digital banking that is tailored to their immediate needs).

[18] *Why Open Banking Represents a Seismic Shift for Fintech*, KNOWLEDGE @ WHARTON (Jan. 16, 2019) [hereinafter *Seismic Shift*], https://knowledge.wharton.upenn.edu/article/open-banking-represents-seismic-shift-fintech/ [https://perma.cc/3V5L-LZK6].

[19] *See* Devon McGinnis, *Please Take My Data: Why Consumers Want More Personalized Marketing*, SALESFORCE BLOG (Dec. 2, 2016), https://www.salesforce.com/blog/2016/12/consumers-want-more-personalized-marketing.html [https://perma.cc/GY6C-4NNU].

[20] Steven Harras, *FDIC Watchdog Worries About Unsupervised Logins for Customer Bank Data*, CONG. Q. ROLL CALL, Mar. 5, 2019, 2019 WL 1032055 (describing the difficulty in improving account safety considering as much as forty percent of online logins to bank accounts are not from actual customers, but from data aggregators that have been authorized access to their personal information).

[21] Nizan Geslevich Packin, *Big Banks vs. Silicon Valley Startups: Whose Customer Financial Data Is It Anyway?*, FORBES (Apr. 19, 2019, 2:15 PM), https://www.forbes.com/sites/nizangpackin/2019/04/19/big-banks-vs-silicon-valley-startups-whose-customer-financial-data-is-it-anyway/#31c9768b5155 [https://perma.cc/T7VJ-LK8J]; Ben Isaacson, *As Mobile Apps Proliferate, Data Protection Has to Keep Up*, AM. BANKER (July 22, 2019), https://www.americanbanker.com/opinion/as-mobile-apps-proliferate-data-protection-has-to-keep-up [https://perma.cc/7WGF-SSJN] (discussing tradeoffs that prioritize convenient services over safety and privacy, and the significant risks that result).

[22] *Id*.

[23] *See, e.g.*, Robin Sidel, *Big Banks Lock Horns with Personal-Finance Web Portals; J.P. Morgan, Wells Fargo Are Snarling the Flow of Data to Popular Websites that Help Consumers Manage Their Finances*, WALL ST. J. (Nov. 4, 2015, 7:30 PM), https://www.wsj.com/articles/big-banks-lock-horns-with-personal-finance-web-portals-1446683450 [https://perma.cc/M3CH-ZQMR]; Frances Schwartzkopff, *Banks Facing Data Crisis May Need Political Help*, *Denmark Warns*, BLOOMBERG (Dec. 8, 2019), https://www.bloomberg.com/news/articles/2019-12-08/banks-may-need-political-help-to-

early 2019 was Cushion, a startup that helps users win refunds in fees charged by financial institutions using a chatbot.[24] According to its statements, Cushion needed very broad permission to request data, but banks did not want to share the requested data.[25] Similarly, in December 2019, news broke that many of PNC Bank's customers were having difficulties connecting their bank accounts to the Venmo app.[26] These customers could not access PayPal's mobile payment service due to the rivalry among banks, FinTech companies, and the middlemen—data aggregators—that connect banks and FinTech companies.[27]

As suggested in the tensions above, the banks' motivation to limit technology companies' access to data may not be so pure. First, banks are forced to give a competitive advantage to the financial industry's new entrants,[28] and laws such as the European Union's PSDII entail a uni-directional flow of consumer data. This means banks must share access to their customers' data with FinTech companies, but FinTech companies are not required to share their information with banks. Second, banks do not wish to be liable for losses of funds or data, but, under current rules, banks are likely covering the losses for breaches. Moreover, many FinTech companies do not have the funds to cover losses, and some may be losing money and/or raising capital. This means either consumers will absorb their losses for

---

survive-big-tech-a-nordic-view [https://perma.cc/VRV3-NHEB] (explaining that "[f]irst there was the financial crisis of 2008. Then years of negative interest rates. Now, banks face what one financial regulator calls the 'real game changer.' . . . [T]he next big threat for banks is the rapid spread of big tech into financial services. The competitive tool is personal data and the playing field is far from even."); *see also* Jennifer Surane, *Big Banks' Clampdown on Data Puts Silicon Valley Apps on Alert*, BLOOMBERG (Mar. 26, 2019), https://www.bloomberg.com/news/articles/2019-03-26/jpmorgan-s-clampdown-on-data-puts-silicon-valley-apps-on-alert [https://perma.cc/ZBB7-3J67].

[24] Surane, *supra* note 23.

[25] *Id*.

[26] Yuka Hayashi, *Venmo Glitch Opens Window on War Between Banks, Fintech Firms*, WALL ST. J. (Dec. 14, 2019), https://www.wsj.com/articles/venmo-glitch-opens-window-on-war-between-banks-fintech-firms-11576319402 [https://perma.cc/6LPD-LC63].

[27] *Id.*

[28] *See generally* Ryan Browne, *Europe's Banks Brace for a Huge Overhaul that Throws Open the Doors to Their Data*, CNBC (Jan. 11, 2018, 3:01 AM), https://www.cnbc.com/2017/12/25/psd2-europes-banks-brace-for-new-eu-data-sharing-rules.html [https://perma.cc/687D-9VFA]. In terms of customer data management in the financial sector:

> Banks have long been at an advantage when it comes to data on their customers. From current accounts to credit cards, established lenders have access to vast amounts of information that financial technology (fintech) competitors could only dream of . . . . that could all be about to change . . . . banks operating in the European Union will be forced to open up their customer data to third party firms —that is, when customers give consent.

Id.

oversharing personal data, or they would expect deep-pocketed banks to do so, which makes banks prefer to err on the side of caution and limit access to data.[29] Third, banks are lagging behind FinTech companies in customer service, customized experience,[30] and deliverance of innovative offerings,[31] often because the banks are heavily regulated and simply cannot offer the same things as the FinTech companies.

Unlike banks and FinTech entities, the data aggregators have received minimal attention from regulators.[32] Yet data aggregators have a growing role in the financial ecosystem [33] and include Plaid, Intuit, Finicity, Envestnet|Yodlee, Morningstar/ByAllAccounts, Fiserv/CashEdge, and MX.[34] Data aggregators are barely subject to any regulation,[35] have received little scholarly attention, and most

---

[29] *See* Hayashi, *supra* note 26.

[30] *See Customer Expectations*, *supra* note 16.

[31] *Id.* (stating that 56% of customers actively seek to buy from the most innovative businesses, which consistently introduce new products and services; 63% of customers expect businesses to offer new products and services more frequently than ever before; and 66% of customers say businesses now need to do more to impress them with new offerings).

[32] *Investor Alert: Know Before You Share: Be Mindful of Data Aggregation Risks*, FIN. REGUL. AUTH. (Mar. 29, 2018) [hereinafter *Know Before You Share*], https://www.finra.org/investors/alerts/be-mindful-data-aggregation-risks [https://perma.cc/ZNH9-HTUC]. For consumers looking for smarter financial solutions:

> There are many companies—often called data aggregators—ready to help you organize your financial life. However, before you share your account information and other sensitive financial details with data aggregators, it pays to know how these services operate, and how to protect yourself from potential privacy and security risks.

Id.

[33] *See generally* Kimberly L. Wierzel, *If You Can't Beat Them, Join Them: Data Aggregators and Financial Institutions*, 5 N.C. BANKING INST. 457 (2001) (explaining that data aggregators enable consumers to turn over their different accounts' login credentials at various banks to one operator, which in turn lets them view all of their data from one site).

[34] *See* MX Technologies Inc., *A List of Financial Data Aggregators in the United States*, MX (Mar. 5, 2018), https://www.mx.com/moneysummit/a-list-of-financial-data-aggregators-in-the-united-states [https://perma.cc/V3VE-LRHW]. The report mentions eight data aggregators—the seven stated above and Quovo, which was acquired by Plaid in 2019. *See* Penny Crosman, *What Happens If Mastercard and Visa Gobble Up All the Data Aggregators*, AM. BANKER (June 29, 2020, 3:39 PM), https://www.americanbanker.com/news/what-happens-if-mastercard-and-visa-gobble-up-all-the-data-aggregators [https://perma.cc/CZ4M-B36S] [hereinafter Crosman, *Mastercard and Visa Gobble Up*]. Additionally, a "newer competitor in aggregation is Akoya, which spun off in February [2020] from Fidelity Investments and is now owned by Fidelity." *Id.*

[35] Penny Crosman, *Why a Clear Answer to the Data-Sharing Debate Remains Elusive*, AM. BANKER (Feb. 23, 2017, 3:39 PM), https://www.americanbanker.com/news/why-a-clear-answer-to-the-data-sharing-debate-remains-elusive [https://perma.cc/66X3-57M4] [hereinafter Crosman, *Data-Sharing Debate*]. Experts have expressed concerns about how

consumers have never even heard of them or know what they do.[36] It is remarkable how data aggregators became powerful without many of us noticing, especially considering "[w]hen aggregators access account numbers, many store them indefinitely, often unbeknownst to customers. This puts customers and their money at risk."[37] It is questionable whether consumers actually know what risks they are exposed to as a result of their data being shared between banks and different third-parties.[38]

Data aggregators are here to stay. In the U.S., there are thousands of banks and even more FinTech companies offering services to consumers that need data aggregators to communicate, transact, and trust each other while sharing data. FinTech companies' data gathering is typically done by one of two ways: (i) screen-scraping of public data from a website[39]; and (ii) APIs, a technology that enables

---

data aggregators are so minimally regulated given their significant role in the financial ecosystem:

> The data aggregators are very lightly regulated. They don't have a lot of the strict, hard obligations banks and other institutions have[.] . . . That means there's a lot of innovative stuff going on here, but lately the amount of data people are keeping around for big data uses has been troubling.

Id.

[36] Penny Crosman, *Is Finra's Dire Warning About Data Aggregators on Target?*, AM. BANKER (Apr. 9, 2018, 4:54 PM), https://www.americanbanker.com/news/is-finras-dire-warning-about-data-aggregators-on-target [https://perma.cc/729J-42HW] [hereinafter Crosman, *Finra's Dire Warning*] (explaining that data "[a]ggregators are almost always a middleman. When you use an online service or app or even a service from a provider that uses aggregation under the hood, there are very few end customers that realize the aggregator is acting on their behalf as their agent.").

[37] Hayashi, *supra* note 26 (quotations omitted); *see* THE CLEARING HOUSE, CONSUMER SURVEY: FINANCIAL APPS AND DATA PRIVACY SURVEY 5–6 (2019), https://www.theclearinghouse.org/-/media/New/TCH/Documents/Data-Privacy/2019-TCH-ConsumerSurveyReport.pdf [https://perma.cc/8H57-8PD9] [hereinafter CONSUMER SURVEY] (finding that, for example, only 21% of the surveyed consumers were aware that financial apps continue to have access to their data until they revoke their bank credentials).

[38] When surveyed, most consumers responded that they want the "seamless experience" of FinTech, and also the data security and privacy traditionally offered by banks. CONSUMER SURVEY, *supra* note 37, at 7–8.

[39] *See, e.g.*, WINN & WRIGHT, *supra* note 6; Jeffrey Kenneth Hirschey, *Symbiotic Relationships: Pragmatic Acceptance of Data Scraping*, 29 BERKELEY TECH. L.J. 897, 897 (2014) (discussing automated data collection on the Internet). Screen-scraping was recently held by the 9th Circuit not to constitute "hacking." *See* hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 999 (9th Cir. 2019).

programmers to integrate data from one source into third-party apps, restrict how apps tap data, and contractually limit the data's usages.[40]

Visa understood the importance of financial data sharing, as well as data aggregators' impact on innovative financial services, and in early 2020, it announced plans to purchase Plaid, the biggest data aggregator.[41] Originally, Plaid stated that its goal was to enable FinTech companies to offer innovative services to consumers, thereby increasing competition among providers, lowering service costs, and enhancing consumer access to services.[42] However, in May 2020, Plaid already changed course, declaring its plan to launch Plaid Exchange, a platform that puts banks, Visa's biggest customers, in the driver's seat.[43] Specifically, Plaid Exchange is meant to let banks control data-sharing efforts, as it is "a bank product that will enable banks to expose APIs to a range of trusted FinTech developers."[44] Then, in June 2020, MasterCard reinforced the industry's understanding of the critical role of data aggregators when it announced its plans to buy Finicity to compete with Visa and Plaid in the financial services race.[45] But in November 2020, the U.S. Department of Justice ("DOJ")—after examining the Visa-Plaid deal—sued to block the $5.3 billion acquisition, citing competition concerns.[46] The DOJ alleged that the largest card network buying the data aggregator would slow FinTech innovation and benefit only Visa and big banks.[47]

---

[40] *See, e.g.*, WINN & WRIGHT, *supra* note 6 ("The earliest examples of 'Open API Banking' appear to have emerged in the United States as innovative business models used by some banks.").

[41] David Z. Morris & Jeff John Roberts, *Visa's New Monopoly*, FORTUNE (Jan. 15, 2020, 7:50 A.M.), https://fortune.com/2020/01/15/visas-new-monopoly/ [https://perma.cc/S9WH-6738].

[42] *Id.* This would make Plaid become a part of Visa, whose customers are big banks. *Id.*

[43] Tim Sloane, *Visa Acquisition Prospect Plaid Intros Open Banking API Strategy that Mimics Mastercard's*, PAYMENTS J. (May 21, 2020), https://www.paymentsjournal.com/visa-acquisition-prospect-plaid-intros-open-banking-api-strategy-that-mimics-mastercards [https://perma.cc/JQ3F-GJNQ].

[44] *Id*.

[45] *See* Laura Noonan, *Mastercard to Buy US Open-Banking Group Finicity for $1bn*, FIN. TIMES (June 23, 2020), https://www.ft.com/content/0c42b31f-cbf3-4dd7-97ad-3ec6ff2db00e [https://perma.cc/7KXL-72M5]. Mastercard's $1 billion purchase of Finicity is a deal that expands its footprint in open banking. *Id.*

[46] Brent Kendall & AnnaMaria Andriotis, *Justice Department Files Antitrust Lawsuit Challenging Visa's Planned Acquisition of Plaid,* WALL ST. J. (Nov. 5, 2020, 3:38 PM), https://www.wsj.com/articles/justice-department-files-antitrust-lawsuit-challenging-visa-s-planned-acquisition-of-plaid-11604591434 [https://perma.cc/U96H-XG6C].

[47] *Id.* ("[DOJ] alleg[ed] [that] the deal would eliminate the nascent but significant competitive threat that Plaid poses to Visa in the online debit market."). Likewise, neutralizing Plaid would help Visa's biggest customers—banks—as it could stop data aggregators from using bank customers' data of the banks. Anna Hrushka, *Visa's Plaid Deal Faces Antitrust Scrutiny from Justice Department,* BANKINGDIVE (Oct. 28, 2020),

This Article examines consumers' ability to manage their financial data—an issue that is unclear in the U.S. unlike in other places in the world—and explores the roles of data aggregators, FinTech companies, and consumers in managing this data. In the U.S., the right to access financial data is affiliated with Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the Dodd-Frank Act),[48] which has not yet been interpreted by the judicial system or any government agency. But while the time has clearly come to regulate the issue of data sharing in the consumer finance context, lawmakers and government agencies that have commented on the topic failed to issue clear standards or binding rules and much uncertainty remains. First, in 2017, the Consumer Financial Protection Bureau ("CFPB")[49] released a set of non-binding principles on consumer-authorized use of financial data.[50] But the principles are broad, generic, and do not confirm whether Section 1033 preserves third-parties' right to pull data directly from bank customers' accounts.[51] Second, a 2018 Department of the Treasury report embraced a similar approach. [52] Third, in 2018, the Financial Industry Regulatory Authority ("FINRA")[53] issued a warning to investors about data aggregators and their activities

---

https://www.bankingdive.com/news/visas-plaid-antitrust-department-of-justice/587939/ [https://perma.cc/5HH9-ES7M].

[48] 12 U.S.C. § 5301.

[49] Rory Van Loo, *Making Innovation More Competitive: The Case of Fintech*, 65 UCLA L. REV. 232, 237 (2018) [hereinafter Van Loo, *Making Innovation More Competitive*]. Van Loo explains how the CPFB came to life and its main goal, stating:

> Prior to the 2008 financial crisis, banking regulators carried a dual mission of protecting consumers and ensuring financial stability. This pairing subordinated consumer protection to stability. To solve this problem in the wake of the subprime mortgage crisis, Congress launched a new agency, the Consumer Financial Protection Bureau . . . . The CFPB took over most of stability regulators' consumer protection powers but has no stability mission.

Id.

[50] CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION 3–5 (2017) [hereinafter CFPB CONSUMER PROTECTION], https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf [https://perma.cc/QE69-87KQ].

[51] Telis Demos, *Fintech Startups Want to Save One Key Page of Dodd-Frank*, WALL ST. J. (Feb. 2, 2017), https://www.wsj.com/articles/fintech-startups-want-to-save-one-key-page-of-dodd-frank-1486035001 [https://perma.cc/5VDV-8RDQ].

[52] U.S. DEP'T OF THE TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES: NONBANK FINANCIALS, FINTECH, AND INNOVATION 31 (2018) [hereinafter 2018 Treasury Report].

[53] ANDREW STOLTMANN & BENJAMIN P. EDWARDS, FINRA GOVERNANCE REVIEW: PUBLIC GOVERNORS SHOULD PROTECT THE PUBLIC INTEREST 1 (2017) (explaining that FINRA "plays a vital role in regulating the securities industry"). FINRA describes itself as "an independent, not-for-profit organization authorized by Congress to protect America's investors by making sure the securities industry operates fairly and honestly." *Id.*

in the context of open banking and data portability,[54] but never went beyond that. Fourth, in early 2019, the Federal Deposit Insurance Corporation ("FDIC") inspector general expressed concerns about unsupervised logins for customer bank data.[55] Lastly, in 2020, the CFPB organized a symposium dedicated to financial data sharing, indicating that it might finally be on the regulators' radar screen.[56]

As this Article shows, the fight over the management of consumer financial data is focused on a type of potential harms that may flow from conduct in the data-driven economy, and is not unique or limited to the U.S. The EU's adoption of a top-down financial regulation—the "open API banking" PSDII—is pro-innovation and anti-screen-scraping, but is still very one-sided,[57] and addresses the issue of data sharing only in the context of payments.[58] In contrast, the U.S.'s market-led approach to open banking has resulted in banks,[59] data aggregators, and FinTech

---

[54] *See Know Before You Share*, *supra* note 32.

[55] The FDIC was created after the collapse of thousands of banks during the Great Depression, and it is the vehicle through which the federal government insures deposits if an FDIC-backed institution fails. John T. Holden, *Trifling and Gambling with Virtual Money*, 25 UCLA ENT. L. REV. 41, 52, n.54 (2018). In that context, Steven Harras recommends:

> Policymakers and examiners "must keep pace with the adoption of new financial technology to assess its impact on the safety and soundness of institutions and the stability of the banking system." That includes the practices of data aggregators acting as middlemen between fintech companies and banks . . . . [because] however much banks seek to limit outsider access to consumer information, data aggregators can still collect consumer data for use by fintech developers without the permission or knowledge of the bank.

See Harras, *supra* note 20. (quoting OFF. OF INSPECTOR GEN., FDIC, TOP MANAGEMENT AND PERFORMANCE CHALLENGES FACING THE FEDERAL DEPOSIT INSURANCE CORPORATION 7 (2019), https://www.fdicoig.gov/report-release/top-management-and-performance-challenges-facing-federal-deposit-insurance [https://perma.cc/BZ3Y-QF6B]).

[56] *See* CONSUMER FIN. PROT. BUREAU, BUREAU SYMPOSIUM: CONSUMER ACCESS TO FINANCIAL RECORDS: A SUMMARY OF THE PROCEEDINGS (July 2020), https://files.consumerfinance.gov/f/documents/cfpb_bureau-symposium-consumer-access-financial-records_report.pdf [https://perma.cc/73MC-DCSS].

[57] *See Seismic Shift*, *supra* note 18.

[58] BASEL COMM. ON BANKING SUPERVISION, REPORT ON OPEN BANKING AND APPLICATION PROGRAMMING INTERFACES 5 (2019), https://www.bis.org/bcbs/publ/d486.pdf [https://perma.cc/LKM9-V8GT] ("Some frameworks, such as the . . . PSD2 . . . apply only to specific types of data, like payments processing data, and provide third parties with both 'read' and 'write' access to data and payment . . . . [T]he UK's open banking initiative additionally requires the inclusion of publicly-available information on branch and ATM locations, bank products and fees. In contrast, Australia's framework provides 'read-only' rights for data aggregation purposes and will eventually cover industries beyond banking.").

[59] *See* Penny Crosman, *Fintech Glasnost: Why U.S. Banks Are Opening Up APIs to Outsiders*, AM. BANKER (July 8, 2015, 3:30 PM), https://www.americanbanker.com/news/

companies trying to reach private agreements and understandings.[60] For example, some banks and FinTech companies have partnered to form the Financial Data Exchange ("FDX"), a nonprofit that attempts to tackle the challenge of securely sharing consumers' financial data.[61]

This Article advocates for adopting consumer data regulation that would be inspired by the newly enacted Australian Consumer Data Right Bill ("CDR"),[62] arguing that market-led solutions are simply not enough to address consumer data sharing because of two main reasons: (i) consumers should have the legal right to manage their financial data, and the CFPB should be the one to address this issue while incorporating key concepts such as transparency, consumers' informed consent to sharing data, competition laws, data security, financial institutions' liability, and consumer protection into its potential regulation; and (ii) data aggregators, their activities, their impact on the market, and their transactions with key players in the financial industry, without scrutiny, are too significant to be left unregulated.

First, consumers should have the legal right to manage their financial data. Therefore, a government agency must oversee and enforce the related rights and obligations connected with consumer data sharing. In the absence of a meta agency created for this purpose, many have identified the CFPB as the leading agency on consumer protection and FinTech-related issues and argued it should assume the role

---

fintech-glasnost-why-us-banks-are-opening-up-apis-to-outsiders [https://perma.cc/PW5V-JV5T].

[60] Similarly, the voluntary Model Agreement that the Clearing House ("TCH") released on November 12, 2019, is meant to help banks and FinTech companies establish legal terms for the sharing of bank-held consumer data. *See Value and Benefit of Model Data Access Agreement*, THE CLEARING HOUSE (Nov. 12, 2019), https://www.theclearinghouse.org/connected-banking/-/media/3b6d0100f58148dd8416af58104faba6.ashx [https://perma.cc/XXT8-DP49] [hereinafter *Model Data Access Agreement*]. Specific banks and data aggregators have also been trying to work together. *See, e.g*, *JPMorgan Chase, Envestnet|Yodlee Sign Agreement to Increase Customers' Control of Their Data*, BUS. WIRE (Dec. 5, 2019, 8:00 AM) [hereinafter *Increase Customers' Control*], https://www.businesswire.com/news/home/20191205005462/en/JPMorgan-Chase-Envestnet-Yodlee-Sign-Agreement-Increase [https://perma.cc/S8NG-HY83].

[61] *See Financial Industry Unites to Enhance Data Security, Innovation and Consumer Control*, FIN. SERV.-INFO. SHARING ANALYSIS CENT. (Oct. 18, 2018) [hereinafter FS-ISAC], https://www.fsisac.com/article/financial-industry-unites-enhance-data-security-innovation-and-consumer-control [https://perma.cc/SN4W-W6ER].

[62] Australia's Consumer Data Right (CDR) rules attempt to add personal data protection as an economy-wide right, to be applied sector-by-sector at the designation of the Australian Treasurer. *See generally* AUSTL. COMPETITION & CONSUMER COMM'N, CONSUMER DATA RIGHT RULES OUTLINE (2019), https://www.accc.gov.au/system/files/CDR-Rules-Outline-corrected-version-Jan-2019.pdf [https://perma.cc/6JEG-YW6T] (explaining the CDR).

of the lead agency regulating and monitoring such issues.[63] Moreover, the CFPB appears to be the natural candidate for this role, as it has the understanding, involvement, and experience in consumer financial data related matters. Specifically, in 2016, it even requested information about market practices related to access to consumers' data, per Section 1033,[64] and in 2017, it released non-binding "Consumer Protection Principles" related to consumer-authorized use of financial data,[65] expressing its vision for a safe, and workable data aggregation market.[66] This Article argues that as part of the CPFB's leadership on such issues, it should take on the regulation and supervision of data aggregators,[67] and consumer financial data management.[68]

This role could be tricky for the CFPB, which faced a series of challenges from all directions: "political and legal, empirical and anecdotal—about each and every part of its operations."[69] The CFPB's opponents launched a campaign against it shortly after the 2016 presidential elections mainly because of its structure,[70] which

---

[63] This is especially needed as currently, different administrative government agencies have started to create regulatory models to govern their turfs of the data economy, but no agency has stepped up to become the go-to agency on FinTech matters. *See, e.g.*, Van Loo, *supra* note 14, at 531–32 (exploring what the CFPB has done in its first several years to regulate FinTech).

[64] Barbara S. Mishkin, *CFPB Issues Request for Information on Consumer Access to Financial Information*, BALLARD SPAHR: CONSUMER FIN. MONITOR (Nov. 18, 2016), https://www.consumerfinancemonitor.com/2016/11/18/cfpb-issues-request-for-information-on-consumer-access-to-financial-information [https://perma.cc/E8DS-XXTT].

[65] CFPB CONSUMER PROTECTION, *supra* note 50, at 1–5.

[66] *Id.* at 1.

[67] Rory Van Loo, *The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance*, 72 VAND. L. REV. 1563, 1606, 1609 (2019) [hereinafter Van Loo, *The Missing Regulatory State*] (arguing that regulatory monitoring of businesses is essential for protecting privacy and promoting consumer protection). "Congress has imposed similar minimum annual monitoring of oil and gas platforms, underground mines, large banks, credit rating agencies, and nuclear plants." *Id*.

[68] It is therefore not surprising that in October 2020, the CPFB has decided to move forward with plans to issue a final rule in connection with consumers' rights to access their financial data, and published an advance notice of proposed rulemaking (ANPR) addressing Section 1033 of the Dodd-Frank Act. *See* Consumer Access to Financial Records, 85 Fed. Reg. 71,003 (proposed Nov. 6, 2020) (to be codified at 12 C.F.R. ch. X) [hereinafter the CPFB's 2020 ANPR]; Kate Berry, *CFPB Sets Stage for Long Fight on Data-Sharing Rule*, AM. BANKER, (Nov. 13, 2020, 1:30PM), https://www.americanbanker.com/news/cfpb-sets-stage-for-long-fight-on-data-sharing-rule [https://perma.cc/5G78-W5KV].

[69] Hosea H. Harvey, *Constitutionalizing Consumer Financial Protection: The Case for the Consumer Financial Protection Bureau,* 103 MINN. L. REV. 2429, 2430–31 (2019).

[70] The 2010 Dodd-Frank Act's creation of the CFPB reflects Congress' careful thought to the structure of the Bureau, and the attempt to strengthen consumer financial protection in addition to shield federal oversight of consumer finance from short-term political interests.

Congress designed to protect its work and mission from narrow political interests.[71] This opposition campaign continued with a new CFPB Acting Director's appointment, who halted implementation of certain rules and slowed enforcement efforts.[72] Lastly, the campaign sought a Supreme Court's holding on the CFPB's structure and scope of work, "in a case that has become a flashpoint in a partisan battle over financial reform and the president's constitutional powers."[73] In *Seila Law LLC v. Consumer Financial Protection Bureau,*[74] the Supreme Court focused on the CPFB's single leader's independent tenure protections meant to enable the CFPB to better protect consumers from financial institutions. The CFPB's opponents argued that this structure does not align with the "notions of presidential control over the executive branch of the government."[75] Publishing its decision on June 29, 2020, the Court struck down the leadership structure as unconstitutional.[76] While the holding seems to jeopardize the CFPB's operations, some commentators argue it "is a sheep that comes in wolf's clothing."[77] Seven of the nine justices have left untouched all other aspects of the CFPB's operations, with Chief Justice Roberts writing for the majority: "the CFPB's structure and duties remain fully operative without the offending tenure restriction."[78] This means that *Seila* represents a consumer victory because (i) no other constitutional challenges to the CFPB's authority remain; (ii) the constitutional challenges, which impeded the CFPB's enforcement work, have now been settled; and (iii) the immediate effect of *Seila* is to eliminate protections for the CFPB's single leader, the President's appointee that had been confirmed for five years, but can, post-*Seila,* be easily terminated. Therefore, *Seila's* biggest effect will likely be a new director appointment with every newly elected President. Hopefully, such personnel changes will not immobilize the CFPB's operations, and it will continue to protect consumers, their interests, and their financial data rights.

Second, market-led solutions are not enough to address consumer financial data issues because data aggregators are too significant to be left unregulated.[79] These

---

[71] Patricia A. McCoy, *Inside Job: The Assault on the Structure of the Consumer Financial Protection Bureau*, 103 MINN. L. REV. 2543, 2545 (2019).

[72] *See* Leonard Kennedy, Patricia A. McCoy & Ethan Bernstein, *The Consumer Financial Protection Bureau: Financial Regulation for the 21st Century*, 98 CORNELL L. REV. 1141, 1146–49 (2012) (describing the powers Congress bestowed upon the CFPB).

[73] John Kruzel & Harper Neidig, *The 7 Most Anticipated Supreme Court Decisions*, THE HILL (June 7, 2020, 12:00 PM), https://thehill.com/regulation/court-battles/501437-the-7-most-anticipated-supreme-court-decisions [https://perma.cc/5M36-5SCR].

[74] 140 S. Ct. 2183 (2020).

[75] *See* Richard Cordray, Opinion, *Why the CFPB's Loss at the Supreme Court Is Really a Win*, WASH. POST (June 29, 2020, 4:20 PM), https://www.washingtonpost.com/opinions/2020/06/29/why-cfpbs-loss-supreme-court-is-really-win/ [https://perma.cc/3WGU-DBH2].

[76] *Id.*

[77] *Id.*

[78] 140 S. Ct. at 2209.

[79] *See* Steven Harras, *Regulators Need to Help Banks Manage Fintech Risks, FDIC IG Says in Report*, CONG. Q. ROLL CALL, FEB. 27, 2019, 2019 WL 948553.

include the problem of consumers' fictional consent, liability issues, security risks, and even systemic risk, in addition to stifling innovation and anti-trust concerns.

Moreover, much like credit rating agencies prior to the 2008 financial crisis[80]—too important and influential of gatekeepers to be left untouched—more than a decade later, it is clear data aggregators, which collect, maintain, and share consumer financial data, have become too important to be left alone, and must be regulated by the relevant government agencies.[81]

II. CONSUMER FINANCIAL DATA

A. It's All About the Data

The concept of open banking aims to level the financial industry's playing field by offering a competitive advantage to FinTech companies, which otherwise might never compete with big banks.[82] In some parts of the world, like the EU, open banking initiatives are legally binding, and large banks must comply. In others, open banking initiatives result from market demands, and in particular, consumer demand for better, faster, and more user-friendly products and services, which are served by FinTech companies' offerings.[83] Either way, the trend pressures big banks into sharing their customers' information, and American banks have found themselves

---

[80] After the 2008 financial crisis, it became clear that there was a need for greater government regulation of rating agencies, especially given the conflicts of interest in their business model, which did not comply with appropriate due diligence standards. *See, e.g.*, Frank Partnoy, *How and Why Credit Rating Agencies Are Not Like Other Gatekeepers*, *in* FINANCIAL GATEKEEPERS: CAN THEY PROTECT INVESTORS? 59, 60–61 (Yasuyuki Fuchita & Robert E. Litan eds., 2006); Arthur R. Pinto, *Control and Responsibility of Credit Rating Agencies in the United States*, 54 AM. J. COMP. L. 341, 342–43 (2006).

[81] Indeed, according to a 2019 Basel Committee on Banking Supervision Report: "[w]ithin each jurisdiction, multiple authorities can have a role in addressing issues related to banks' sharing of customer-permissioned data with third parties owing to the multi-disciplinary aspects of open banking. Relevant authorities may include, for example, bank supervisors, competition authorities, and consumer protection authorities . . . . Given the variety of authorities involved and various mandates of these authorities, greater coordination may be needed." *See* BASEL COMM. ON BANKING SUPERVISION, *supra* note 58, at 5.

[82] Penny Crosman, *How APIs Are Being Used at Citi, BBVA and Other Leading Banks*, AM. BANKER (May 27, 2019, 10:00 PM), https://www.americanbanker.com/news/how-apis-are-being-used-at-citi-bbva-and-other-leading-banks [https://perma.cc/CPN3-2YBD].

[83] *See, e.g.*, Cheng-Yun Tsang, *From Industry Sandbox to Supervisory Control Box: Rethinking the Role of Regulators in the Era of FinTech*, 2019 U. ILL. J.L. TECH. & POL'Y 355, 358 (2019) ("In recent years, many jurisdictions are implementing the so-called 'open banking' policies to enable efficient customer data sharing between banks and payment service providers.").

needing to set up contracts with data aggregators such as Intuit, Plaid, Finicity, and Yodlee, that in turn share data with FinTech companies using APIs.[84]

Open banking, using APIs, began as an alternative[85] to the globally disliked practice of screen-scraping,[86] also known as "web scraping,"[87] in which a software automatically "contact[s] various Web sites and extract[s] relevant information."[88] In the context of banking, the term refers to a non-bank that offers products and services, and obtains bank customers' secure credentials.[89] The non-bank then uses

---

[84] *Id.* (detailing how banks and data aggregators use APIs); *see also* Alex Konrad, *Fintech Startup Plaid Is Now Valued at $2.65 Billion After $250 Million Raise*, FORBES (Dec. 11, 2018), https://www.forbes.com/sites/alexkonrad/2018/12/11/mary-meekers-first-post-kleiner-deal-fintech-startup-plaid-now-valued-at-265-billion/#3fc53c2977d6 [https://perma.cc/7CMU-UYC6]. Konrad explains:

> If you're a consumer who has signed up for apps like Acorns or Robinhood, there's a good chance you used Plaid without knowing it. At its most basic, Plaid helps developers embed a snippet of code within their apps that prompts you to input your banking info and then securely confirm it with the bank itself.

Id.

[85] *See Model Data Access Agreement*, *supra* note 60, at 1. The Clearing House advocated for a transition to APIs in order to enhance "safety and security of customer account data, [and] facilitate a consumer consent model focused on clarity and transparency of the data sharing process and enable future fintech innovation." *Id.*

[86] Scrapers have even been referred to, in one extreme case, as "a low lying snake belly scum sucking rat" who should be "quartered and hung . . . ." Tamburo v. Dworkin, 974 F. Supp. 2d 1199, 1210 (N.D. Ill. 2013).

[87] Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act,* 24 B.U. J. SCI. & TECH. L. 372, 381 (2018) ("Courts have struggled to settle on a common terminology for web scraping, let alone what types of activity should meet the definition.").

[88] Shea *ex rel.* American Reporter v. Reno, 930 F. Supp. 916, 929 (S.D.N.Y. 1996) (the first decision to define a web scraper). A more detailed definition comes from the First Circuit in the 2003 scraping case EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 60 (1st Cir. 2003):

> A scraper, also called a "robot" or "bot," is nothing more than a computer program that accesses information contained in a succession of webpages stored on the accessed computer. Strictly speaking, the accessed information is not the graphical interface seen by the user but rather the HTML source code — available to anyone who views the site—that generates the graphical interface. This information is then downloaded to the user's computer.

Id.

[89] Lael Brainard, Governor, Fed. Rsrv. Bd., at the Northwestern Kellogg Public-Private Interface Conference on New Developments in Consumer Finance: Research & Practice: Where Do Banks Fit in the Fintech Stack? 10 (Apr. 28, 2017), https://www.federalreserve.gov/newsevents/speech/brainard20170428a.htm [https://perma.cc/V6HZ-NTMZ]. Brainard explains:

the credentials to access the customers' bank accounts and takes their financial data, which it saves in an app.

B. Keeping Up with Customer Expectations: Faster & Cheaper

Studies have shown that customer satisfaction is the key to corporate success.[90] Consumers' expectations and demands from their service providers are constantly changing as the bar keeps rising in our fast-paced technology-dependent era. Like other types of services, consumers want and expect speed in financial services.[91] For example, if a digital banking app cannot do something consumers want when it is needed, or if, even one time, customers cannot easily access or login to the app, they might abandon the app.[92] Likewise, lowering costs is also important. When surveyed, consumers indicated they wanted the innovation of FinTech when dealing with financial service providers, but they also wanted the data security and privacy offered by traditional banks.[93] In particular, consumers wanted to share, manage, and control their financial data, but two-thirds of the surveyed users expressed concerns about data privacy and sharing.[94] Therefore, a critical question is how can

---

> 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 . . . 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.

Id.

[90] *See* Andre Schwager & Chris Meyer, *Understanding Customer Experience*, HARV. BUS. REV. (Feb. 2007), https://hbr.org/2007/02/understanding-customer-experience [https://perma.cc/KQ4H-2TPJ].

[91] Mark Smedley, *Why the Future of Banking Is 'Open,'* WALL ST. J. (Jan. 11, 2018), https://partners.wsj.com/oracle/future-banking-open/ [https://perma.cc/G88N-BQ52] ("Customers now expect their financial providers to offer more than just transactional services. Rather, they want innovations that help them manage their financial matters conveniently and securely from any device.").

[92] *See* Ruby Hinchliffe, *Nationwide Exec: Banks Can't Do Everything*, FINTECH FUTURES (Oct. 4, 2019), https://www.fintechfutures.com/2019/10/nationwide-exec-banks-cant-do-everything [https://perma.cc/34Q5-FT9E].

[93] Press Release, The Clearing House, The Clearing House Supports Financial Data Exchange Work on API Technical Standards (Oct. 18, 2018), https://www.theclearinghouse.org/payment-systems/articles/2018/10/data-privacy-10-18-2018 [https://perma.cc/3P36-V4RG].

[94] *Id*.

we safely reach open banking goals while keeping in mind the key pillars of financial regulation—prudential regulation and consumer protection?[95]

Technology companies are subject to far less regulation than traditional financial institutions, and that advantage enables FinTech companies to offer consumers faster and cheaper services and products.[96] In return, consumers' demands for these services and products have increasingly pushed more technology companies to operate in the financial service landscape. As a recent *TechCrunch* article title stated, "[e]very startup is a bank—or wants to be."[97] Illustrating this sentiment, the CEO of Citibank in an annual bankers' conference in 2019 recalled "meeting a young Silicon Valley entrepreneur several years ago" that looked at him "and pretty much said, 'We've come to eat your lunch, old man.'"[98]

C. Data Aggregators

Joining the FinTech revolution, "data aggregators"—entities that "access, aggregate, share, and store consumer financial account and transaction data they acquire through connections to financial services companies,"[99]—have become key financial industry players. These companies

> 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.[100]

---

[95] *See, e.g.*, Ruth Plato-Shinar, *Financial Consumer Protection in the Post Financial Crisis Era: Can the American CFPB Serve as a Model for Other Jurisdictions?*, 54 TEX. INT'L L.J. 171, 172 (2019).

[96] *See* Kristin Johnson, Frank Pasquale & Jennifer Chapman, *Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation*, 88 FORDHAM L. REV. 499, 505 (2019) (discussing the gaps in the supervision of FinTech companies and how that encourages them to engage in regulatory arbitrage).

[97] Alex Wilhelm & Kate Clark, *Every Startup Is a Bank—or Wants to Be*, TECHCRUNCH (Nov. 8, 2019, 7:00 AM), https://techcrunch.com/2019/11/08/every-startup-is-a-bank-or-wants-to-be/ [https://perma.cc/89BJ-DUF5]; *accord* Alex Wilhelm & Natasha Mascarenhas, *Why Is Every Startup a Bank These Days?*, CRUNCHBASE (Oct. 30, 2019), https://news.crunchbase.com/news/why-is-every-startup-a-bank-these-days/ [https://perma.cc/BC86-HNMF].

[98] Brendan Pedersen, *Citi's Corbat Warns Banks: Don't Become 'the Dumb Utility*,*'* AM. BANKER (Nov. 20, 2019, 6:21 PM), https://www.americanbanker.com/news/citigroups-corbat-warns-banks-dont-become-the-dumb-utility [https://perma.cc/6K6L-UE43].

[99] 2018 Treasury Report, *supra* note 52, at 23–24.

[100] *Id*.

In the U.S., there are several major data aggregators[101] and the scope and sophistication of their services ranges.[102] Some data aggregators mainly aggregate financial account balances, transactions data, or credit card activity. Others support FinTech app providers that offer certain types of products, such as student loans or services like fees payment monitoring.[103]

Data aggregators make data available by providing a platform through which FinTech companies interface with consumers. They make it easier for FinTech companies to operate. There are only a few major data aggregators versus thousands of financial institutions, and data aggregators have usually sunk the costs of connecting to financial institutions, so FinTech companies can focus solely on designing products or services to the aggregators' specifications rather than thousands of banks.[104]

But, prior to starting interfaces with FinTech companies, data aggregators gain access to consumers' information directly from the bank. The aggregators then attempt to put the consumers' financial information under one roof—the consumer's "dashboard"[105]—which exhibits one's "investments, savings, insurance policies, and credit balances."[106] Additionally, a dashboard can include services like tax planning, budgeting, data on home value or mortgage, and more inclusive, costly services, like portfolio analysis, financial advice, auto bill-payments, and credit monitoring.[107]

Data aggregators can also track data from non-financial entities and add data from external financial accounts to existing financial providers like a bank. Either way, data aggregation happens and is typically done via screen-scraping or APIs.[108]

---

[101] *See* MX Technologies Inc., *supra* note 34.

[102] *See generally* Michael Kitces, *The Six Levels of Account Aggregation #FinTech and PFM Portals for Financial Advisors*, KITCES (Oct. 9, 2017, 7:01 AM), https://www.kitces.com/blog/six-levels-account-aggregation-pfm-fintech-solutions-accounts-advice-automation/ [https://perma.cc/A7LZ-ZGBH] (describing the evolution of the data aggregation services).

[103] *Id.*

[104] *Id.*

[105] *Potential Benefits and Risks of the Increased Use of Data in Financial Services Applications: Hearing Before the S. Comm. on Banking, Hous. & Urb. Affs.*, 115th Cong. 2 (2018) (statement of Brian Knight, Dir., Innovation & Governance Program, Mercatus Ctr. at George Mason Univ.), https://www.banking.senate.gov/imo/media/doc/Knight%20Testimony%209-18-18.pdf [https://perma.cc/X8Q6-TGFZ] ("Third-party aggregators, acting on a consumer's behalf, can now allow consumers to see all of their accounts from different financial services providers at a glance. This convenient display of information can help consumers more effectively assess and manage their finances.").

[106] *Know Before You Share*, *supra* note 32.

[107] *Id*.

[108] 2018 Treasury Report, *supra* note 52, at 25–26.

1. Screen-scraping

If data aggregators and FinTech app providers do not have a direct connection to operate FinTech apps using data stored at financial services companies, they usually screen-scrape. When screen-scraping, consumers provide their full account login credentials—usernames and passwords—to use FinTech apps.[109] In particular, consumers' secure login credentials enable data aggregators to "scrape" data on a daily basis. Scraping is done manually or through automated processes, which entails a code that reaches out to third-party websites, connects using the consumers' security credentials, gets the relevant account information, and if needed, executes transactions.[110] While this process makes screen-scraping an effective method of obtaining data, it also creates significant vulnerabilities and security-related drawbacks. For example, one significant drawback is that banks are often not aware when their customers' data is being screen-scraped.[111]

Additionally, consumers do not understand the consequences of giving their credentials to a third-party rather than logging in directly to their own financial services company.[112] There is a growing disconnect between consumers' perceptions of and knowledge about financial data collection practices. Specifically, 70% of surveyed consumers who use financial apps were confident their banking information was private and secure, but (i) 80% were not fully aware that the apps they use, or the third-parties associated with their apps, may store their bank account username and password; and (ii) only 21% were aware that financial apps have access to their data until they revoke permissions.[113] Similarly, normalizing the practice of sharing banking login credentials exposes consumers to various risks. First, fraudsters pretending to be data aggregators can potentially trick and deceive consumers. Second, hackers can attempt to break into data aggregators' systems and steal consumers' login credentials. Third, rogue employees working for data aggregators can easily abuse access to the accounts and financial data.[114] Lastly, if allowing screen-scraping as a commonly used method continues, regulators will be unable to require banks to stiffen up authentication by requiring certain types of multifactor authentication, such as biometrics.[115]

---

[109] Screen-scraping is not a recent development. As far back as 2001, regulators identified the practice of sharing consumer login credentials for data aggregation services as raising additional risks. *See* OFF. OF THE COMPTROLLER OF THE CURRENCY, OCC BULL. 2001-12, BANK-PROVIDED ACCOUNT AGGREGATION SERVICES: GUIDANCE TO BANKS (2001), https://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-12.html [https://perma.cc/PUL6-F9YU]; FED. FIN. INSTS. EXAMINATION COUNCIL, E-BANKING, IT EXAMINATION HANDBOOK D-1 (2003), https://ithandbook.ffiec.gov/media/274777/ffiec_itbooklet_e-banking.pdf [https://perma.cc/VM2V-N9G4].

[110] *Know Before You Share*, *supra* note 32.

[111] 2018 Treasury Report, *supra* note 52, at 25–26.

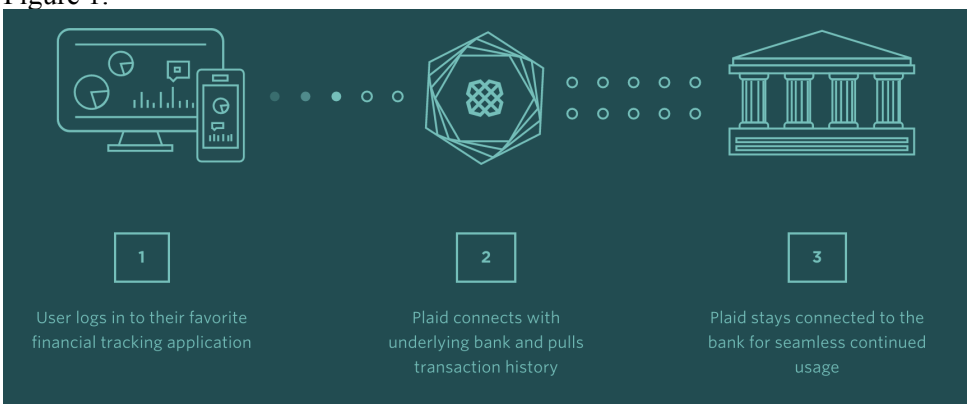
[112] *See* CONSUMER SURVEY, *supra* note 37, at 5.

[113] *Id*. at 3–6.

[114] *See* Crosman, *Data-Sharing Debate*, *supra* note 35.

[115] *Id*.

Figure 1.



The above image shows how information sharing works when conducted using Plaid as a middleman.[116]

2. APIs

Using APIs is another way to access consumer financial data because APIs grant direct feed.[117] APIs are codes that connect two or more systems, and enables clearly-stated communications and information exchange between the connected systems to operate apps and various types of software.[118] Essentially, APIs are a technology-enabled agreement—almost a contract of sort—that empowers computer systems or data sources to work with or be used by a different software. Unlike screen-scraping, data aggregations that rely upon APIs typically entail parties to a certain agreement because the entities chose to partake in data sharing.[119] Hence, financial services providers can potentially use APIs to enable the inclusion of vigorous security features, as well as "greater transparency and access controls for consumers," stronger focus on data accuracy, and more reliable and affordable data technology costs.[120]

---

[116] Gordon Wintrob, *How Plaid's API Brings Finance into the 21st Century*, GET PUT POST (Mar. 15, 2016), https://getputpost.co/how-plaid-s-api-brings-finance-into-the-21st-century-efc174028f09 [https://perma.cc/2AHM-3XA3].

[117] 2018 Treasury Report, *supra* note 52, at 26, n.47.

[118] *Id.* ("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.").

[119] *Id.*

[120] *Id.*

While APIs are becoming more common,[121] their development can be pricey, which means smaller banks with fewer resources might not utilize them.[122] APIs can be created to be open or restricted to specifically designated partners.[123] This design choice gives banks executing APIs too much power: in an Open API system, any third-party data aggregator or FinTech app provider that meets specific standards agreed upon in advance can access consumer financial data and build consumer-facing apps. Differently, a restricted API system, which is often referred to as a Partnered API system, is based on limited, two-sided agreements between banks and data aggregators or FinTech app providers.[124]

---

[121] *Cf.* Ron Shevlin, *Open Banking Won't Work in the U.S.*, FORBES (Apr. 15, 2019), https://www.forbes.com/sites/ronshevlin/2019/04/15/open-banking-wont-work-in-us/#718b1f3f1e52 [https://perma.cc/E43F-37SV] ("Achieving scale requires a platform (like an Amazon or Goldman) who can integrate many providers . . . . Being able to create a technology platform to do this has been beyond the reach of most banks and credit unions.").

[122] *See* BASEL COMM. ON BANKING SUPERVISION, *supra* note 58, at 6. The Committee determined:

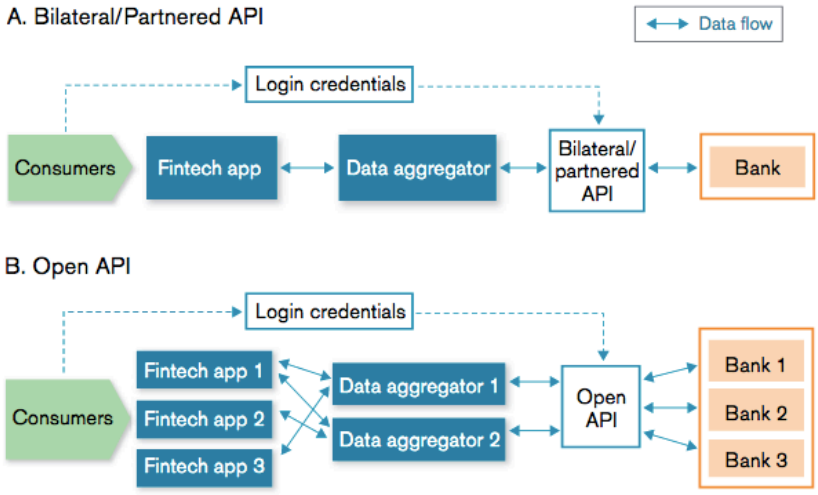
> [S]ome challenges associated with the universal use of APIs remain. The time and cost to build and maintain APIs (particularly when done on a bilateral basis with multiple organisations), the lack of commonly accepted API standards in some jurisdictions, and the economic cost for smaller banks to develop and adopt APIs have been cited as challenges.

Id.

[123] 2018 Treasury Report, *supra* note 52, at 26.

[124] *Id*. at 27.

Figure 2.



The above graph shows how information sharing works when conducted using a Partnered API system vs. an Open API system.[125]

Consumers must give consent to either the banks or the API access point in open and restricted API systems. In contrast, under the screen-scraping data sharing method, consumers must share their login credentials.

3. Improving Data Aggregation

In recent years there seems to be a growing understanding that consumers should have dependable and secure access to their data and that they should utilize FinTech apps, if desired.[126] But "there is a lack of consensus on what secure and reliable access" to consumers' financial data should entail.[127] Therefore, "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."[128] Meanwhile, consumers are stuck in the middle of the debate, suffering from consequences ranging from banks choking off data to exposing consumers to privacy and security risks, of which they might not be aware.[129]

---

[125] *Id.* at 26–27.

[126] *Id*. at 27.

[127] *Id*.

[128] Bob Hedges, *Banking Perspectives: Consumer Data in an API-Enabled World*, THE CLEARING HOUSE, https://www.theclearinghouse.org/banking-perspectives/2017/2017-q4-banking-perspectives/articles/open-banking [https://perma.cc/9B2T-8QWX] (last visited July 7, 2020).

[129] 2018 Treasury Report, *supra* note 52, at 27.

Acknowledging some of these dangers, FINRA published a strongly worded warning in 2018 addressing the risks associated with sharing account data with data aggregators. [130] The risks "include potential vulnerability to cyber fraud, unauthorized transactions, and identity theft. A key risk is that the aggregators could be storing *all* consumer financial information or security credentials in one place, creating a new and heightened security risk for consumers."[131] FINRA's warning is important. Data aggregators are trusted with access to investors' financial accounts but are not regulated like financial institutions.[132] They collect, store, and maintain data as they see fit while relying on cloud services such as Amazon Web Services.[133]

Data aggregators are hardly the only ones relying on cloud services. All major industries and government agencies do the same, but this reliance has largely been ignored in the context of cybersecurity risks.[134] Yet, such risks become very relevant when dealing with massive amounts of aggregated personal information. Moreover, not being regulated like banks means that if data aggregators are compromised in a breach, or if FinTech apps have exploitable vulnerabilities, then the login credentials of accounts, including traditional bank accounts, could be jeopardized.

---

[130] *See* Crosman, *Finra's Dire Warning*, *supra* note 36.

[131] *Know Before You Share*, *supra* note 32.

[132] *See* Crosman, *Finra's Dire Warning*, *supra* note 36. However, commenting on the issue of regulation, some believe that if the data is "encrypted, tokenized and split across multiple regions in Amazon Web Services . . . [t]here's no way to pull a single transaction . . . or . . . routing number and connect it to an individual." *Id.* (quotations omitted). Similarly, a spokeswoman for one of the biggest data aggregators, Envestnet|Yodlee, said Yodlee:

> Adheres to, and in many cases exceeds, the security and risk management standards required to engage with consumers and their financial data. Yodlee is supervised and examined by the [Office of the Comptroller of the Currency] and all major regulators, including nearly 200 individual audits by financial institutions over a recent 24-month period.

Id. (quotations omitted). Similarly, the CEO of Finicity stated that he "does not see a need for data aggregators to go through the same regulatory scrutiny as banks . . . . I'm not holding assets, I'm a service provider. I'm not a bank . . . . It's a little cavalier to say aggregators need to be held to the same regulatory standard." *Id.* (quotations omitted).

[133] *Id*. (describing how a data aggregator executive argued that data is clearly safer with the aggregator since it is a professional organization that logs in through secure methods than with individuals who "[log] in from an unsecure Wi-Fi network in a coffee shop").

[134] *See generally* Nizan Geslevich Packin, *Too-Big-to-Fail 2.0? Digital Service Providers as Cyber-Social Systems*, 93 IND. L.J. 1211 (2018) (elaborating on the need for greater security in critical digital services). Any potential harm can be massive in terms of privacy and financial loss. "For example, according to estimates, a recent four-hour outage of Amazon's S3 cloud storage system that was not the result of a cyberattack, cost S&P 500 companies at least $150 million. Accordingly, losses resulting from a large-scale attack on a cloud service are estimated in the billions." *Id.* at 1236.

If customers' credentials are jeopardized, they would be exposed to data and financial losses with very limited, if any, legal recourse.[135] Similarly, focusing on the issue of credential sharing, banks have maintained that if consumers share their credentials with third-parties and fraud takes place, liability protections like Regulation E—establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer systems[136]—will not be available for consumers.[137] The issue, however, is broader than just credential sharing. Any time information is shared with a third-party, that information can be compromised with the level of risk depending on the type of information being shared and the method used to share the information.[138]

However, industry participants believe that the most dangerous type of data sharing is done via screen-scraping because after consumers share login information, data aggregators extract transaction information to populate their services and store and maintain the credentials, sometimes even after the relationship with the consumer ends.[139] But what is worse is that consumers frequently forget sharing their login information and delete the apps for which they shared their data. Yet, data aggregators continue to pull data from the often unsuspecting banking sites.[140] Furthermore, even when banks suspect such activities, screen-scraping interferes

---

[135] *See* Crosman, *Finra's Dire Warning*, *supra* note 36.

[136] 12 C.F.R. §§ 205.1–205.20 (2020). Regulation E implements the Electronic Fund Transfer Act, which creates a framework that defines rights, liabilities, and obligations of participants in the electronic fund and remittance transfer systems. *Id.*

[137] Moreover, the banks "face ambiguity and uncertainty as to the applicability of certain privacy rules, the Bank Secrecy Act provisions and regulations, and Anti-Money Laundering standards." COUNCIL OF INSPECTORS GEN. ON FIN. OVERSIGHT, TOP MANAGEMENT AND PERFORMANCE CHALLENGES FACING FINANCIAL-SECTOR REGULATORY ORGANIZATIONS 6 (2019), https://www.sec.gov/files/CIGFO-TMPC-Report-July-2019.pdf [https://perma.cc/Z5CR-T5LV].

[138] *See* Crosman, *Finra's Dire Warning*, *supra* note 36.

[139] *See* Natalie S. Talpas, Senior Vice President and Digit. Prod. Mgmt. Grp. Manager, PNC Bank, Statement at the Consumer Financial Protection Bureau Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act 5 (Feb. 26, 2020), https://files.consumerfinance.gov/f/documents/cfpb_talpas-statement_symposium-consumer-access-financial-records.pdf [https://perma.cc/48DV-JLXV]. Talpas concludes:

> Most consumers also do not realize that the aggregator may continue to obtain this information even if the consumer stops using or deletes the financial app. Rather, to cease the aggregator's collection of information, the consumer must affirmatively revoke the authorization provided to the aggregator. However, the means of doing so often are not clear or easy.

Id.

[140] *Id*.

with their ability to create vigorous risk-based profiles of the banks' users since data aggregators can login from different locations at different times through codes.[141]

In May 2020, a group of consumers focused on some of these challenging data sharing issues and filed a class action against Plaid.[142] The complaint raised causes of action based on: invasion of privacy; the Computer Fraud and Abuse Act; the Stored Communications Act; unjust enrichment; California Business and Professions Code Section 17200; Article I, Section I of the California Constitution; the Anti-Phishing Act of 2005; California Civil Code Sections 1709 and 1710; and California's Comprehensive Data Access and Fraud Act.[143]

According to the complaint, "Plaid's software is used by more than 2,000 apps to link consumer financial accounts, and about 1 in 4 people in the U.S. have an account linked via Plaid . . . ."[144] The complaint alleged that "Plaid uses that access to deceptively obtain bank account information from users, accessing information back up to five years, averaging 3,700 transactions per consumer . . . ."[145] In addition, Plaid "allegedly gathers information on accounts maintained for others such as relatives and children, and has amassed data from over 200 million distinct financial accounts."[146] Allegedly,

> [W]hen a user enters their bank login information on an app that uses Plaid, the credentials, including security layers such as security questions and answers and one-time passwords, are transmitted directly to Plaid, rather than to the bank. Plaid then uses that information to access the consumer's bank account multiple times a day, gathering private information and then selling it . . . .[147]

---

[141] *Id*. at 6–8. Responding to this argument, data aggregators have claimed that they can

> [G]ive banks all the IP addresses they'll communicate from ahead of time, so the bank can identify them as they come in[] . . . [and disagreed with the notion] that banks' servers can't handle the traffic from data aggregators. [Bill Harris, CEO of the financial planning app provider Personal Capital, said,] [i]n 2017, we have massively scalable computers[.] . . . Google handles 40,000 data requests per second. There is so much available from relatively small machines at a relatively low price. For anybody who knows how to spell IT, handling these kinds of volumes is nothing.

Crosman, *Data-Sharing Debate*, *supra* note 35.

[142] Complaint at 1–2, Cottle v. Plaid Inc., No. 4:20-cv-03056-DMR (N.D. Cal. May 4, 2020).

[143] *Id.*; Maeve Allsup, *App Users Say Plaid Collects Bank Logins Without Consent (1)*, BLOOMBERG L. (May 5, 2020, 5:16 PM), https://news.bloomberglaw.com/class-action/app-users-say-plaid-collects-bank-logins-without-consent [https://perma.cc/QA4C-4YLE].

[144] Allsup, *supra* note 143.

[145] *Id.*

[146] *Id.*

[147] *Id.*

The complaint further claims that if Plaid "would be acquired by Visa in a $5.3 billion deal that would give Visa access to Plaid's data," that such a deal would be yet "another example of Plaid selling consumer data without consent . . . ."[148] According to the allegations, all consumers see is a login screen with their banks' logos, but that screen is operated by Plaid, which misrepresents the situation for users, who are not presented with adequate privacy policies or terms of use.[149]

Accordingly, data aggregators, FinTech app providers, and U.S. banks are searching for better approaches to data aggregation. The use of APIs instead of screen-scraping has obvious advantages,[150] thereby leading to the development of a middle-ground solution, in which data aggregators implement APIs that banks currently use and leverage to populate their sites.[151]

But using the API method for handling data has certain limitations that can result in parties resorting to screen-scraping.[152] First, while some data aggregators have entered into mutual agreements to access data using an API, this approach can prove challenging to scale considering just how many financial institutions operate

---

[148] *Id.* Note, however, that based on its recently filed complaint against Visa, the DOJ believes that the main reason to stop Visa's acquisition of Plaid relates to antitrust issues. Complaint, USA v. Visa Inc., 4:20-cv-07810 (N.D. Cal. Nov. 5, 2020). Particularly, according to the recently filed DOJ lawsuit, Visa is a rich and powerful monopolist that has led the online debit market field for years, holding approximately 70% of the market. *Id.* at 8. Barriers to entry combined with "Visa's long-term, restrictive contracts with banks, are nearly insurmountable, meaning Visa rarely faces any significant threats to its online debit monopoly." *Id.* at 3. The DOJ lawsuit claims that when Visa realized how Plaid—a provider of services that enable consumers and merchants to transact, as it supports and connects thousands of FinTech apps, with more than 11,000 domestic financial institutions, and over 200 million consumer bank accounts—could meaningfully compete with Visa, it decided to take action and buy Plaid. *Id.* at 3–4. The DOJ further argues that the acquisition would result in higher prices for online debit transactions, less innovation, and would raise competitors' barriers to entry. *Id.* at 2–3.

[149] Allsup, *supra* note 143 ("A login screen with your bank's branding is actually controlled by and connected to Plaid, the suit says, which uses bank logos to provide a false sense of comfort for users. Additionally, the privacy policy is not meaningfully presented to users, the suit claims.").

[150] *See Increase Customers' Control*, *supra* note 61. Envestnet|Yodlee, one of the biggest data aggregators, explained that their

> partnership with Chase will allow further consumer choice, reliability, and insight into how and where their data is being used, along with improved overall financial well-being . . . . [T]he secure API uses a token-based approach, [and] customers will no longer need to give out their username and password—confidential credentials that should always be treated with the utmost care.

Id.

[151] *Id*.

[152] 2018 Treasury Report, *supra* note 52, at 27–28.

in the U.S.[153] Second, access to data via APIs is usually one-sidedly limited, controlled, interrupted, or terminated by financial institutions.[154] APIs are simply gateways that allow developers to integrate transaction and account data from banks into third-party apps and restrict how much and how often apps can tap information while also contractually limiting what they can do with it later.[155] As such, data aggregators and FinTech companies claim that financial institutions largely refuse to enable direct access to their data or to set up truly open APIs.[156] They argue that without some sort of regulatory guidance, API access would be limited to specific types of information dictated by financial institutions, as opposed to consumers, and could be subject to unreasonable and disproportionate liability.[157] Lastly, APIs can serve as a gateway to the data center by which attackers can efficiently attack the backend via bots and compromised or impersonating applications.[158] Application

---

[153] *Id.* at 27.

[154] *See* Sidel, *supra* note 23.

[155] API contracts outline the "terms and conditions" of the service, mandate how the relevant APIs can be used by third-party developers, and include details about their structure, guarantees and limitations. *See* Markos Zachariadis & Pinar Ozcan, *The API Economy and Digital Transformation in Financial Services: The Case of Open Banking* 8 (SWIFT Inst. Working Paper No. 2016-001, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975199 [https://perma.cc/SN7C-QSH2].

[156] *See, e.g.*, DANIEL CASTRO & MICHAEL STEINBERG, CTR. FOR DATA INNOVATION, BLOCKED: WHY SOME COMPANIES RESTRICT DATA ACCESS TO REDUCE COMPETITION AND HOW OPEN APIS CAN HELP 2 (Nov. 6, 2017), http://www2.datainnovation.org/2017-open-apis.pdf [https://perma.cc/7C2R-9MD7].

[157] 2018 Treasury Report, *supra* note 52, at 34.

[158] Rusty Carter, *APIs: The Trojan Horses of Security*, HELP NET SECURITY (Sept. 10, 2018), https://www.helpnetsecurity.com/2018/09/10/api-insecurity/ [https://perma.cc/UW7G-FZX9]. Carter claims

> published apps can provide a roadmap for an attacker to target APIs and, as a result, a backend data centre . . . . Cybercriminals have realised that API calls that originate from inside an app are a blueprint for the infrastructure inside a data centre. What's worse, they can use those same API calls to hide their malicious purposes – like a Trojan horse gaining access through the front door. . . . [S]ophisticated attackers will focus their efforts on targeting a single application. By compromising web or mobile apps they can emulate the behaviour of an unmodified application to establish a baseline of legitimate access to the backend. This pattern of behaviour can then be widened to slowly exfiltrate data over time and find subtle violations of the data access control, often using methods that the "normal" application already uses — rendering noisy, detectable exploits unnecessary. These seemingly innocuous requests essentially become the attacker's most effective tool . . . . Less sophisticated attackers try to compromise app APIs by simply injecting malicious content into API request fields. This is a relatively low-effort method to uncover vulnerabilities when the requests are processed . . . . More savvy attackers, however, are able to target a single app by taking a more sophisticated approach, which is designed to circumvent both WAF

endpoints are highly vulnerable and "are becoming more attractive to attackers due to [banks] using [them] to make things easier and more convenient for their customers."[159]

Attempting to solve these limitations, different players from across the data aggregation ecosystem collaborate to create open APIs that serve the needs of all industry participants.[160] For example, in May 2020, Plaid, which originally catered to FinTech companies' needs, changed course following Visa's announcement of Plaid's purchase and the Coronavirus crisis that made many of its FinTech customers unsuccessful or try to pivot, and launched Plaid Exchange prioritizing banks' interests.[161] Plaid Exchange, in which banks call the shots regarding data-sharing efforts, is

---

> and RASP security methods. They can establish a baseline of legitimate backend access by mimicking the behaviour of unmodified applications.

Id.

[159] *Id*.

[160] An example includes the Open Financial Exchange ("OFX") Consortium, which started in 1997. *See* Press Release, OFX Consortium, OFX 2.2 Released with OAuth-Token Based Authentication (Apr. 7, 2016, 12:30 PM), https://www.businesswire.com/news/home/20160407006078/en/OFX-2.2-Released-OAuth-Token-based-Authentication [https://perma.cc/6K8P-6JB3]. The OFX specification is a unique standard for the exchange of financial data between financial institutions and consumers. *Id.* In April 2016, the OFX Consortium released OFX 2.2, containing new standards such as data tags and tokenized authentication solutions for exchanges of data. *Id.* In 2017, JPMorgan Chase also came to an agreement with Intuit, using a read-only API that was based on the OFX 2.2 standard and tokenizing authentication using OAuth 2.0, which banks such as Wells Fargo use as well. *See* Crosman, *Data-Sharing Debate*, *supra* note 35. In the banks' opinion,

> "The most important part of this is giving control to the customer," JPMorgan's Dimon said in a press release announcing the Intuit partnership. The use of the OAuth standard means each third party will have a different "token" that allows them to read data from a user's account. Users can set those tokens to expire or delete, or modify them through the bank website.

Id. Similarly, the Aggregation Services Working Group of the Financial Services Information Sharing and Analysis Center ("FS-ISAC"), which includes representatives from all relevant stakeholders of the financial industry, launched a new version of its API for secure, tokenized data transfer. *See* Warwick Ashford, *FS-ISAC Enables Safer Financial Data Sharing with API*, COMPUTERWEEKLY.COM (Feb. 13, 2018), https://www.computerweekly.com/news/252434931/FS-ISAC-enables-safer-financial-data-sharing-with-API [https://perma.cc/Z2AE-8GRA].

[161] Ron Shevlin, *Plaid Launches API Exchange to Accelerate Open Banking and Digital Transformation*, FORBES (May 19, 2020, 8:00 AM), https://www.forbes.com/sites/ronshevlin/2020/05/19/visas-plaid-launches-api-exchange-to-accelerate-open-banking-and-digital-transformation/#7f02ff7c2b37 [https://perma.cc/U9NX-9N5M] [hereinafter Shevlin, *Plaid Launches API Exchange*] ("Plaid's core customer base—fintechs—are hurting because

> a bank product that will enable banks to expose APIs to a range of trusted fintech developers. Banks that utilize Plaid Exchange will also gain visibility into which 3rd parties have access to customer accounts and be able to communicate that to the customer and turn connectivity on and off.[162]

This enables Plaid, as the data aggregator and the middleman, to identify and control access from FinTech companies. The biggest American banks, like JPMorgan Chase or Wells Fargo, have already created direct access paths for major data aggregators or created their own APIs.[163] In contrast, small banks have not followed the big banks because they typically lack the resources needed to develop their own APIs.[164] According to Plaid, "[t]he real shift here is this is standardized, almost open-finance-in-a-box. It's built around an API core and we can implement it at scale with any bank that wants it."[165] Standardizing is important. Open banking is based on common standards and definitions that make data sharing usable, and that can happen if Plaid Exchange serves as a platform, as displayed in the image below.

---

of the COVID-19 crisis. Fintech lenders have been hit hard with loan defaults, while challenger banks are suffering from reduced payments volume.").

[162] *See* Sloane, *supra* note 43. Sloane notes

> Banks that choose to work with Plaid to build their API would then have a modern token-based system for their customers. For instance, just like on a social network, customers would be able to see if they have connected their bank account with a third-party service and disable those connections. Financial institutions could also leverage Plaid Exchange to build new services that connect directly with your main bank account through the API. Companies would be able to see if connections are working fine, which would make it much easier to identify issues with the infrastructure.

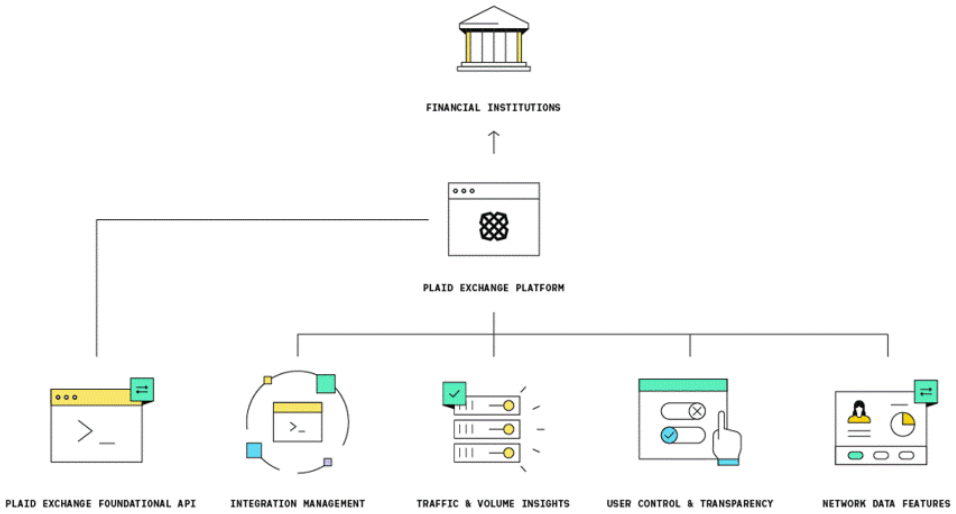
Id.

[163] *See* Penny Crosman, *Plaid Launches Exchange to Help Banks Share Data with Fintechs*, AM. BANKER (May 19, 2020 12:32 PM), https://www.americanbanker.com/news/plaid-launches-exchange-to-help-banks-share-data-with-fintechs [https://perma.cc/2PN4-QMXB] [hereinafter Crosman, *Plaid Launches Exchange*].

[164] *Id.*

[165] *Id*.

Figure 3.



Plaid Exchange Platform[166]

Likewise, trade groups are starting to shape their views into developed principles with respect to data aggregation.[167] After all, APIs are viewed as a way to allow for innovation to thrive while providing more security by using data aggregators as intermediaries.[168]

This API-based compromise solution seems to strike a delicate balance. Still some FinTech companies do not want to work with existing APIs, criticizing them

---

[166] Niko Karvounis & Jesse Dhillon, *Introducing Plaid Exchange*, PLAID BLOG (May 20, 2020), https://blog.plaid.com/introducing-plaid-exchange/ [https://perma.cc/H9DS-D4WB].

[167] *See, e.g.*, SEC. INDUS. & FIN. MKTS. ASS'N, SIFMA DATA AGGREGATION PRINCIPLES 1 (2018), https://www.sifma.org/wp-content/uploads/2018/04/sifma-Data-Aggregation-Principles.pdf [https://perma.cc/7ZUU-DHPG] (affirming that consumers can "use third-parties to access their financial account data" and "such access should be safe and secure"). *See also* Ron Barasch, *Yodlee, Quovo and Morningstar ByAllAccounts: Statement of Joint Principles for Ensuring Consumer Access to Financial Data*, ENVESTNET|YODLEE (May 11, 2018), https://www.yodlee.com/blog/envestnet-yodlee-quovo-and-morningstar-byallaccounts-statement-of-joint-principles-for-ensuring-consumer-access-to-financial-data/ [https://perma.cc/5LYH-QQMP] (suggesting a Secure Open Data Access framework that consists of the following elements: (i) consumers should be able to access their financial data for any legitimate app use; (ii) consumers have to provide affirmative consent in connection with the use of their data; (iii) all parties that deal with consumer data must comply with the best practices for security standards and transparency; and (iv) the party liable for a consumer's financial loss has to compensate the consumer).

[168] *See* CASTRO & STEINBERG, *supra* note 156, at 10–11.

as hurting innovation by offering too little, too slowly.[169] Such FinTech companies have not been waiting idly by for banks to reduce API access or pull the plug on data entirely. They have instead actively worked on high-tech ways to outsmart and outmaneuver banks' blocking technology.[170] They have also extended the fight beyond technological innovation and into Washington, lobbying for open banking. They argue that open banking means that consumers are the owners of their data and decide how—and if—they share it with third-parties.[171] FinTech companies want their apps to ask consumers for permission to access their accounts and require banks to abide by that consent and allow their apps to access and manage the data.[172]

D. Current Legal Landscape

Ideally, many U.S. banks would prefer to block FinTech companies' servers from accessing customer data. Banks believe FinTech apps collect more data than needed, save it in an unsafe way, and sell it to third-parties—all practices that can

---

[169] Discussing the early days of APIs, the advantage of platforms that use them, and the network effects that could be generated by this, Peter Menell wrote that

> The ability to control interfaces through intellectual property protection, technological protections (such as digital rights management), and contracts became a major part of these industries. Having innovative, competitively-priced products continued to be important, but establishing and building a successful software-based platform became the key to success. Companies could use API strategies to lock in consumers and lock out competitors. . . . Other computer companies used API strategies to control access to their video game platforms, cell phone networks, replacement parts (such as ink cartridges for printers), and graphical user interfaces. The contours of intellectual property rules governing interoperability strategies . . . became a major battleground.

Peter S. Menell, *Rise of the API Copyright Dead: An Updated Epitaph for Copyright Protection of Network and Functional Features of Computer Software*, 31 HARV. J.L. & TECH. 305, 318–19 (2018) (footnotes omitted).

[170] Banks notice these maneuvering attempts. For example, PNC started blocking data aggregators from accessing its clients' accounts after identifying "multiple different aggregators" trying to bypass its security protocol. *See* Hayashi, *supra* note 26 (quotation omitted).

[171] *See*, for example, the advocacy efforts of the Financial Data and Technology Association ("FDATA"), a global association of FinTech companies, which has been coordinating the campaign for delivery of Open Banking across the globe since 2018, at FIN. DATA & TECH. ASS'N, https://fdata.global/ [https://perma.cc/BQ53-7XXX] (last visited July 7, 2020). *See also FDATA North America Mission Statement*, FDATA, https://fdata.global/north-america/ [https://perma.cc/FCT2-QUPS] (last visited Oct. 4, 2020).

[172] *See* Hayashi, *supra* note 26.

lead to the exposure of customers' account numbers and passwords.[173] Banks also argue against the FinTech companies' stance that limiting or regulating their access to private data hurts innovation, an argument which some commentators have made in various contexts as well.[174] The banks believe limiting access to banks' consumer financial data is the best way to promote consumer protection principles and promote their clients' best interests. Based on *Cottle vs. Plaid*, the class action filed in May 2020, at least some consumer groups agree that data aggregators' screen-scraping practices must be legally prohibited.[175]

1. The Dodd-Frank Act

The legal status of third-parties' rights to access consumers' financial data is murky in the U.S. Pursuant to the CFPB's November 2020 advance notice of proposed rulemaking ("ANPR"), it is affiliated with the Dodd-Frank Act's Section 1033, which provides, "among other things, that subject to rules prescribed by the Bureau of Consumer Financial Protection (Bureau), a consumer financial services provider must make available to a consumer information in the control or possession of the provider concerning the consumer financial product or service that the consumer obtained from the provider."[176] The CFPB also issued a request for information in November 2016 about market practices related to consumer access to financial information, citing to Section 1033, which "provides for consumer rights to access financial account and account-related data in usable electronic forms."[177] In 2016, various financial institutions, as well as the American Bankers Association ("ABA"), submitted comment letters in response, questioning Section 1033's applicability to consumer-authorized data access by third-parties as opposed to consumers' direct access.[178] Additionally, the ABA discouraged the CFPB from

---

[173] *See* Jennifer Surane, *JPMorgan's Clampdown on Data Puts Silicon Valley Apps on Alert*, FIN. ADVISOR (Mar. 26, 2019, 5:00 AM), https://www.fa-mag.com/news/jpmorgan-s-clampdown-on-data-puts-silicon-valley-apps-on-alert-43982.html?print [https://perma.cc/D42Q-4DWJ].

[174] *See generally* Yafit Lev-Aretz & Katherine J. Strandburg, *Privacy Regulation and Innovation Policy*, 22 YALE J.L. & TECH. 256 (forthcoming 2020) (explaining that although some industry players argue that privacy regulation will "stifle" innovation, its potential impact on innovation does not justify blanket opposition). "[S]ome sorts of privacy regulation designed to address misaligned market demand signals can potentially mitigate failures of appropriability and provide a more socially beneficial portfolio of innovation incentives." *Id.* at 256.

[175] *See* Complaint, Cottle v. Plaid, No. 4:20-cv-03056-DMR (N.D. Cal. May 4, 2020).

[176] *See* the CPFB's 2020 ANPR, *supra* note 68.

[177] *See* Request for Information Regarding Consumer Access to Financial Records, 81 Fed. Reg. 83,806 (Nov. 22, 2016).

[178] *See* E-mail from Robert A. Morgan, Vice President, Emerging Tech., on behalf of the Am. Bankers Ass'n to the Consumer Fin. Prot. Bureau (Feb. 21, 2017), https://www.consumerfinancemonitor.com/wp-content/uploads/sites/14/2017/02/ABA-Comment-CFPB-Data-Aggregators.pdf [https://perma.cc/C785-XDQU].

engaging in planned Section 1033 rulemaking, as indicated in its 2020 ANPR, cautioning that handing over passwords to third-parties is risky. Particularly, the ABA stressed that third-parties constantly pulling data from bank servers is technologically burdening and could destabilize financial networks.[179]

In October 2017, the CFPB released the "Consumer Protection Principles" for participants in the developing market for services based on the consumer-authorized use of financial data.[180] According to the CFPB, the principles are not legally binding rules. Instead, the principles merely express the agency's "vision for realizing a robust, safe, and workable data aggregation market that gives consumers protection, usefulness, and value."[181] As such, the principles are intended "to help safeguard consumer interests as the consumer-authorized aggregation services market develops," and address issues such as access to data.[182] In particular, the principles permit consumers to "authorize trusted third parties to obtain" their data "from account providers to use on behalf of consumers, for consumer benefit, and in a safe manner."[183] The principles also provide guidance for third-party providers of services, stressing issues such as protecting consumers' data from security breaches, obtaining clear and informed consent from consumers, and limiting access to data to include only necessary information to provide the services consumers seek.[184]

In its 2018 report, the Treasury Department embraced an expansive approach recommending "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."[185] But understanding that such regulatory interpretation would impact incentives, the Office of the Comptroller of the Currency (OCC) stated in its 2020 Bulletin that even when

> a bank is not receiving a direct service from a data aggregator and if there is no business arrangement, banks still have risk from sharing customer-permissioned data with a data aggregator. Bank management should perform due diligence to evaluate the business experience and reputation of the data aggregator to gain assurance that the data aggregator maintains controls to safeguard sensitive customer data.[186]

---

[179] *Id*.

[180] CFPB CONSUMER PROTECTION, *supra* note 50, at 1–5.

[181] *Id.* at 1.

[182] *Id.*

[183] *Id.*

[184] *Id*.

[185] 2018 Treasury Report, *supra* note 52, at 31.

[186] Off. of the Comptroller of the Currency, OCC Bulletin 2020-10: Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29 (Mar. 5, 2020), https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html [https://

But FinTech companies and data aggregators want more legal protection from Section 1033, believing it preserves their right to pull data from customers' bank accounts.[187] Lobbying for that acknowledgment, several FinTech companies and data aggregators formed the Consumer Financial Data Rights, advocating for consumers' rights to "innovative products and services that improve their financial well-being and are powered by unfettered access to" financial data.[188] They claim such access to financial data is vital for customers wanting to enjoy financial health and allows third-parties to provide better user experiences.[189]

2. Who's the Boss (Agency)?

It seems pretty straightforward that the government agency responsible for regulating and supervising consumer financial data sharing should be the CFPB. No lead-agency assumes the responsibility for all matters that lay in the intersection of finance, technology, and consumer protection. Therefore, in the absence of a consumer finance and technology-focused regulator, different administrative government agencies have been forced to create regulatory models for governing their respective portions of the data economy.[190] For example, the FTC and the DOJ enforce, *inter alia*, specific laws that touch upon consumers' data privacy and security and national competition laws.[191] The FTC mainly deals with unfair or deceptive acts or practices in or affecting commerce, and enforcing specific laws, such as COPPA, Fair Credit Reporting Act ("FCRA"),[192] and GLB.[193] The DOJ

perma.cc/JGK2-USST].

[187] Demos, *supra* note 51.

[188] Envestnet|Yodlee, *New Industry Group Established to Support Consumers' Right to Access Their Financial Data*, CISION PR NEWSWIRE (Jan. 19, 2017, 8:00 PM), https://www.prnewswire.com/news-releases/new-industry-group-established-to-support-consumers-right-to-access-their-financial-data-300392644.html?mod=article_inline [https://perma.cc/E2FR-9C9W].

[189] *See id.*

[190] *See, e.g.*, Van Loo, *supra* note 14, at 531–32 (exploring what the CFPB has done in its first several years to regulate FinTech).

[191] *See* Org. for Econ. Coop. & Dev. [OECD], *Consumer Data Rights and Competition—Note by the United States*, at 2, DAF/COMP/WD(2020)39 (June 12, 2020), https://one.oecd.org/document/DAF/COMP/WD(2020)39/en/pdf [https://perma.cc/E7TY-EQYB].

[192] Fair Credit Reporting Act, 15 U.S.C. §§ 1681–91. "Congress enacted [the] FCRA in 1970 to ensure fair and accurate credit reporting, promote efficiency in the banking system, and protect consumer privacy." Safeco Ins. Co. of Am. v. Burr, 551 U.S. 47, 52 (2007).

[193] *See* OECD, *supra* note 191, at 2.

> On the consumer data rights side, the FTC has brought hundreds of cases and obtained billions in penalties to protect the privacy and security of consumer data, enforcing the FTC Act's general prohibition of "unfair or deceptive acts or

brings both criminal and civil enforcement actions to protect consumers' health, safety, economic security, identity integrity, and antitrust related issues, which also prompted it to file its 2020 lawsuit against Visa and Plaid's proposed transaction.[194]

But unlike the FTC and DOJ, media outlets, various government agencies, and even the CFPB itself all believe that the CFPB has the mandate to regulate consumer data management.[195] This is not surprising. The CFPB has done a great deal to regulate FinTech under the umbrella of technology-related issues, particularly its 2016 request for information about market practices related to access to consumers' financial information.[196] The former CFPB Director, Richard Cordray, stressed the CFPB's readiness to protect consumers' right to share their data with data aggregators by executing binding regulations if needed.[197] Further supporting this

> practices in or affecting commerce." The FTC also enforces domain specific statutes such as the Children's Online Privacy Protection Act of 1998 (COPPA), which restricts collection and use of personal information pertaining to children under the age of thirteen, the Fair Credit Reporting Act (FCRA), which protects information collected by consumer reporting agencies, and the Financial Services Modernization Act of 1996 (Gramm-Leach-Bliley Act or GLB), which regulates the use and dissemination of consumers' "non-public personal information" by "financial institutions," broadly defined. The FTC also enforces federal competition law.
>
> The DOJ's Civil Division, Consumer Protection Branch, brings both criminal and civil enforcement actions to protect consumers' health, safety, economic security, and identity integrity. This work often implicates consumer data and privacy rights. The Consumer Protection Branch's civil authorities include jurisdiction over actions referred by the FTC seeking civil penalties under the FTC Act. It also has broad criminal authorities to carry out its mission. The DOJ's Antitrust Division has separate authority to enforce the federal competition laws.

Id. (footnotes omitted).

[194] *Id.*; Hrushka, *supra* note 46.

[195] *See, e.g.*, 12 U.S.C. § 5533(e) (stating that the CFPB should consult with the Board of Governors of the Federal Reserve System, the OCC, the FDIC, and the FTC to ensure, to the extent appropriate, that any regulation based on section 1033 includes similar requirements on covered persons, factors into account terms under which covered persons do business both in the U.S. and elsewhere, and does not require or promote the use of any specific technology in order to develop systems for compliance); *An Open Road for Open Banking?*, PYMNTS (Nov. 9, 2020), https://www.pymnts.com/news/digital-banking/2020/open-road-for-open-banking/ [https://perma.cc/29PB-VBNE] (explaining that by issuing its 2020 ANPR, the CFPB signaled its plan to focus on Section 1033 and that more rulemaking regarding financial data is on the horizon).

[196] *See, e.g.*, Van Loo, *supra* note 14, at 531.

[197] Richard Cordray, Dir., Consumer Fin. Prot. Bureau, Prepared Remarks at the Field Hearing on Consumer Access to Financial Records (Nov. 17, 2016), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-

notion, Cordray indicated in a different speech in 2016 that the CFPB was prepared to and capable of imposing a PSDII-type of regulation if necessary.[198]

The CFPB is indeed up for the data management regulation task. Although it missed an opportunity to regulate access to financial data when it released non-binding principles in 2017, which failed to initiate formal regulatory action,[199] this may be because the CFPB has no authority over antitrust law.[200] In the EU, for example, the regulator that handled data access in connection with banking also had antitrust authority.[201] While the CFPB lacks such authority, and many practitioners, scholars, and politicians have criticized its legal actions,[202] the CFPB's existence and areas of focus should no longer be questioned, even though its leadership structure was found unconstitutional following the *Seila* decision.[203] Moreover, no other governmental organizations or bureaus seem to have the expertise, legal power, and motivation to handle FinTech and consumer protection related issues, such as consumer data management.[204] Likewise, no other agencies have been suggested to potentially take on this regulatory role. Accordingly, the CFPB is the agency that should be responsible for consumers' data management. In that capacity, the CFPB should start by focusing on consumer financial data to broaden any such regulation to be more comprehensive and expansive as the Australian CDR, which covers the management of all consumer data.[205]

Starting with and focusing on financial data, the CFPB must conduct periodic checks to ensure that data aggregators are operating according to pre-determined standards, which it must develop. These checks would enable the bureau to protect

---

richard-cordray-field-hearing-consumer-access-financial-records [https://perma.cc/7UPG-4MFE].

[198] Richard Cordray, Dir., Consumer Fin. Prot. Bureau, Prepared Remarks at Money 20/20, (Oct. 23, 2016), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-richard-cordray-money-2020 [https://perma.cc/2DN5-L9TX] ("[W]e are gravely concerned by reports that some financial institutions are looking for ways to limit, or even shut off, access to financial data rather than exploring ways to make sure that such access, once granted, is safe and secure.").

[199] CFPB CONSUMER PROTETION, *supra* note 50, at 1–5.

[200] *See* Rory Van Loo, *Rise of the Digital Regulator*, 66 DUKE L.J. 1267, 1326 (2017) [hereinafter Van Loo, *Rise of the Digital Regulator*].

[201] EUR. BANKING AUTH., REPORT ON INNOVATIVE USES OF CONSUMER DATA BY FINANCIAL INSTITUTIONS 8–16 (2017), https://www.eba.europa.eu/documents/10180/1720738/Report+on+Innovative+uses+of+data+2017.pdf [https://perma.cc/DY98-FF2U].

[202] *See, e.g.*, Harvey, *supra* note 69, at 2434.

[203] Seila Law LLC v. Consumer Fin. Prot. Bureau, 140 S. Ct. 2183 (2020).

[204] *See* Van Loo, *Making Innovation More Competitive, supra* note 49, at 255–57. *But see* Dylan Tokar, *FTC to Clarify Its Power to Regulate Big Tech*, WALL ST. J. (Sept. 12, 2019, 5:02 PM), https://www.wsj.com/articles/ftc-to-clarify-its-power-to-regulate-big-tech-11568322161 [https://perma.cc/H39X-K3EY] (explaining that the FTC is in the process of defining how U.S. competition laws apply to big tech so it can better enforce anti-competitive behavior).

[205] For more information about the CDR, *see supra* note 62.

consumers' privacy.[206] But, supervision of large entities that are critical to the financial industry, such as data aggregators, might not be enough. Not only does the CFPB need to regulate consumer financial data sharing, but it also needs to monitor data aggregators and financial data sharing practices because these could cause systemic risk. In particular, the globally operated Switzerland-based Basel Committee on Banking Supervision believes system interconnections between banks and FinTech companies "may provide a pathway for a cybersecurity incident at a financial technology company to infect the banking system."[207] At the same time, operational risks may be of concern when banks have numerous FinTech services and relationships. Banks "face ambiguity and uncertainty as to the applicability of certain privacy rules, the Bank Secrecy Act provisions and regulations, and Anti-Money Laundering Standards" in the face of these relationships.[208]

III. DATA SHARING: TOO SIGNIFICANT TO BE LEFT UNREGULATED

A. The U.S. Market-Based Approach

Different from the EU and other places in the world, where a top-down regulatory approach concerning consumer financial data sharing has been adopted,[209] efforts to create standards to better handle data sharing in the U.S. are unsurprisingly developing under a market-based approach.[210] Whether preferred or not,[211] a market-based approach in financial regulation characterizes the American

---

[206] *See* Van Loo, *The Missing Regulatory State*, *supra* note 67, at 1586.

[207] *See* COUNCIL OF INSPECTORS GEN. ON FIN. OVERSIGHT, *supra* note 137, at 6.

[208] *Id.*

[209] *See* PSDII, 2015 O.J. (L 337) 35, *supra* note 14.

[210] *See* Karen Bartleson, *Market-Driven Standards and the IEEE-SA*, 18 IEEE INTERNET COMPUTING 58 (2014) (defining the market-driven model as a "model by which global standards are created, adopted, and recognized worldwide. In it, the very developers and users of technological innovations—as opposed to a centralized body—drive the development and adoption of the standards.").

[211] IEEE STANDARDS ASS'N BD. OF GOVERNORS, IEEE STANDARDS ASSOCIATION PUBLIC POLICY STATEMENT: POLICIES ACCEPTING GLOBAL, MARKET-DRIVEN STANDARDS SHOULD BE EMBRACED IN INTERNATIONAL TRADE DISCUSSIONS AND REGULATORY ENVIRONMENT 1–2 (2019), http://globalpolicy.ieee.org/wp-content/uploads/2019/03/IEEE18025.pdf [https://perma.cc/94JT-HWLB]. IEEE asserts that

> Unlike country-driven standards, the market-driven standards development paradigm favors no nation and fosters a global environment where technology standards compete for implementation on their own merits. This paradigm of market-driven standardization has been proven to ensure strong integration, interoperability, and increased synergies along the technological innovation chain, while allowing for the representation of the broadest possible cross-section of stakeholders.

financial markets.[212] As part of the efforts taking place in the U.S., banks, FinTech companies, and data aggregators have been trying to find middle ground regarding consumer financial data sharing. For example, in October 2018, some banks and FinTech companies partnered to form the Financial Data Exchange ("FDX"), a nonprofit that is a subsidiary of the Financial Services Information Sharing and Analysis Center ("FS-ISAC") that attempts to tackle the challenges of securely sharing consumers' financial data.[213] The nonprofit's goal is to develop standards for consumer data sharing to preserve security while still motivating innovation.[214] Among other objectives, it tries to think of ways to incorporate the thousands of smaller U.S. community banks and credit unions that, when combined together, have a significant market share in the financial industry.[215]

Similarly, other industry-led initiatives have been taking place to create market-based solutions, including the creation of a Model Agreement by the Clearing House ("TCH").[216] The TCH agreement is non-binding and helps financial players establish legal terms for sharing bank-held consumer data. It facilitates API agreements and encourages the adoption of API technology.[217] It was developed with input from industry participants and is intended to accelerate the legal review process during negotiations to ensure that key data security requirements are

---

Id.

[212] *See, e.g.*, Kevin S. Haeberle & M. Todd Henderson, *A New Market-Based Approach to Securities Law*, 85 U. CHI. L. REV. 1313, 1315–17 (2018) (arguing for an intermediate market-based approach towards achieving the optimal level of corporate disclosure rather than a pure market-based one).

[213] FS-ISAC, *supra* note 61.

[214] *Id.*

[215] *See* Shevlin, *supra* note 121 ("Problem is, partnering doesn't scale. Achieving scale requires a platform (like an Amazon or Goldman) who can integrate many providers. . . . Being able to create a technology platform to do this has been beyond the reach of most banks and credit unions.").

[216] *See TCH Gives Banks an Open Banking Template*, PYMNTS (Nov. 15, 2019), https://www.pymnts.com/data/2019/tch-gives-banks-an-open-banking-template/ [https://perma.cc/TX6Q-QKYQ]. Considering how APIs have developed historically,

> [O]nly the largest banks have had the resources—and the time—to devote to the extensive and technical application programming interface (API) integration, testing and compliance, and the legal and contractual reviews necessary to meet FI standards for data sharing . . . . That has left smaller FIs [financial institutions], without those resources, at a competitive disadvantage. After a year-long effort to address this disparity, TCH released a template . . . designed to help banks link with FinTech firms, connect to APIs and shorten the journey to financial services innovation.

Id.

[217] *See Model Data Access Agreement*, *supra* note 60, at 1–2.

understood.[218] The agreement aims to reduce the need to negotiate the same terms each time parties enter into an agreement,[219] and the use of it is voluntary.[220] Finally, specific banks and data aggregators have also been trying to work together and create all sorts of other joint programs and understandings.[221]

But market-led initiatives are not enough. The U.S. should regulate consumer financial data sharing, addressing key issues that should not be left for the markets to solve.

1. Issues with Consumer Financial Data Sharing

(a) Banks' Liability

Banks have tried to create obstacles for third-parties to access their customers' accounts and data.[222] One of the main reasons banks push back is that the "use of a third-party service provider does not" reduce banks' responsibility to ensure the activities are performed in a safe manner and in compliance with the appropriate laws, just as if the banks were to conduct the activities in-house.[223] Therefore, the key issue for banks when dealing with third-party service providers, FinTech companies or data aggregators, is liability.

In the November 2019 Basel Committee on Banking Supervision report, the banks' concerns were echoed:

> With more parties and intermediaries involved in the provision of financial services in an open banking model, it is more difficult to assign liability and the amount of damages to the customer, if any. The level of clarity and granularity of regulations governing customer redress vary across jurisdictions and, in some cases, may not have been updated to take open banking business models into consideration. [224]

Moreover,

> Banks may face reputational risk, even in jurisdictions where there are established liability rules. Many banks view themselves as custodians of

---

[218] *See TCH Gives Banks an Open Banking Template*, *supra* note 216.

[219] *Id.*

[220] *Id*.

[221] *See, e.g.*, *Increase Customers' Control*, *supra* note 60 ("With this new agreement, Envestnet|Yodlee is committing to send 100% of its requests for Chase customer data through the bank's secure API, or application programming interface. This will ensure the apps can receive Chase customer data they need while customers control what's shared with whom.").

[222] *See* Van Loo, *Rise of the Digital Regulator*, *supra* note 200, at 1286.

[223] 2018 Treasury Report, *supra* note 52, at 74.

[224] *See* BASEL COMM. ON BANKING SUPERVISION, *supra* note 58, at 7.

> their customers' data and customers place great confidence in the banks' ability to safeguard their data. In addition, customers often turn to the regulated entity ([i.e.,] their bank) first with complaints and disputes, even if the third-party is responsible for the erroneous transaction or data breach.[225]

Likewise, as mentioned above, banks face uncertainty regarding the applicability of various privacy laws, such as the Bank Secrecy Act, and anti-money laundering standards in connection with their relationships with FinTech companies and data aggregators.[226] The banks are not sure which privacy and confidentiality rules apply, to which entity, and to what extent, and do not want to be liable for consumers' privacy violations and damages.[227]

(b) Consumer Informed Consent

The process of accessing customers' bank accounts to retrieve their data is based on the customers giving their account credentials to the non-bank as a third-party.[228] It is questionable, however, if customers give informed consent for this process to take place creating a major problem.[229] In fact, it is not clear if customers even understand that a FinTech app and their bank are not the only ones involved in each financial transaction engaged in by consumers, or who else they are giving consent to access their data.[230] As mentioned above, many consumers do not know what data aggregators are or what they do.

The absence of informed consent is a problem. Following the 2008 crisis, it became widely accepted that consumer informed consent and disclosure are critical, especially when dealing with FinTech companies and other non-bank financial institutions, to guarantee the safe functioning of our financial markets.[231] Therefore, Dodd-Frank Act sections 115(f) and 165(d) granted the Financial Stability Oversight Council and the Federal Reserve Board the legal ability to mandate additional

---

[225] *Id.*

[226] *See* COUNCIL OF INSPECTORS GEN. ON FIN. OVERSIGHT, *supra* note 137, at 6.

[227] *See* Crosman, *Finra's Dire Warning*, *supra* note 36.

[228] *Id.*

[229] This issue is at the heart of the lawsuit alleging that no consent has been given. *See* Complaint at 50, Cottle v. Plaid, No. 4:20-cv-03056-DMR (N.D. Cal. May 4, 2020). Likewise, this lack of understanding has been the central issue in an October 2020 lawsuit filed by TD Bank against Plaid, in which the bank claimed Plaid mimicked its login page in an effort to "dupe" its customers, who were linking their bank accounts to payment apps, believing they are entering their personal data into TD's platform. *See* Hrushka, *supra* note 47. Moreover, studies have shown that most consumers do not know of data aggregators' involvement in their FinTech app interaction. *See* 2018 Treasury Report, *supra* note 52, at 25.

[230] *See* 2018 Treasury Report, *supra* note 52, at 25, and Berry, *supra* note 68.

[231] *See* Packin & Lev-Aretz, *Big Data and Social Netbanks, supra* note 12, at 1277–78.

periodic public disclosures of all financial companies including FinTech entities in order to "support market evaluation of the risk profile, capital adequacy, and risk management capabilities thereof."[232] Likewise, the CFPB has dealt with the issue of transparency from different angles and through various tools.[233] Much like banks and other traditional financial institutions, data aggregators such as Plaid should also be required to abide by transparency and disclosure requirements and policies.

But disclosure is not enough.

> It is a widely acceptable notion that most consumers do not read these guidelines, policies, and terms of service. This notion is generally supported by empirical studies, anecdotal evidence, and the reported personal record of legal scholars and judges. Reasons for not reading vary and range from lack of interest and difficulty in understanding the legal language, to the time consuming nature of those contracts and consumers' nonexisting bargaining power. When a great number of consumers all enjoy the same product under the same contract, users are further incentivized not to read because they feel reassured that the terms must be reasonable.[234]

In the context of FinTech transactions operated via data aggregators' services, the problem of fictional consent[235] is worsened. Consumers do not know what data

---

[232] *Id.* (quoting Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, §115(f), 124 Stat. 1367, 1406 (2010) (codified at 12 U.S.C. § 5325(f))).

[233] *Id.* at 1283.

[234] *Id.* at 1279 (footnotes omitted). Lev-Artez and I concluded earlier,

> Real people don't read standard form contracts. Reading is boring, incomprehensible, alienating, time consuming, but most of all pointless. We want the product, not the contract. Besides, lots of people bought the product or the service along with the same contract and seem happy enough, so we presume that there must be nothing particularly important buried in the contract terms.

Id. Accord Omri Ben-Shahar, *The Myth of the 'Opportunity to Read' in Contract Law* 1–4 (John M. Olin Program in L. & Econ., Working Paper No. 415, 2008).

[235] Margaret Jane Radin, Comment, *Boilerplate Today: The Rise of Modularity and the Waning of Consent,* 104 MICH. L. REV. 1223, 1231 (2006). Considering how online services purport to obtain user consent,

> Consent is fictional when the terms are filed somewhere we cannot access, as in airline tariffs. Consent is fictional when almost all of us click on-screen boxes affirming that we have read and understood things we have not read and would not understand if we did. Consent is fictional on websites whose terms of service state that just by browsing the site, whether or not one ever clicks on the terms, one has agreed to whatever the terms say, now or as they may be changed in the

aggregators are or their involvement in transactions. They also cannot directly connect FinTech apps with their banks in the same way they directly communicated with their banks. Furthermore, often in the digital content world, terms of service enable the provider to revise its terms at any given point in time[236]—a practice that, if used by data aggregators, would not only place users more at risk, but also contradict common understandings of contract law doctrines and financial institutions' disclosure obligations.[237]

"From a legal and policy perspective, users should be aware of the product they buy and the price they pay for it—be it in actual money, money equivalences, time (e.g., to fill out a survey), or personal information."[238] The cybersecurity, privacy, and financial harm dangers posed by screen-scraping are a great example of a significant price consumers may pay in exchange for being able to access FinTech apps' services or products. Paying a significant price and exposing themselves to different potential harms and dangers seems more reasonable when consumers make a choice to bind themselves to the conditions knowingly and willingly, after hearing the possible options and consequences. "When the terms of the service are successfully communicated, consumers, either individually or through the formation of advocacy groups, can propose stipulations, and the dialogue between those networks and their consumers is kept viable and open."[239] The current norms that data aggregators have developed in connection with using consumers' bank account credentials, which might not be based on clear and informed consumer consent, and screen-scraping consumers' financial data,[240] should not be legally or socially accepted.

Given the above, many commentators have criticized the practice of screen-scraping,[241] arguing that APIs offer a more secure method of accessing financial

---

future. Consent is fictional when the contract ends, as one I saw recently did, with "By reading the above you have agreed to it."

Id.

[236] *See, e.g.*, Douglas v. U.S. Dist. Court for Cent. Dist. of California, 495 F.3d 1062, 1067 (9th Cir. 2007) (discussing whether a service provider may change the terms of its service contract by posting a changed contract on its site with no additional notice). The court determined that service provider's customers should not be bound by revised terms in absence of notice. *Id.*

[237] *See* Patricia Sánchez Abril, *Private Ordering: A Contractual Approach to Online Interpersonal Privacy*, 45 WAKE FOREST L. REV. 689, 704–05 (2010) (suggesting that traditional preconditions to contracting are not being met online).

[238] *See* Packin & Lev-Aretz, *Big Data and Social Netbanks, supra* note 12, at 1280.

[239] *Id.* at 1279. *Accord* Ben-Shahar, *supra* note 234, at 1–4.

[240] This is in part what the lawsuit against Plaid alleges. *See* Complaint at 13, 50, Cottle v. Plaid, N.D. Cal., No. 4:20-cv-03056-DMR, (N.D. Cal. May 4, 2020).

[241] Scrapers have been described in various ways, including: (i) an invading army of robots in eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1061, 1065 (N.D. Cal. 2000); (ii) a person walking into a bank with both a safety deposit key and a shotgun in Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1068 (9th Cir. 2016); and (iii) an

information. Similarly, various jurisdictions have promoted access to such data through APIs. In the U.S., however, the legal environment surrounding data scraping is still evolving.[242] Differently, the U.K., via its open banking initiative, has provided detailed standards for data sharing through APIs,[243] and Singapore has promoted the use of bank APIs although it has not made it a regulatory mandate.[244] Similarly, in the EU, rules implementing PSDII proposed by the European Banking Authority would require banks to permit certified third-parties to access consumer data only via APIs and ban screen-scraping.[245] PSDII also contemplates the standardization of APIs.[246] This is not surprising. Unlike the U.S., the implementation of open banking in the EU is based on the region's strict data protection laws, which require informed consent from customers before their account data can be shared with third-parties using APIs. Under the General Data Protection Regulation ("GDPR"), banks will be responsible not only for informing customers of how their data may be used by such third-parties, but also for creating specific contractual and technical safeguards to guarantee that third-parties do not disclose or reuse the information without further approval from customers.[247]

---

interviewer using a tape recorder instead of writing down notes in Sandvig v. Sessions, 315 F. Supp. 3d 1, 16 (D.D.C. 2018).

[242] *See generally* Brainard, *supra* note 89 (analogizing the developing legal environment to the unpredicted advent of smartphone platforms). The 9th Circuit's 2019 decision in the *hiQ Labs* case sets back the battle against "data scraping." Jonathan Stempel, *Microsoft's LinkedIn Loses Appeal over Access to User Profiles*, REUTERS (Sept. 9, 2019, 12:34 PM), https://www.reuters.com/article/us-microsoft-linkedin-profiles/microsofts-linkedin-loses-appeal-over-access-to-user-profiles-idUSKCN1VU21W [https://perma.cc/A88V-Z4BU].

[243] *See generally* OPEN BANKING LTD., GUIDELINES FOR READ/WRITE PARTICIPANTS (2018), https://www.openbanking.org.uk/wpcore/wp-content/uploads/Guidelines-for-Read-Write-Participants.pdf [https://perma.cc/3RJD-QJXN] (describing an Open Banking standards system and responsibilities of members in the system).

[244] Ong Chong Tee, Deputy Managing Dir., Monetary Auth. of Sing., Remarks at the German-Singaporean Financial Forum: The Future of Banking – Evolution, Revolution or a Big Bang? (Apr. 16, 2018), http://www.mas.gov.sg/news/speeches/2018/the-future-of-banking [https://perma.cc/8VWE-64TF].

[245] Although banks have requested a ban on screen-scraping, it was opposed by FinTech companies. Antony Peyton, *No EC Love for European Banks' Screen Scraping Ban Plan*, FINTECH FUTURES (May 22, 2017), https://www.fintechfutures.com/2017/05/no-ec-love-for-european-banks-screen-scraping-ban-plan/ [https://perma.cc/8H5R-5322]. The European Banking Federation proposed a ban on screen-scraping, equating aggregator logins using consumer user names and passwords to "impersonating" consumers. *EBF asks Commission to Support Ban on Screen-scraping*, EUR. BANKING FED'N (May 16, 2017), https://www.ebf.eu/retail-payments/ebf-asks-commission-to-support-ban-on-screen-scraping/ [https://perma.cc/DZ8T-5PEK].

[246] *See* PSDII, 2015 O.J. (L 337) 35, *supra* note 14.

[247] Brian Hurh, Adam D. Maarec & Chris Chamness, *Consumer Financial Data Aggregation and the Potential for Regulatory Intervention*, 71 CONSUMER FIN. L.Q. REP. 20, 25 (2017).

One particular area of concern in connection with screen-scraping is it adds a layer of security concerns to an already alarming problem. Screen-scraping increases cybersecurity and fraud risks as individuals provide their secure login credentials to access FinTech apps,[248] partly because providing login credentials to data aggregators makes it easier for bad actors to get their hands on the credentials to move assets out of accounts.[249]

Therefore, the U.S. should adopt regulation based on APIs and mandate that both banks and third parties must disclose information, alert consumers, and require them to give consent, in different and multiple steps of their transactions with FinTech companies. After all, such an EU-like policy, where banks/Fintechs are responsible not only for informing customers how their data may be used by such third parties, but also for creating specific contractual and technical safeguards to guarantee third parties do not disclose or reuse the information without further, explicit approval from customers, has become an imperative.[250]

(c) Innovating or Getting More Data than Needed?

Data aggregators and FinTech companies look at individual financial data to innovate and offer superior and more efficient or cost-effective services and products. Yet, banks have data entries, which they would want the CFPB to consider as proprietary and thus designate as items that cannot be shared—such as pricing, interest rates, or fee information. Consequently, not getting access to such items would probably limit FinTech companies' abilities to innovate the products and services currently provided by banks. The consumers will miss out on some innovative offerings.

Likewise, on their quest to get information, screen-scraping enables data aggregators to get more data than needed, including sensitive personally identifiable information that can be subsequently stolen or misused,[251] in which case the banks

---

[248] *See* 2018 Treasury Report, *supra* note 52, at 24–25.

[249] See Crosman, *Finra's Dire Warning*, *supra* note 36 (describing how accounts are subject "to cyber fraud, unauthorized transactions and identity theft . . . . [Also, a] key risk is that the aggregators could be storing all consumer financial information or security credentials in one place, creating a new and heightened security risk for consumers.").

[250] Hurh, Maarec & Chamness, *supra* note 247.

[251] The sensitivity of consumer financial data varies. *See generally* Brandon Vigliarolo, *Popular Mobile Banking Apps Are Riddled with Security Flaws, and Android Users Are More at Risk*, TECHREPUBLIC (June 18, 2020, 12:11 PM), https://www.techrepublic.com/article/popular-mobile-banking-apps-are-riddled-with-security-flaws-and-android-users-are-more-at-risk/ [https://perma.cc/C99P-3BSN] ("A study of banking apps for iOS and Android found poor source code protection, cleartext storage of sensitive data, and other serious flaws that make it easy for attackers to break into accounts."). For example, data indicating that a bank account is a checking account is less confidential than the account number. If a FinTech app only needs to know the account type, then it would be unnecessary to identify account numbers.

may likely be on the hook. Moving away from screen-scraping can help solve some of the liability issues, "eliminating the need for login credentials" and lowering the possibility of an unauthorized transaction.[252] But currently, the U.S. industry has not shifted away from screen-scraping.

Moreover, in *hiQ Labs Inc. v. LinkedIn Corp*,[253] after LinkedIn asked hiQ to stop scraping data from its public website and tried to create a technical barrier to prevent the scraping, the Court of Appeals for the Ninth Circuit ruled against LinkedIn.[254] Nevertheless, certain industry players who understand the dangers associated with screen-scraping have started contracting to use APIs, which are conditioned upon contractual liability and indemnification of the (concerned) financial services company,[255] even if doing so is not always easy. Indeed, as mentioned, many data aggregators and FinTech companies are not happy about the limiting nature of APIs and their dependence on the banks' good will for access to data.[256] They argue that their APIs' access is limited to specific types of data dictated by banks, rather than consumers, and push against API agreements' strict contractual liability provisions.[257]

As the U.S. Government Accountability Office ("GAO") noted,[258] financial responsibilities for consumer losses and access to consumer financial transaction data are extremely important issues that must be carefully and quickly addressed. Federal banking regulators and the CFPB understand this and have held multiple discussions on the topic under the sponsorships of the Federal Financial Institutions Examination Council ("FFIEC").[259] No concrete policy or guidelines to direct market participants have been agreed upon as of yet, which is problematic for banks that do not want to be liable for third-parties' doings, consumers, Fintech companies, and data aggregators.[260] As long as the liability issue is not resolved, "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."[261]

---

[252] *See* 2018 Treasury Report, *supra* note 52, at 35.

[253] 938 F.3d 985 (9th Cir. 2019).

[254] *Id.* at 1005.

[255] 2018 Treasury Report, *supra* note 52, at 35.

[256] *See* CASTRO & STEINBERG, *supra* note 156, at 1–2.

[257] *See* 2018 Treasury Report, *supra* note 52, at 34.

[258] *See* U.S. GOV'T ACCOUNTABILITY OFF., FINANCIAL TECHNOLOGY: ADDITIONAL STEPS BY REGULATORS COULD BETTER PROTECT CONSUMERS AND AID REGULATORY OVERSIGHT 54–57 (2018), https://www.gao.gov/assets/700/690803.pdf [https://perma.cc/EYY2-HJ2C] (responding to a congressional request for a report on various aspects of FinTech activities and providing recommendations including changes to the U.S. regulatory structure).

[259] 2018 Treasury Report, *supra* note 52, at 35.

[260] *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 258, at 54–57.

[261] *Id.* at 57.

(d) Data Security Issues

Enabling FinTech companies to collect all sorts of information about consumers increases cybersecurity concerns. The growing cost, regularity, and gravity of data breaches are now key issues in risk management. More than 4,000 known data breaches have shaken, weakened, and almost paralyzed markets during the last decade.[262] Experts believe massive numbers of records encompassing confidential or sensitive data have been compromised, and these global data breaches cost more than $400 billion annually.[263]

Information about financial transactions and social media data present an especially appealing target for hackers.[264] Large financial institutions obtain, store, and maintain noteworthy volumes of personal data. Storage, compilation, and transfer of confidential data make financial institutions extremely desirable targets for hackers.[265] Among the federal laws focusing on the collection, compilation, and handling of sensitive data is the Gramm-Leach-Bliley Act ("GLBA"),[266] which is enforced by the federal banking agencies for depository institutions,[267] the SEC, the Commodity Futures Trading Commission ("CFTC"), and the FTC.[268] These agencies all maintain authority to implement regulations for GLBA, and all agencies but the FTC can also supervise and examine compliance.[269]

But data security standards are completely different for non-financial business entities like retailers or manufacturers. Massive amounts of financial data that includes consumer payment credentials are regularly saved on non-financial business entities' internal or third-party databases used for various promotion and marketing purposes or to rapidly conduct transactions.[270] Such entities, however, need not comply with broad federal data security standards under GLBA or be constantly monitored. Their main obligation to protect data results from the FTC's

---

[262] *Examining the Use of Alternative Data in Underwriting and Credit Scoring to Expand Access to Credit: Hearing Before the Task Force on Fin. Tech. of the H. Comm. on Fin. Serv.*, 116th Cong. 14 (2019) (statement of Kristin N. Johnson, Professor, Tulane Univ. L. Sch.).

[263] *Id.*

[264] *Id.*

[265] *Id.*

[266] Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 & 15 U.S.C.).

[267] *See* Interagency Guidelines Establishing Information Security Standards, 66 Fed. Reg. 8,616 (Feb. 1, 2001); 69 Fed. Reg. 77,610 (Dec. 28, 2004) (promulgating and amending 12 C.F.R. pt. 30, app. B (2014) (concerning the Office of the Comptroller of the Currency)); 12 C.F.R. pt. 208, app. D-2, pt. 225, app. F (2014) (concerning the Federal Reserve Board); 12 C.F.R. pt. 364, app. B (2015) (concerning the Federal Deposit Insurance Corporation).

[268] *See* U.S. DEP'T OF THE TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES: ASSET MANAGEMETN AND INSURANCE 18 (2017).

[269] 2018 Treasury Report, *supra* note 52, at 39.

[270] *Id*.

exercised authority under Section 5 of the Federal Trade Commission Act,[271] which enables the FTC to enforce actions against nonfinancial business entities for unfair or deceptive practices. Since 2002, the FTC has exercised its power to enforce actions more than 60 times,[272] but because its power is restricted to enforcement action, the agency cannot supervise or examine nonfinancial companies on an ongoing basis.[273]

All businesses are subject to state laws, however, and those can include specific data security standards. But as of 2019, only a little over a dozen states have imposed various data security standards to protect consumer financial data,[274] and some are extremely weak. For example, Florida mandates business entities to take "reasonable measures" to protect and secure people's private information collected in "electronic form," and Utah does not distinguish between personal data saved on paper versus electronically.[275]

These few and weak laws are not effective. In the last decade, multiple nonfinancial business entities suffered from major data breaches of consumer financial data. One example was Target in 2013, which publicized that the payment card data of "[a]pproximately 40 million" accounts was compromised.[276] Similarly, in 2014, Home Depot revealed that a data breach resulted in the theft of card payment information of more than 50 million consumers.[277] Likewise, the parent entity of Lord & Taylor and Saks Fifth Avenue reported that the payment credentials of 5 million of its customers were compromised.[278] Such data breaches have affected financial institutions as well.[279]

---

[271] 15 U.S.C. § 45(a)(1).

[272] FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2017, 4 (2017), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf [https://perma.cc/G6Y6-EXD8].

[273] *See id.* at 1 (describing scope of FTC's privacy and protection work).

[274] 2018 Treasury Report, *supra* note 52, at 39.

[275] *Compare* FLA. STAT. ANN. § 501.171(2) (West 2019), *with* UTAH CODE ANN. § 13-44-201 (West 2019).

[276] Press Release, Target Corp., Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores (Dec. 19, 2013), https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car [https://perma.cc/3Q2J-MF6Z].

[277] Press Release, The Home Depot, The Home Depot Reports Finding in Payment Data Breach Investigation (Nov. 6, 2014), http://ir.homedepot.com/news-releases/2014/11-06-2014-014517315 [https://perma.cc/P49V-WRY6].

[278] Mike Murphy, *Saks, Lord & Taylor Data Breach May Affect 5 Million Customers*, MARKETWATCH (Apr. 1, 2018, 5:23 PM), https://www.marketwatch.com/story/saks-lord-taylor-data-breach-may-affect-5-million-customers-2018-04-01 [https://perma.cc/Q5Z4-UVYE].

[279] For instance, JPMorgan Chase suffered a data breach in 2014 and Equifax in 2017. *See, e.g.*, Jessica Silver-Greenberg, Matthew Goldstein & Nicole Perlroth, *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. TIMES (Oct. 2, 2014, 12:50 PM), https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-

There is no federal law creating uniform nationwide standards for alerting consumers about data breaches or for providing simple dispute solving mechanisms.[280] Given this regulatory vacuum, states create their own data breach notification rules, which apply to businesses located in their jurisdictions or transacting with their residents.[281] Therefore, if data breaches occur, businesses could be subject to more than 50 different notification laws.[282] State laws for data breach notification typically provide details regarding the number of impacted consumers that will result in notification requirements, as well as the notification's timing and procedure.[283] But state data breach notification laws vary greatly and include substantively different provisions regarding the nature of data defined as personal information.[284] These variations among the laws cause inefficiencies and make compliance challenging for both non-financial businesses and financial institutions, resulting in disparate treatment for consumers.[285] While Congress attempted to create relevant federal uniform standards a number of times, including during the 114th Congress,[286] no law has been established yet, and no uniform national standards exist. Therefore, consumer financial data is not properly protected.

Lastly, as far as third-parties are concerned, financial institutions are worried about being liable for any potential harms associated with data being used by, transferred, sold to, or hacked or exploited by third-parties. Not only can third-parties intentionally choose to take unregulated actions that would prove harmful and successfully dodge liability, but horrific consequences can also happen without

---

issues/ [https://perma.cc/9Q6J-HHQR]; Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth & Ron Lieber, *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html [https://perma.cc/CE5V-WKXR].

[280] Federal banking regulators have adopted guidance for depository institutions for cases of unauthorized access to consumers' information. *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736 (Mar. 29, 2005).

[281] 2018 Treasury Report, *supra* note 52, at 39–40.

[282] They could be subject to the laws of fifty states, in addition to those of the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands. *See Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGIS. (Mar. 8, 2020), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/W9HF-HCRU] (listing citations to state and territorial laws for reporting a data breach).

[283] *Id*.

[284] For instance, Maryland laws cover individuals' biometric data and other unique biological characteristics, although most states do not. *Compare* MD. CODE ANN., COM. LAW § 14-3501(e)(1)(i)(6) (West 2019), *with* NEV. REV. STAT. ANN. § 603A.040(1) (2019).

[285] *See* Brian Knight, *Federalism and Federalization on the Fintech Frontier*, 20 VAND. J. ENT. & TECH. L. 129, 185–99 (2017).

[286] Data Security Act of 2015, H.R. 2205, 114th Cong. (2015); Data Security and Breach Notification Act of 2015, H.R. 1770, 114th Cong. (2015).

intentional action. Attackers keep searching for the weakest links in the information supply chain and often attempt to hack or harm entities and institutions by indirectly attacking related third-parties or backdoor channels.[287] Third-party providers and websites are exposed to, maintain, and even carry large amounts of data about consumers, making them targets as well.[288] Another problem is that businesses across various industries have become so interconnected and interdependent that hackers can attack advanced cybersecurity systems of bigger businesses by turning to smaller businesses without vigorous protection.[289] These smaller businesses may be third-parties and may hold valuable data. "For example, the hack into the Office of Personnel Management (OPM) was the result of IT system access through a third party."[290]

(e) Consumers' Privacy & Contextual Integrity

The expanded access to financial and non-financial data enabled by the shift towards open banking raises critical issues with respect to protecting the confidentiality of consumers' data. The EU's GDPR attempts to address some of these concerns by creating a fundamental right to privacy that includes people's right to have their data deleted and transferred, among other provisions.[291] Similarly, the Australian CDR[292] creates a singular consumer right that enables all institutions to

---

[287] N.Y. STOCK EXCH., NAVIGATING THE DIGITAL AGE: THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS 207–12 (2015), https://www.nyse.com/publicdocs/Navigating_The_Digital_Age.pdf [https://perma.cc/KE5W-UWCQ].

[288] *See* LONGITUDE RES. & SAS INST., CYBERRISK IN BANKING: A REVIEW OF THE KEY INDUSTRY THREATS AND RESPONSES AHEAD 2 (2013), http://www.ifconsultants.org/whitepapers/cyberrisk-in-banking-106605.pdf [https://perma.cc/62AN-TPW5]. Similarly, a recent study found that hackers hacking into the biggest tech companies can take over the accounts of the tech giants' users and also access third-party websites that the tech giants' users logged in to. Mohammad Ghasemisharif, Amrutha Ramesh, Stephen Checkoway, Chris Kanich & Jason Polakis, *O Single Sign-Off, Where Art Thou? An Empirical Analysis of Single Sign-On Account Hijacking and Session Management on the Web*, 27 USENIX Sec. Symp. 1475, 1475–76, 1489 (2018), https://www.cs.uic.edu/~polakis/papers/sso-usenix18.pdf [https://perma.cc/C3E2-2WHW].

[289] U.S. SMALL BUS. ADMIN., INTRODUCTION TO CYBERSECURITY (2020), https://www.sba.gov/managing-business/cybersecurity/introduction-cybersecurity [https://perma.cc/P62C-VKFG] (last visited Nov. 22, 2020).

[290] *See* Packin, *supra* note 134, at 1258.

[291] Because the GDPR has raised a number of questions about implementation for companies that hold people's data, lack of regulatory clarity with its implementation may add barriers to trade and hurt cross-border regulatory cooperation. *See, e.g.*, Wilbur Ross, *E.U. Data Privacy Laws Are Likely to Create Barriers to Trade*, FIN. TIMES (May 30, 2018), https://www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c [https://perma.cc/LU79-5QVN].

[292] *See supra* note 62.

connect to other data systems.[293] But even with laws in place, issues such as consumer disclosure, consent, and termination appear challenging to handle.[294]

Consumers' authorization should be the legal basis for accessing their financial data.[295] But consumers cannot make informed choices in the absence of a transparent, comprehensible, and accessible disclosure. Without one, it is impossible to understand the risks, costs, and benefits of using FinTech apps and enable third-parties to access and use consumers' personal and financial data.[296] Some FinTech apps and data aggregators offer hard-to-follow disclosures on what data will be collected and how it will be used and saved. In other situations, the disclosures, terms, and conditions may be difficult to find or they may be described in such legalistic terms that consumers will find themselves lost and skip to the "accept" button, or simply reject the product.[297] Since most consumers increasingly use FinTech apps on their smartphones, the chances that they will read and comprehend long, detailed disclosures on their phones diminishes.[298] Moreover, even if "[d]isclosures written in plain language might increase consumer awareness . . . that only works if consumers actually read the 'Terms and Conditions' before downloading the latest financial app."[299]

However, consumers typically do not read disclosures,[300] and many disclosure critics believe not reading is the rational thing to do,[301] because they do not matter. Many prefer convenience over security and continue to rely on their banks for the protection of their data.[302] This should alert banks as it means banks must confirm

---

[293] Sarah Kocianski, *The Globalisation of Fintech—The Australian Example (Part II)*, FORBES (Aug. 19, 2019), https://www.forbes.com/sites/sarahkocianski/2019/08/19/the-globalisation-of-fintech-the-australian-example-part-ii/#bf6ffe77cf95 [https://perma.cc/JB3N-9DDQ].

[294] *See, e.g.*, Jean-Michel Franco, *How Australian Companies Are Failing to Meet Data Privacy Compliance*, FINTECH BUSINESS (Feb. 3, 2020), https://www.fintechbusiness.com/blogs/1654-how-australian-companies-are-failing-to-meet-data-privacy-compliance [https://perma.cc/9JE2-XJ2U].

[295] 2018 Treasury Report, *supra* note 52, at 32.

[296] *Id*. at 32–33.

[297] *Id*. at 32.

[298] *See id.*

[299] Amber Goodrich, *5 Challenges of Sharing Consumer Data*, COMPUT. SERV., INC. (Nov. 8, 2017), https://www.csiweb.com/resources/blog/post/2017/11/08/5-challenges-of-sharing-consumer-data [https://perma.cc/9K4S-ZCNS].

[300] Jeff Sovern, Elayne E. Greenberg, Paul F. Kirgis & Yuxiang Liu, *"Whimsy Little Contracts" with Unexpected Consequences: An Empirical Analysis of Consumer Understanding of Arbitration Agreements*, 75 MD. L. REV. 1, 15–18 (2015).

[301] *Id.* at 18, n.81 (quoting OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 10 (2014)).

[302] According to one survey, 91% of U.S. consumers willingly accept the terms and conditions of apps without reading them, and for consumers aged 18–34, the acceptance rate, without reading them, is 97%. DELOITTE, 2017 GLOBAL MOBILE CONSUMER SURVEY 12 (U.S. ed. 2017), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology

that their customers understand the meaning of legally permitting third-parties to access their accounts or initiate transactions. Moreover, data aggregators often get more information than necessary when providing the consumers' requested products and services.

Lastly, disclosures may not be useful if consumers are unaware of the relationships underlying the services and products they are using. For instance, for FinTech apps that rely on data aggregators to get or process consumers' financial information, the role of data aggregators may be completely opaque to consumers. This issue touches upon the legitimacy of the practice of collection and use of information about unsuspecting individuals by third-parties.

A benchmark theory of privacy sheds light on the legitimacy of such a practice.[303] Helen Nissenbaum's contextual integrity theory[304] offers a conceptual framework of protected private information in connection with the norms of information flow within particular contexts.[305] The theory rejects the traditional distinction of public versus private information. Instead, the theory suggests that data-sharing activities present themselves in a "plurality of distinct realms," all of which are governed by norms of information flow that define the contours of our essential entitlements regarding personal information.[306] The theory differentiates between two types of informational norms: norms of appropriateness and norms of flow or distribution.[307] Norms of appropriateness define if the information of a specific type is appropriate for disclosure in a given context.[308] In addition to determining appropriateness based on context, contextual integrity also considers if the distribution or flow of the information follows the contextual norms of information flow.[309] Accordingly, privacy is invaded when these informational norms are violated.

In the open banking context, norms of appropriateness are ignored when data aggregators collect and use banks' customers' financial information that the customers shared with their FinTech companies in the interest of using a certain app.

-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf [https://perma.cc/TSN9-KU5Q]. *See also Key Findings from the Consumer Digital Behavior Study*, A.T. KEARNEY (Apr. 2018), https://www.atkearney.com/financial-services/the-consumer-data-privacy-marketplace/the-consumer-digital-behavior-study [https://perma.cc/6J5E-3LAS] ("Consumers view banks as their best agent in protecting consumer data privacy and security[.]").

[303] Packin & Lev-Aretz, *supra* note 3, at 387–88.

[304] *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT (2010) (describing the importance of social contexts and context-relative informational norms when considering the right to privacy).

[305] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 136–38 (2004).

[306] *Id.* at 137.

[307] *Id.* at 140.

[308] *Id*.

[309] *Id*.

Norms of information flow are also breached because individuals are generally unaware of data aggregators and do not expect such a use of their financial information at the specific points of when information is created or when their relationship with the FinTech companies' apps begin. Put differently, their right to privacy is violated due to the unexpected flow of personal and financial information from entities that they reasonably expect to collect and use the financial information (*e.g.*, FinTech companies offering apps) to other entities (*e.g.*, data aggregators) that use the same information for various purposes. This is especially the case because consumers often do not have easy ways to revoke their consent to data aggregators' access to their information.[310] Hence, data aggregators may continue to save, use, and even collect information without the consumers having any control over the scope and duration of data being obtained, how it is used, and who gets it.

The contextual integrity theory is directly dependent on individual and societal privacy expectations and those are highly susceptible to changes over time. Thus, if data aggregators grow to become widely-known, widely-accepted players in the financial ecosystem (and perhaps even recognized gatekeepers of sorts), many of the arguments listed above would lose much of their strength because the use of financial and personal information for other purposes would no longer be utterly outside the purview of an individual's expectations. The more people become familiar with data aggregators and their services, the more accepted their practices will be.

(f) Tech and Discrimination-Related Issues

Because of the way they are designed, digital technologies tend to perpetuate historical systems of discrimination.[311] Since consumer financial data can play a role in all aspects of life—finance, insurance, employment, education, medicine, and much more—we need to be careful about who has access to it and how it is being used. As third-party data brokers accumulate massive amounts of data and share it, even if there are categories of data that are protected, processing such large amounts of data often creates the existence of proxies that allow for discrimination against protected classes within or among systems.[312] The problem is, however, that individuals and private sector entities all rely on algorithmic decisions, which typically do not explain their decision-making processes or their reasoning, and make determinations that could be discriminatory, based on the design of and

---

[310] *See* 2018 Treasury Report, *supra* note 52, at 33.

[311] *Banking on Your Data: The Role of Big Data in Financial Services: Hearing Before the H. Fin. Serv. Comm.*, 116th Cong. (2019) (statement of Christopher Gilliard, Macomb Cmty. Coll.), https://financialservices.house.gov/uploadedfiles/hhrg-116-ba00-wstate-gillardc-20191121.pdf [https://perma.cc/D4G6-BGXQ].

[312] *See id.*; *see also* Solon Barocas & Andrew Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 677–80 (2016).

assumptions in the algorithms, or data they worked with.[313] Likewise, public sector entities also rely on algorithmic systems for various purposes.[314]

In addition to the potential discriminatory harm for consumers, banks would not want to be legally liable for discrimination-related harms, which are based on third-parties' improper usages of data, especially since banks are legally required to allocate many resources to comply with binding anti-discrimination legislation.[315] But without proper regulation, banks or consumers will not be able to prevent third-party data brokers from using consumers' financial data in discriminatory ways, or stop "invasions of personal autonomy, existing or prospective, that information technology now makes possible . . . . [because] the basic safeguards cannot be provided by new inventions. They must be provided by the legislative and legal systems of this country."[316]

(g) Market Power and Competition-related Issues

The banks' main concern about FinTech companies operating in the financial industry results from wanting to maintain their own competitive advantage. In some ways, it is the same old story of the incumbent versus the disruptor. Some commentators argue that the competitive advantage issue was the key factor in the Visa-Plaid deal,[317] as banks object to giving their customers' data away to FinTech

---

[313] *See, e.g.*, Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 125–27 (2014) (arguing that due process rights should attach at certain regularized and repetitive data-driven conclusions); Danielle Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1253–55 (2008).

[314] *See* Robert Brauneis & Ellen Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 107 (2018).

[315] Banks must comply with both state and federal laws that forbid them from discriminating. *See, e.g.*, Conor R. Harvey, *Breaking the Bank: Split Interpretations of the Bank Acts in the Era of #MeToo*, 2019 U. CHI. LEGAL F. 473, 478 (2019) ("Today, federal statutory restrictions prohibit discrimination on the basis of age, physical disability, 'race, color, religion, sex, or national origin,' wage garnishment, 'pregnancy, childbirth, or related medical conditions,' military status, jury duty, and a myriad of other classifications . . . . [Moreover] [m]any of these federal anti-discrimination statutes contain express anti-preemption provisions that preserve parallel state laws and remedies." (footnotes omitted)). Noteable examples of such laws include the Community Reinvestment Act, 12 U.S.C. §§ 2901-2907, which focuses on credit extension to low and moderate income populations, and the Equal Credit Opportunity Act, 15 U.S.C. § 1691, which mandates disclosure of reasons for denying the grant of credit.

[316] *See Federal Data Banks, Computers and the Bill of Rights: Hearing Before the Subcomm. on Constitutional Rights of the House Comm. on the Judiciary*, 92d Cong. 765 (1971) (testimony of Jerome B. Wiesner, Provost Elect, Mass. Inst. of Tech.).

[317] *See, e.g.*, Ron Shevlin, *What's Visa Going to Do with Plaid?*, FORBES (Jan. 20, 2020, 5:00 AM), https://www.forbes.com/sites/ronshevlin/2020/01/20/whats-visa-going-to-do-with-plaid/?sh=195baed23559 [https://perma.cc/Z2BB-MPH3] ("Visa bought Plaid to

companies,[318] and risk losing the customers. Analyzing the Visa-Plaid deal, worrying about limiting competition, and consequently hurting innovation, the DOJ determined that without its interference, data aggregators will cooperate with, or get acquired by, strong financial institutions such as the major credit card companies, and serve their interests.[319] But in such circumstances, the interests of the data aggregators are those of their bigger customers—banks—and they will stop supporting FinTech companies to continue to innovate.[320]

Likewise, businesses with more customer information have stronger control over their customers. Understanding this, banks want to share with FinTech companies only the bare minimum. For example, since Zelle is owned and operated jointly by several big banks, banks prefer to have Zelle act as the front-end, rather than a data aggregator, which would obtain a great deal of information about many of the banks' customers.[321] Pushing against data aggregators, PNC Bank decided in 2019 to block their customers' access to Venmo, Zelle's rival payment app.[322]

---

quietly kill it. Who makes money for Visa? Their issuing banks and credit unions. Who are Plaid's customers? Neobanks and non-banks wanting to pull deposits out of banks and credit unions. In the end, organizations follow the most direct economic incentives." (internal quotation omitted)).

[318] *See* Pedersen, *supra* note 98 (describing how the biggest banks' CEOs believe that while banks "should be open to partnerships with technology and fintech companies, they need to be careful not to give away too much in the process").

[319] *See* Complaint, USA v. Visa Inc., 4:20-cv-07810 (N.D. Cal. Nov. 5, 2020).

[320] *See* Crosman, *Mastercard and Visa Gobble Up*, *supra* note 34. According to industry leaders,

> "If more moats are created to control personal financial information, there will be no ability for new businesses to create value around this data, let alone consumers having the ability to cross the water toward new value." Leimer pointed out that these two mergers will likely slow down the pace of innovation for the acquired firms, at least until the each deal and all its ramifications are worked out. Another issue, in his view, is control and lack of choice. "When large data platforms become larger through acquisition or broader business extension, we lose choices, both in founders of new fintech firms and developers of new financial applications," he said. "We need to continue to see, at least in the U.S., given how many financial institutions still exist, innovation that helps develop consumer value around savings, income and spend optimization, and long-term wealth creation through investments."

Id. (quoting Brad Leimer, co-founder of Unconventional Ventures).

[321] Stacy Cowley, *Cash Faces a New Challenger in Zelle, a Mobile Banking Service*, N.Y. TIMES (June 12, 2017), https://www.nytimes.com/2017/06/12/business/dealbook/mobile-banking-zelle-venmo-apple-pay.html [https://perma.cc/A2JL-HWC9].

[322] *See* Hayashi, *supra* note 26.

(i) Market Size and Volume

Even if the incumbents try to maintain their advantage non-competitively, the winds are changing in the financial industry in recent years. The growing size of technology companies in the financial industry has been impossible to miss. Covering more products, services, and populations, technology companies have raised attention and capital. For example, valuations of the biggest private companies expanded significantly that by 2019, there were 39 venture capital-backed FinTech unicorns—companies valued at more than one billion dollars—"worth a combined $147.37 billion";[323] compared to at least six of the 39 FinTech companies reaching unicorn status in the U.S. in 2018.[324] Moreover, U.S. FinTech companies raised 43% more capital than in 2017, and globally, FinTech companies entered into more than 1,700 deals worth nearly $40 billion.[325] However, being the incumbents, banks already have a great deal of information on consumers and businesses. Therefore, the banking industry's recent push against technology companies is at least partially driven by the tremendous disruption that these companies are causing to the landscape of the financial industry. Companies like Mint, for example, provide consumers with an aggregated snapshot of their accounts from multiple financial institutions.[326] Without access to banks' data, Mint's business would collapse. Thus, if banks try to avoid losing ground by choking off the data, they put tremendous pressure on FinTech companies and can potentially drive some out of business. Most FinTech companies are dependent on access to banks' data. As a result, FinTech companies started lobbying against the banks' reluctance to grant them access to customer data, arguing that it hurts the consumer and stifles innovation.[327]

(ii) Bi-Directional Flow of Data – Learn from Australia

In the U.S. and the EU's PSDII, open banking has been promoted as a one-sided initiative. Moreover, open banking has been described as a seismic shift for

---

[323] *See Fintech Trends to Watch in 2019*, CB INSIGHTS, https://www.cbinsights.com/research/report/fintech-trends-2019/ [https://perma.cc/26PL-CM3W] (last visited July 7, 2020).

[324] Jeff Kauflin, *The 11 Biggest Fintech Companies in America in 2019*, FORBES (Feb. 4, 2019, 9:45 AM), https://www.forbes.com/sites/jeffkauflin/2019/02/04/the-10-biggest-fintech-companies-in-america-2019/#7213320432b9 [https://perma.cc/5J95-EYXB].

[325] *See* CB INSIGHTS, *supra* note 323.

[326] Geoffrey A. Fowler, *These Apps Can Finally Get You to Save Money*, WALL ST. J. (June 16, 2015), https://www.wsj.com/articles/these-apps-can-finally-get-you-to-save-money-1434477296 [https://perma.cc/JJ8L-MQSA].

[327] Ethan Wolff-Mann, *A Banking War over Access to Your Data Is Stifling Innovation*, YAHOO! FIN. (Sept. 28, 2017), https://finance.yahoo.com/news/banking-war-access-data-stifling-innovation-143439973.html [https://perma.cc/4QPX-ND4W].

FinTech companies.[328] Consequently, banks are fighting the demands for a uni-directional flow of data, arguing that such a one-sided initiative is problematic, not only for their business operations, but also because it does not serve the consumers' best interests.[329] The more consumers adopt FinTech's products and services, the more banks will want and need access to FinTech's data to properly serve their customers and be able to fully connect information about investments, insurance, loans, etc., back to their own databases. Moreover, consumers might expect and want to see that information gets shared with their banks as well.

This consumer-facing bi-directional flow of data is one of the key premises in the Australian CDR, which creates a singular consumer right.[330] The CDR allows individuals and business consumers to access data on their own consumption of goods and services. Thus, the law enables "consumers to direct custodians to share their data with accredited entities, which have 'satisfactory security and privacy safeguards' in place."[331] Also, importantly, the definition of CDR data is

---

[328] *See Seismic Shift*, *supra* note 18.

[329] *Id.* (explaining that for banks to be willing to participate, the open banking initiative should not be "[l]et's make this a uni-directional flow of data" but instead proceed with "the expectation that it's bi-directional").

[330] *See* Kocianski, *supra* note 293. The reciprocity principle is central to the CDR, and the intention is for it "to apply economy wide on a sector-by-sector basis where this will increase competition and lead to greater consumer outcomes." *See* DATA GOVERNANCE AUSTL., REVIEW INTO OPEN BANKING IN AUSTRALIA 3, (2019), https://treasury.gov.au/sites/default/files/2019-03/T282002-Data-Governance-Australia.pdf [https://perma.cc/WPD6-ACEU]. Therefore, the intended data flow would be bi-directional, *i.e.* banks will share their data with FinTech companies, which in return will share their data with banks. The CDR's goal is to "improve customer choice and convenience by allowing data to be shared with third parties," as it is believed that this will increase competition in all the participating sectors, such as banking, and would enable consumers to obtain greater value for their money. *See* The Treasury, Austl. Gov't, Consumer Data Right – Fact Sheet, https://static.treasury.gov.au/uploads/sites/1/2018/02/180208-CDR-Fact-Sheet-1.pdf [https://perma.cc/WH5M-N2DC] (last visited Nov. 22, 2020). In addition, it is believed that the two-way sharing nature of the law "will improve the flow of information in the economy and encourage the development of new products and applications that reach more consumers and are better tailored to their needs." THE TREASURY, AUSTL. GOV'T, CONSUMER DATA RIGHT 2 (2018), https://treasury.gov.au/sites/default/files/2019-03/t286983_consumer-data-right-booklet.pdf [https://perma.cc/985Z-E2WK].

[331] Adam Salter & Prudence Smith, *How Does Australia's New Consumer Data Right Work?*, JONES DAY: INSIGHTS (May 2019), https://www.jonesday.com/en/insights/2019/05/australia-consumer-data-right [https://perma.cc/9TXW-8XNL]. But some commentators have criticized the mandatory two-way data sharing, arguing, for example, that

> 1. [Mandatory two-way data sharing] would undermine new and competing business models through enforced levelling of any strategic advantage such as line item data from credit card transactions that are appended by a fintech then having to be shared back to the Financial Institution; 2. For efficiency-seeking and strategic reasons, over time Data Holders may not support any other modes of

intentionally broad and includes all data that relates to the consumer, regardless of whether it was created or collected inside or outside Australia.[332] It is part of an Australian effort to give consumers access to and "the ability to transfer their personal data to third parties. . . . [B]anking is just the beginning. Not only will it include more types of financial product than seen elsewhere—eventually it will cover mortgages, loans and investments" and go even further to include telco and utility data.[333] So while the CDR requires the biggest banks to release APIs that grant access to credit card transaction and deposit account data, a general consensus exists in Australia regarding the bi-directional flow of the data initiative.[334]

(h) The Need for an Industry Standard

Understanding that standardization is key, industry players have attempted to collaboratively create standardized data elements for financial products and services.[335] In addition to helping address liability issues, standardization could raise market efficiency, as it would make it easier to conduct comparative analysis of

---

> data sharing than under CDR Open Banking, and if current drafting holds, ensures that more valuable data from the Data Recipient has to be reciprocated; and 3. data equivalency issues . . . . In addition to increasing overhead costs, the reciprocity concept would erode innovation by transferring participants' flows of enhanced data directly to competitors. Should enhanced start-up and fintech data be made freely available to the wider market, replication of products and services is possible, which will ultimately discourage innovation. Therefore it is reasonable to expect the reciprocity concept will further entrench established participants in an already highly concentrated market, leaving little incentive to drive better outcomes for the customer. Unless legislation is designed to protect intellectual property to encourage new product offerings in isolation from competitors, there is little reason for start-ups and fintechs to become CDR participants, or start new ventures within the initiative framework.

Submission from Ian Boyd, Fin. Indus. Dir., Xero Australia, to the Senate Econ. Comm. on Open Banking (2019), https://www.aph.gov.au/DocumentStore.ashx?id=492d8f37-777a-4639-9dea-214d83c2b73c&subId=666878 [https://perma.cc/4Z7M-SX29].

[332] Data may even become subject to the CDR through a reciprocity mechanism, meaning those who wish to become accredited and receive designated data at a consumer's request must be willing to share equivalent data, in response to a consumer's request. The detail and extent of reciprocity is dealt with under the CDR rules. *See* Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth) 16–18 & 25–26, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr6281_ems_58a7c56b-36e3-4388-acf8-58455b983a76%22 [https://perma.cc/GCX7-T6MH].

[333] Kocianski, *supra* note 293.

[334] *See* Salter & Smith, *supra* note 331; *see also* Kocianski, *supra* note 293.

[335] *See* Crosman, *Plaid Launches Exchange*, *supra* note 163.

compatible and clean data.[336] But while various entities, including the Open Financial Exchange ("OFX") and FS-ISAC, tried to lead standardization attempts,[337] consensus has been hard to reach.

One hurdle is that any possible solution would likely need to be part of a broader regulation meant to enhance consumers' safe and secure management of their data. Thinking of such an approach, market participants have founded the nonprofit Financial Data Exchange ("FDX") in order to move the financial services industry towards the adoption of an API standard ("FDX API") to access consumer financial data.[338] FinTech apps that employ the FDX API enable individuals to log in and be authenticated by their banks.[339] According to FDX, the only financial information that will be accessed is what consumers have specifically agreed to share with the particular FinTech apps they use.[340] This enables the FDX API to include only data that is truly needed and approved by the users.[341] The FDX API attempts to provide a framework that enables scalable technology solutions, useful even to small financial institutions that wish to offer more tech-driven services at minimal costs. The framework is royalty-free to use in perpetuity by all parties.[342]

Seeing no regulatory solution in sight, but desperate for solutions in the market-based American financial services industry, industry participants have been quick to adopt the FDX API standard. In November 2019, FDX announced that its

---

[336] Conrad Sheehan, *To Capitalize on Open Banking, the Industry Needs Standards*, AM. BANKER (Apr. 10, 2018), https://www.americanbanker.com/opinion/to-capitalize-on-open-banking-the-industry-needs-standards [https://perma.cc/YA8X-F9CG] (explaining that financial services companies typically use "disparate and customized formats to send and share information" but arguing that standardization in the financial industry would be more effective for capitalizing on APIs).

[337] *See* FS-ISAC, *supra* note 61; Press Release, OFX Consortium, *supra* note 160.

[338] *Banking on Your Data: The Role of Big Data in Financial Services: Hearing Before the H. Fin. Serv. Comm.*, 116th Cong. 1–2 (2019) (statement of Don Cardinal, Managing Dir., Fin. Data Exch.) [hereinafter Cardinal Statement], https://financialservices.house.gov/uploadedfiles/hhrg-116-ba00-wstate-cardinald-20191121.pdf [https://perma.cc/Y85E-PVUM]. *See also FDX Managing Director Don Cardinal Testifies Before Congress on Big Data in Banking and Financial Data Security*, PR NEWSWIRE. (Nov. 21, 2019), https://www.prnewswire.com/news-releases/fdx-managing-director-don-cardinal-testifies-before-congress-on-big-data-in-banking-and-financial-data-security-300963460.html [https://perma.cc/V6NX-V4QG] [hereinafter FDX] (explaining that consumer demand for FinTech apps drove the innovation in financial services, and FDX believes the entire financial ecosystem should enable consumers to use their data safely).

[339] *See* Cardinal Statement, *supra* note 338, at 4–5.

[340] *Id*.

[341] *Id.* at 2 (explaining that five core principles of financial data sharing—Control, Access, Transparency, Traceability, and Security—guide and represent FDX's understanding of the key elements of secure and visible data sharing).

[342] *Id.* at 5.

membership includes 72 members, compared to just 23 at its 2018 launch.[343] Similarly, between January 2019 and April 2020, the number of U.S. customers that the FDX API serviced grew from 2 to 12 million.[344] Plaid, which has launched Plaid Exchange, hoped to become the U.S. platform that enables open banking across the country, serving the biggest, as well as mid-sized, banks.[345]

IV. MORE ON REGULATING CONSUMER DATA SHARING

Different from the bottom-up, market-based American approach, the EU has adopted a top-down approach to consumer data.[346] The PSDII, which has been described in a headline as "EU Fires [the] Starting Gun for Banks vs. Fintech Fight over Payments," encourages technological developments that disrupt existing businesses.[347] It requires, however, using a Secure Customer Authentication ("SCA"), "which authenticates the identity of" customers "and their right to make" transactions, prior to making electronic payments.[348] SCA is based on the use of two or more elements: (i) knowledge (something only users know); (ii) possession (something only users possess, such as cell phones that can receive codes); and/or (iii) inherence (something only the users have, such as fingerprints).[349]

But the PSDII is not weakness-free. Its legally binding uni-directional flow of data is not only unfair to banks but also does not serve consumers well.[350] Additionally, the PSDII is limited—it only focuses on payments and does not cover all consumer data or even other consumer financial data, such as mortgages or savings.[351] And since the EU's approach is top-down, its weaknesses are not likely

---

[343] *The Financial Data Exchange Reports Strong First-Year Growth; Now Protecting Online Financial Data for Five Million Consumers, Including Business Customers, Through 72-Member Network*, FIN. DATA EXCH., (Nov. 6, 2019), https://financialdataexchange.org/FDX/News/Press-Releases/FDX_First_Year_Growth.aspx?WebsiteKey=deae9d6d-1a7a-457b-a678-8a5517f8a474 [https://perma.cc/645L-V3L4].

[344] *Id.*

[345] *See* Karvounis & Dhillon, *supra* note 166.

[346] *See* PSDII, 2015 O.J. (L 337) 35, *supra* note 14.

[347] Huw Jones, *EU Fires Starting Gun For Banks vs. Fintech Fight over Payments*, REUTERS (Nov. 27, 2017) https://www.reuters.com/article/us-eu-payments-regulations/eu-fires-starting-gun-for-banks-vs-fintech-fight-over-payments-idUSKBN1DR1AZ [https://perma.cc/5NV8-QTJ7].

[348] Alan Brener, *Payment Service Directive II and Its Implications*, *in* DISRUPTING FINANCE: FINTECH AND STRATEGY IN THE 21ST CENTURY 103, 115–16 (Theo Lynn & John G. Moody eds., 2019).

[349] *Payment Services Directive: Frequently Asked Questions*, EUR. COMM'N (Jan. 12. 2018), http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm [https://perma.cc/GP28-ZLZ5].

[350] *See Seismic Shift*, *supra* note 18.

[351] *See* BASEL COMM. ON BANKING SUPERVISION, *supra* note 58, at 5 ("[T]he EU's . . . PSD2 . . . appl[ies] only to specific types of data, like payments processing data.").

to be addressed quickly, and it is hard to see how industry participants' initiatives could modify the binding compliance standards or change the legal status quo.

The U.S. should regulate consumer financial data sharing in order to address key issues that should not be left unsolved. These include the problem of consumers' fictional consent, data and financial liability issues, data security risks, and even systemic risk, in addition to innovation and competition-related concerns. Without such regulation, the U.S. can find itself in a world where Visa and MasterCard own the biggest data aggregators, as a result of transactions that mainly benefit big banks.[352]

Additionally, regulating data aggregators and data sharing could also help address other issues relevant to the financial industry, such as data aggregators' operation as gatekeepers of FinTech operations and the possibility of banks' operating as platforms, as further explained in this section.

A. Rating Agencies—An Analogy

Broad access to financial data increases the chance that information may be lost, stolen, or misused by data aggregators. Thus far, regulators have ignored data aggregators' activities and the risks associated with them. However, if Visa and Mastercard were to own the biggest data aggregators, they would essentially become the gatekeepers and the toll collectors for all types of FinTech and open-banking operations.[353] Therefore, the potential acquisitions of large data aggregators should matter to regulators, along with the way data aggregators conduct their operations and how those operations impact consumers and the financial system.

Regulating data aggregators' operations is not necessarily bad for business. Lighter-touch regulation also played a key role in the 2008 financial crisis. In particular, the major rating agencies ("RAs")—Moody's, Standard & Poor's, and Fitch—contributed to the crisis with their high ratings of residential mortgage-backed securities that facilitated the development of a bubble. Once it burst, disastrous consequences led to the post-crisis regulation of RAs.[354] RAs prepare, publish, and maintain credit ratings on investments. Companies that issue securities want a rating from the RAs in order to better market their securities, increase their offering price, or fulfill contractual requirements posed by actors with whom they transact.[355] In our signaling economy, these ratings inform institutional investors whether investments are sound, and so investors highly consider the opinions of RAs

---

[352] *See* Crosman, *Mastercard and Visa Gobble Up*, *supra* note 34.

[353] *Id*.

[354] *See* JOSEPH C. LONG, MICHAEL J. KAUFMAN & JOHN M. WUNDERLICH, 12A BLUE SKY LAW § 9:154 (2010) (updated June 2020).

[355] *Id*.

who function as gatekeepers.[356] The three big RAs determine businesses' creditworthiness.[357]

In an era where data aggregators have essentially become the gatekeepers of consumer financial data, their interaction with financial institutions and FinTech companies should be regulated, even if the data aggregators mainly function as middlemen. RAs, for example, are also gatekeepers that usually do not issue or sell securities themselves. But, courts have determined that their ratings of securities can be viewed as *de facto* false statements of fact, even if they are usually held to be professional opinions.[358] Opinions, much like facts, can be substantially incorrect or misleading and thus must adhere to the same legal standards.[359] Therefore, while RAs usually only assign ratings on securities issued by other entities, they can still face secondary liability under blue sky laws, state common law, and even primary scheme liability. Secondary liability attaches to any participant that helps security sellers, including the assignment of ratings that induce investors to buy securities.[360] This could be somewhat analogous to data aggregators arguing that the apps they helped connect to banks are at fault for potential risks that materialized and the damage that resulted. Rather, secondary liability should attach to data aggregators if they helped FinTech companies gain access to financial data, and the FinTech companies then took advantage of the data in an illegal or harmful way.

Likewise, the common law recognizes claims for fraud and negligent misrepresentation against RAs. Specifically, RAs are subject to a common law cause of action if they give ratings without exercising reasonable care that the investor then reasonably relied upon.[361] The proof standard for a negligent misrepresentation argument is favorable for investors as the standard is lower than scienter.[362] This common law theory, with some changes, can be useful in thinking of ways to regulate data aggregators' interactions with financial institutions and FinTech companies, in connection with their commitment to consumer protection principles.

---

[356] *See, e.g.*, J&R Mktg., SEP v. Gen. Motors Corp., 549 F.3d 384, 393 (6th Cir. 2008) (describing credit-rating agencies as financial market gatekeepers).

[357] *See* LONG, KAUFMAN & WUNDERLICH, *supra* note 354.

[358] *See, e.g.*, Plumbers' Union Local No. 12 Pension Fund v. Nomura Asset Acceptance Corp., 632 F.3d 762, 775 (1st Cir. 2011) (outlining instances in which an opinion may be held as false or misleading).

[359] *See, e.g.*, Omnicare, Inc. v. Laborers Dist. Council Const. Indus. Pension Fund, 575 U.S. 175, 179 (2015) (interpreting Section 11 of the 1933 Act); NNN Durham Off. Portfolio 1, LLC v. Grubb & Ellis Co., No. 12-CVS-3945, 2016 WL 7489690, at *26–27 (N.C. Sup. Ct. 2016) (interpreting the North Carolina Securities Act).

[360] *See, e.g.*, *In re* Nat'l Century Fin. Enter., Inc., 580 F. Supp. 2d 630, 649–50 (S.D. Ohio 2008) (describing Ohio blue sky laws).

[361] *See, e.g.*, Anschutz Corp. v. Merrill Lynch & Co., 785 F. Supp. 2d 799, 827–28 (N.D. Cal. 2011) (sustaining claim against credit rating agency for California common law negligent misrepresentation); King Cnty., Washington v. IKB Deutsche Industriebank AG, 708 F. Supp. 2d 334, 336–47 (S.D.N.Y. 2010) (sustaining claim against credit-rating agency under New York common law fraud).

[362] *See, e.g.*, *In re* Nat'l Century Fin. Enter., Inc., 580 F. Supp. 2d at 640–44.

Data aggregators, as gatekeepers of consumer data, should be subject to a common law claim if they facilitate, without exercising reasonable care, transactions that caused harm between financial institutions and FinTech companies that do not meet certain pre-determined standards.

The focus on potential harm is key. The greater the amount of consumer financial data held by data aggregators, the greater the possible harm to consumers resulting from a data breach.[363] Currently, data aggregators are not subject to a particular regulatory scheme similar to financial institutions. In addition to state consumer protection laws, data aggregators are only subject to generic federal consumer protection laws, which the FTC enforces.[364] Thus, the absence of regulatory oversight of data aggregators and the flow of consumer financial data via FinTech apps raise major risks for consumers,[365] especially, as the data aggregators' security practices are not comparable to financial institutions' standards and the FinTech apps third-party providers' security practices are even weaker.[366]

The provisions in the GLBA govern how financial institutions[367] must use certain tools to ensure the security and confidentiality of customer data, safeguard against any foreseen harms, and shield against unapproved access to databases and systems.[368] Financial institutions are required to describe their practices to clients, and show how their institutions' data security plans and policies are protecting confidential information.[369] The federal banking agencies, the SEC, CFTC, and the FTC enforce the GLBA.[370] As part of its enforcement, the FTC stated the primary information security provisions in its Safeguards Rule,[371] which requires financial institutions to evaluate and create a clear security plan that details an entity's business strategy in connection with guarding customer data, including detecting and managing system failures.[372] Referring to data aggregators and FinTech

---

[363] 2018 Treasury Report, *supra* note 52, at 37 ("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.").

[364] To the extent that data aggregators or FinTech companies are providing services to a bank, the services provided are subject to the third-party oversight framework imposed by banking regulators under the Bank Service Company Act. *See* Bank Service Company Act, 12 U.S.C. §§ 1861–67; AM. BANKERS ASS'N, FINTECH—PROMOTING RESPONSIBLE INNOVATION 8 (2018), https://www.aba.com/Advocacy/Documents/fintech-treasury-report.pdf [https://perma.cc/NDG2-3WXZ].

[365] AM. BANKERS ASS'N, *supra* note 364, at 3–4.

[366] 2018 Treasury Report, *supra* note 52, at 37.

[367] Under the GLBA, financial institutions include companies that offer consumer financial products or services like loans, financial or investment advice, or insurance. 15 U.S.C § 6827(4)(B).

[368] *Id.* § 6801(b).

[369] *Id*. § 6803(c)(3).

[370] 2018 Treasury Report, *supra* note 52, at 39.

[371] 15 U.S.C. §§ 6801, 6805(b); 16 C.F.R. pt. 314 (2002).

[372] 16 C.F.R. §§ 314.3–.4 (2002).

companies, the FTC has noted that both entities offer financial services and products as financial institutions under GLBA and are subject to its rules.[373]

Becoming more aware of the concerns associated with consumer data sharing, the House Committee on Financial Services held a hearing on November 21, 2019, that included the following two new legal initiatives: (i) The Safeguarding Non-Bank Consumer Information Act, H.R. ____, which seeks to clarify GLBA's privacy provisions and give the CFPB authority over the Safeguards Rule; and (ii) the Financial Information Data Modernization Act, H.R. ____, which seek to clarify "non-financial institutions" and "financial data" for the protection of the consumer under the GLBA.[374] The hearing focused on how big technology firms, which have increasingly entered the financial industry, are subject to an unclear legal framework, compared to financial institutions.[375] For example, how big technology platforms' consumer data has "been utilized for credit underwriting [decisions], discriminatory housing advertisements, and other purposes."[376]

The hearing addressed the need for a federal regulation.[377] In the absence of such regulation, the complex and inconsistent regulatory environment may jeopardize the country's position as a global leader in technology and add undesired complexities and inefficiencies.[378] The patchwork benefits mainly the multimillion-dollar data compliance industry and puts small business owners and entrepreneurs at a disadvantage,[379] causing them to become more dependent on bigger, wealthier players. Otherwise, if small business owners fail to comply with regulations, the cost will be high,[380] and consumers will see the direct effects. Hence, we need a federal law that offers a reliable set of standards for online as well as offline businesses,

---

[373] *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED. TRADE COMM'N (Apr. 2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying [https://perma.cc/E4SE-2FP8] (stating that the Safeguards Rule applies to companies that receive information about the customers of other financial institutions).

[374] *Banking on Your Data: The Role of Big Data in Financial Services: Hearing Before the H. Fin. Servs. Comm.*, 116th Cong. (2019) (memorandum by Fin. Servs. Comm. Majority Staff), https://financialservices.house.gov/uploadedfiles/hhrg-116-ba00-20191121-sd002.pdf [https://perma.cc/ T8GY-PHP3].

[375] *Id.*

[376] *Id.* (quotation omitted).

[377] *See* Michael Beckerman, *Americans Will Pay a Price for State Privacy Laws*, N.Y. TIMES (Oct. 14, 2019), https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html [https://perma.cc/LX6D-5FCF] (explaining that states are rushing to pass their own legislation, creating a patchwork of privacy laws, as the modern data economy is too big to regulate at the state level).

[378] *Id*.

[379] *Id*.

[380] A study by IBM Security and the Ponemon Institute showed that the global average cost of a data breach is $3.92 million. *2019 Cost of a Data Breach Report*, IBM, https://www.ibm.com/security/data-breach [https://perma.cc/36GL-DVTZ] (last visited July 7, 2020). At $8.19 million, the U.S. had the highest average cost in the world. *Id.*

irrespective of where their users are located,[381] that would offer safeguards for consumers and predictability for companies.[382]

Any such federal-level regulation of data aggregation should be analogous in some respects to RAs regulation as gatekeepers and may involve tasking data aggregators with managing digital identities too.[383] This would mean providing digital versions of individuals' identities, thereby replacing identity cards, which people typically carry with them. Witnessing the growing marketplace for digital identities, various entities already use some type of digital identity to verify payment data or offer different services.[384] In terms of efficiency, data aggregators, with API-enabled access to customer data from the different financial players across the market, will perform processes needed for digital identities' verification faster, more effectively, and at lower costs.[385]

B. Open Banking: A Platform–Like Business Model?

Mandatory open banking initiatives can push banks to involuntarily become "Platform as a Service" kind of providers.[386] Operating as a platform that relies on APIs might benefit all stakeholders. Banks could securely and quickly exchange data

---

[381] Discussing this issue in the context of banks, *see, e.g.*, Nat'l City Bank of Ind. v. Turnbaugh, 463 F.3d 325, 332 (4th Cir. 2006) ("[When banks] are unable to operate under uniform, consistent, and predictable standards, their business suffers, which negatively affects their safety and soundness.").

[382] *See, e.g.*, Howard H. Stevenson & Mihnea C. Moldoveanu, *The Power of Predictability*, HARV. BUS. REV. (July–Aug. 1995), https://hbr.org/1995/07/the-power-of-predictability [https://perma.cc/VB9W-4WLU] (discussing how implementing measurable and predictable business practices can assist in creating certainty and improving businesses).

[383] Erin Jane Illman, *Data Privacy Laws Targeting Biometric and Geolocation Technologies,* 73 BUS. LAW. 191, 194–95 (2018).

[384] *Id.* at 195 ("As companies look to the future, many believe that drivers' licenses, passports, and other forms of identification will be replaced with digital identification that can be accessed and verified from anywhere in the world with a single fingerprint or eye scan.").

[385] Realizing this potential, in January 2020, news broke of Visa's interest in purchasing Plaid for $5.3 billion. *See* Morris & Roberts, *supra* note 41 ("Plaid occupies a gatekeeper role between conventional banks and the app-based upstarts—including Venmo, Chime, Coinbase and Robinhood—trying to disrupt them.").

[386] "PaaS, or Platform-as-a-Service, is a cloud computing model that provides customers a complete platform—hardware, software, and infrastructure—for developing, running, and managing applications without the cost, complexity, and inflexibility of building and maintaining that platform on-premises." Sunil Joshi, *PaaS (Platform-as-a-Service)*, IBM, https://www.ibm.com/blogs/cloud-computing/2014/02/what-is-platform-as-a-service-paas/ [https://perma.cc/4PMC-XNQF] (last visited July 7, 2020); *see also* NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 800-145, THE NIST DEFINITION OF CLOUD COMPUTING 2–3 (2011).

with third-parties, and profit from it.[387] Similarly, allowing users to interact with banks as platforms by incorporating APIs would allow third-parties to plug straight into the relevant code, historical information, and data feeds. Moreover, parties could connect, integrate, create, and exchange value,[388] as banks would function like matchmakers, integrating all parties,[389] enabling data aggregators to empower consumers by letting them monitor all accounts simultaneously.[390]

Some banks have started to consider the platform/integration concept.[391] Information economy companies such as Google, Netflix, Uber, Airbnb, Facebook, Instagram, Amazon, eBay, Alibaba, and even PayPal have all transitioned into models where they engage in e-commerce using APIs that connect smartphones, and integrate data analytics, cloud computing, AI, and social-production.[392] Among the

---

[387] Falon Fatemi, *How APIs Can Transform Your Company*, FORBES (Mar. 21, 2019, 3:37 PM), https://www.forbes.com/sites/falonfatemi/2019/03/21/how-apis-can-transform-your-company/#1ab2d58d668c [https://perma.cc/SL2J-2D49].

[388] *See* GEOFFREY G. PARKER, MARSHALL W. VAN ALSTYNE & SANGEET PAUL CHOUDARY, PLATFORM REVOLUTION: HOW NETWORKED MARKETS ARE TRANSFORMING THE ECONOMY—AND HOW TO MAKE THEM WORK FOR YOU 2 (2016) (explaining that the key to the platform business model is that it "uses technology to connect people, organizations, and resources in an interactive ecosystem in which amazing amounts of value can be created and exchanged"). *See also* Zachariadis & Ozcan, *supra* note 155 at 12–13.

[389] *AFT Vantage Point: Ron Shevlin Weighs in on the Platformification of Fintech*, ASS'N FOR FIN. TECH. (Jan. 8, 2019), http://aftweb.com/aws/AFT/pt/sd/news_article/209486/_PARENT/layout_details/false [https://perma.cc/SH9P-9F9G].

[390] *See* Crosman, *Finra's Dire Warning, supra* note 36. Explaining their importance, one data aggregator executive stated that "I would argue the system would be less safe if we weren't in it. . . . I have a 401(k)—I generally don't check it regularly, so if funds are missing, how are you going to know that as a consumer and fix that? We make that easier by allowing for the free flow of data." *Id.*

[391] In April 2019, Goldman Sachs announced its plans to start integrating between developers and its clients. "The bank is also offering engineers $100,000 to build new applications using the bank's code. . . . By letting outsiders tinker with its code, Goldman hopes to . . . earn the loyalty of computer-driven 'quant' traders . . . ." Liz Hoffman, *Goldman's Trading Floor Is Going Open-Source–Kind Of*, WALL ST. J. (Apr. 3, 2019, 9:01 AM), https://www.wsj.com/articles/goldmans-trading-floor-is-going-open-source-kind-of-11554285602 [https://perma.cc/F6LW-UGEG]. Similarly, JPMorgan recently started permitting customers to use certain features of its trading engine. Hugh Son, *JPMorgan Chase & Co. Recently Began Allowing Clients to Use Some Features of Athena, Its Trading Engine*, CNBC (Nov. 5, 2018, 10:06 AM), https://www.cnbc.com/2018/11/05/jp-morgan-selling-trading-software-in-glimpse-of-wall-streets-future.html [https://perma.cc/D9RA-7XE4]. Likewise, Bank of America introduced a new digital dashboard designed to make it easier for entrepreneurs to manage their financials. *Bank of America Introduces New Digital Tools for Small Business*, BLOOMBERG (Feb. 6, 2019), https://www.bloomberg.com/press-releases/2019-02-06/bank-of-america-introduces-new-digital-tools-for-small-business [https://perma.cc/74YV-N8E7].

[392] *See, e.g.*, José Manuel de la Chica, *PSD2 and Open APIs in Banking: Is This the Start of the Exponential Era in FinTech and Online Payments*, BBVA (June 3, 2016),

model's advantages are the higher rate of apps, both in terms of quantity and development speed.[393] Moreover, banks that would adopt this model would be able to monetize the APIs in the digital-economy, through which outside innovators can develop API-consuming apps and pay fees in order to use the API.[394] Lastly, for banks, the adoption of a platform model might prove to be superior to other models as it could result in lower transaction costs economics.[395] Operating as a platform, banks can reduce searching, matching, negotiation, and contracting costs,[396] and lower information asymmetries.[397]

Realizing these benefits, data aggregators do not want to be left behind and miss this opportunity to serve as a middleman. Therefore, they have initiated ways to stay relevant, such as supporting the biggest banks in their own created systems. For example, in 2019, JPMorgan Chase entered into an agreement with a leading data aggregator that addresses some concerns relating to sharing financial data.[398] According to the agreement, customers provide their consent to share data with any

---

https://bbvaopen4u.com/en/actualidad/psd2-and-open-apis-banking-start-exponential-era-fintech-and-online-payments [https://perma.cc/A6Q7-RP45]; PARKER, ALSTYNE & CHOUDARY, *supra* note 388, at 2.

[393] Platforms offer a scalable route for faster development. As an example

> [C]onsider the case of iPhone as a product platform. Apple would have never been able to develop such an immense number of applications by using their organisational resources alone. Instead, by opening up their product and making its features available to an entire community of developers through open APIs, they managed to unlock new sources of value at a much higher rate both in terms of quantity . . . but also in terms of speed . . . and scope . . . .

Markos Zachariadis, Pinar Ozcan & Dize Dinckol, *The Economics and Strategy of Platforms: Competing in the Era of Open Banking*, *in* THE BOOK ON OPEN BANKING 59, 61 (2018).

[394] Hoffman, *supra* note 391. Specifically,

> Goldman has written hundreds of code snippets, known as APIs, that allow users to plug straight into Marquee. They can tap Goldman's historical data to find out whether a trading strategy would actually make money and assemble customized baskets of securities to hedge their portfolios. Many of these APIs will be available on GitHub.

Id.

[395] Ronald Coase constructed society's understanding of the role of transaction costs. *See* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 23 (6th ed. 2003) (stating that "new law and economics" began with Ronald Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960), and Guido Calabresi, *Some Thoughts on Risk Distribution and the Law of Torts*, 70 YALE L.J. 499 (1961)).

[396] *See* Zachariadis & Ozcan, *supra* note 155, at 9.

[397] *Id*.

[398] *See Increase Customers' Control*, *supra* note 60.

particular FinTech app, and using the bank's platform, access a transparent dashboard with the types of information that can be shared about them and decide what to share with which app.[399] Likewise, addressing concerns regarding the extent of permission, using token-based security in the secure API[400] enables JPMorgan Chase to share only the type of data that the FinTech app or third-party needs and only from accounts specified by customers.[401] The third-party will use the information to help customers make better, more informed decisions about their accounts, and customers will be able to see which third-parties got linked to their accounts and cancel access to apps at any time.[402]

But, the bank platform-model option has weaknesses too, and so without regulation requiring it, it is not clear how broadly adopted it would ever be. First, as discussed above, for resources-related reasons, smaller banks are unable to adopt it as easily, but without it will not be relevant.[403] Thus, for such mid-size and smaller banks, solutions like Plaid's "API connectivity in a box" would be ideal. Second, adopting such a model could be a bad strategic move for some of the big banks, as they could unintentionally give rise to competitors or not notice new services built on their technology that they have spent a long time creating and designing.[404] For example, Zynga, maker of the FarmVille game, created its online-gaming empire by utilizing Facebook's technology and users.[405] Similarly, Uber utilized Google Maps to enable its drivers to find their way while navigating.[406] Lastly, there might be some merit in the FinTech companies' arguments against limiting the scope of the permission to data they are granted and its impact on innovation.

---

[399] *Id*.

[400] *See* Crosman, *Data-Sharing Debate*, *supra* note 35. Crosman notes,

> Users can set those tokens to expire or delete, or modify them through the bank website. . . . The tokenization means "you're not typing your user name and password into the aggregator's service and giving them credentials[.]" . . . The user logs in to the aggregator and is redirected to the bank account to authorize the aggregator to do certain things. . . . "Standing on the shoulders of OAuth is really good idea, [sic] because it's a robust standard that's used in many places."

Id. (quoting Joseph Lorenzo Hall, chief technologist and director of the internet architecture project at the Center for Democracy and Technology in Washington).

[401] *Id*.

[402] *See id*.

[403] *See* Shevlin, *supra* note 121.

[404] *Id*. *See* Shevlin, *Plaid Launches API Exchange, supra* note 161.

[405] *See* Dean Takahashi, *How Zynga Grew from Gaming Outcast to $9 Billion Social Game Powerhouse*, VENTURE BEAT (Dec. 12, 2011, 7:00 AM), https://venturebeat.com/2011/12/12/zynga-history/view-all/ [https://perma.cc/SAG3-G3ZY].

[406] *See* FDX, *supra* note 338, at 7.

V. CONCLUSION

Customers should have control of their data, and manage it as they see fit, but there are many risks associated with doing so, especially when dealing with financial data. Therefore, any attempt to regulate the management of consumer financial data requires careful tiptoeing around the issue, as laws that emphasize privacy and data security could result in creating difficulties for consumers to access their information. However, despite the potential harms, consumer financial data should not be a battleground among banks, FinTech companies, and data aggregators. If managed properly, data sharing could turn into a consumer empowering tool that offers innovative services and products,[407] while complying with principles of consumer protection and systemic risk.

Consumer financial data should be shared in a safe, secure, and symmetrical way, based on clear, logical, and widely accepted standards of operation outside of the siloed approach that is currently still adopted in the financial services industry.[408] Smartphones and apps are not going away.[409] The open banking trend, driven by customer-permissioned sharing of data, created and enabled by the proliferation of smart devices, has the potential to transform banking services and banks' business models. And banking might be just the beginning. Indeed, if we get this singular consumer right in the banking context, we might be able to even go further to include telco and utility data. After all, banking is different from other industries, and innovative changes taking place in other sectors with respect to data sharing might be dangerous to adopt in the banking industry. As banks innovate and try to stay relevant, it is important that regulators and businesses remember that.

While industry consortia or the adoption of a platform model could help create the open banking common definitions and standards that are needed in order to make data sharing usable, a market-led solution will not be enough. The CFPB must develop a carefully designed, thoughtful regulation, which will prioritize consumers' interests and make data sharing transparent, but not overly taxing for consumers to understand and consent to.

Data aggregators would benefit from regulation that anchors them as the key financial players they have become in the U.S., with rights and obligations as gatekeepers that bridge between FinTech companies and banks, even in a futuristic

---

[407] Kristin Moyer, *Screen-scraping vs. APIs Is a Sideshow. Here's the Real Battle*, AM. BANKER (June 15, 2016, 1:19 PM), https://www.americanbanker.com/opinion/screen-scraping-vs-apis-is-a-sideshow-heres-the-real-battle [https://perma.cc/7DUT-ECTR].

[408] Financial institutions are known for operating in "silos": loans in one department, deposits in a different one, and mortgages at a different place. Chris Nichols, *How to Stop Treating Bank Departments Like Silos*, CTR. ST. BANK (June 4, 2018), https://csbcorrespondent.com/blog/how-stop-treating-bank-departments-silos [https://perma.cc/KL74-DLC4].

[409] Even the U.S. 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." Riley v. California, 573 U.S. 373, 385 (2014).

era in which screen-scraping would be less used. Banks, which must adapt to the new ecosystem, could also benefit from working with FinTech companies to improve and enrich their offered products and services. Operating as a platform might not be such a bad thing for big banks, and more importantly, working with FinTechs would enable banks to get more timely, relevant, and quality data, than they currently have access. For example,

> The ability to update data when it's available is a win for banks that want to use timely data from other institutions' accounts. But . . . if customers don't log in, updates from the aggregated banks don't happen, and banks don't see the transaction data from other institutions until the customer logs in again.[410]

Lastly, carefully designed regulation will empower consumers, help them gain legal control over their data, benefit from increased competition, and enjoy innovative products and services. This does not need to be tolling for consumers. There are ways to offer more transparency and guidance in order to obtain informed consent to data sharing, without drowning consumers in lengthy detailed explanations and warnings. The CFPB's structure and actions might face some challenges, but the bureau has proven itself as highly effective in enforcing financial protection laws, and succeeding in enforcement actions,[411] which are key in order to get consumer financial data sharing right.

---

[410] Shevlin, *Plaid Launches API Exchange*, *supra* note 161.

[411] *See, e.g.*, Christopher L. Peterson, *Consumer Financial Protection Bureau Law Enforcement: An Empirical Review*, 90 TUL. L. REV. 1057, 1093–1103 (2016); Gretchen Morgenson, *The Watchdog Protecting Consumers May Be Too Effective*, N.Y. TIMES (Feb. 10, 2017), https://www.nytimes.com/2017/02/10/business/consumer-financial-protection-bureau-gretchen-morgenson.html [https://perma.cc/9ZSN-6DWU].