2023

Navigating the Potential Regulatory Landscape Under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act for Fintechs

Kelly Hogan

Navigating the Potential Regulatory Landscape Under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act for Fintechs

Kelly Hogan

I. INTRODUCTION

A. The Statute, its Objective, and the Need it Fills

While the Dodd-Frank Wall Street Reform and Consumer Protection Act ("the Act") was passed to reform the financial regulatory landscape and protect consumers, one of its ancillary objectives was to foster innovation.[1] This is apparent by the plain language of Section 1021 of the Act, which states that:

> [t]he Bureau is authorized to exercise its authorities . . . for the purposes of ensuring that . . . consumers are provided with timely and understandable information to make responsible decisions about financial transactions . . . [and that] markets for consumer financial products and services operate transparently and efficiently to facilitate access and innovation.[2]

By potentially providing consumers with more access to, and autonomy over the portability of, the financial data they generate, the Act seeks to address the lack of competition that is restraining innovation in the financial services industry. A key component of the Act that works to promote competition and, therefore, innovation is Section 1033. Section 1033 of the Act mandates that "covered persons" make available to consumers, upon their requests, any information relating to the requesting consumer's financial product or service that they obtained from the covered person (including any transactions, costs, charges, and usage data) and in the covered person's control.[3] The Act also prescribes that information be made available in

---

[1] President Barack Obama, Remarks by the President at Signing of Dodd-Frank Wall Street Reform and Consumer Protection Act (July 21, 2010), available at https://obamawhitehouse.archives.gov/the-press-office/remarks-president-signing-dodd-frank-wall-street-reform-and-consumer-protection-act.
[2] Pub. L. No. 111-203 §§ 1021(b)(1), (5), 124 Stat.1979-1980 (codified at 12 U.S.C. §§ 5511(b)(1), (5) (2010)).
[3] Pub. L. No. 111-203 § 1033(a), 124 Stat. 2008 (codified at 12 U.S.C. § 5533(a) (2010)).

electronic format that is usable by consumers,[4] and grants the Consumer Financial Protection Bureau (the "Bureau") the authority to promulgate rules aimed at promoting, developing, and using standardized forms of this information, including machine readable files that would be made available to consumers[5]. There are modest limits to what data must be made available to consumers.[6] The Bureau is afforded the power and discretion to collaborate with other Federal agencies, including the Federal Trade Commission, to (1) ensure the uniformity of rules as they relate to covered persons, (2) take into account the conditions covered persons face domestically and abroad, and (3) ensure that the Bureau does not promulgate rules that would favor any type of technology used to comply with rules or regulations promulgated under Section 1033.[7]

Industry expert, Thomas P. Brown, expressed in his pre-Symposium submission to the Bureau[8] that consumers' lack of options as to how they can share their data in order to receive bespoke financial services limits their leverage to be able to exit from relationships with preeminent financial service providers (i.e., big banks) even when they are dissatisfied.[9] This lack of consumer-data portability exacerbates the lack of financial-services options consumers have because the incumbent financial institutions do not face competition and, therefore, do not have a sense of urgency to innovate in order to increase customer satisfaction and retention.[10] Similarly, Fintechs that would otherwise provide an infusion of new financial-services solutions

---

[4] *id.*
[5] Pub. L. No. 111-203 § 1033(d), 124 Stat. 2008 (codified at 12 U.S.C. § 5533(d) (2010)).
[6] Pub. L. No. 111-203 §§ 1033(b)(1)-(4), 124 Stat. 2008 (codified at 12 U.S.C. §§ 5533(b)(1)-(4) (2010))(stating "a covered person may not be required . . . to make available . . . any confidential information, including an algorithm used to derive credit [or similar] scores . . . [;] information collected . . . for the purpose of preventing fraud . . . or making any report regarding other unlawful or potentially unlawful conduct [;] any information required to be kept confidential by any other provision of law; or [] any information that the covered person cannot retrieve in the ordinary course of its business with respect to that information")
[7] Pub. L. No. 111-203 §§ 1033(e)(1)-(3), 124 Stat. 2008 (codified at 12 U.S.C. §§ 5533(e)(1)-(3) (2010)).
[8] *see infra* § II(A)(1)(b).
[9] Letter from Thomas P. Brown, Section 1033 of Dodd-Frank—A Decade of Waiting for the Green Flag to Drop (pre-Symposium submission), at 1 (2020) (on file with the Bureau).
[10] *See id.*

are also disincentivized from doing so, as consumers would be unable to reward their innovation by easily sharing data with them and paying for their product.[11] This proposition rests on the principle of network effects, which is the principle that a platform's value increases as the number of participants increases. A regulatory landscape that would create a vast amount of consumers with portable data (i.e., a choice to enter and exit relationships with financial service providers as they please, sharing specific data they please) would spur innovation by new Fintechs entering the market to win consumers' business, which would encourage incumbent financial institutions to create new products and services to retain customers; this innovation would prompt consumers to utilize their increased data portability to engage in the marketplace of financial products and services. A flourishing system such as this one is a great example of positive network effects, where increased consumer engagement leads to an increase in the rate of innovation, and vice versa.

B. Persons Covered by the Act

While certain sections of Title X of the Act qualify which covered persons can be regulated by the Bureau,[12] Section 1033 does not so limit the Bureau's reach. Therefore, by the plain language of the statute, the persons subject to the Bureau's rulemaking under Section 1033 will consist of any individual, business, trust, estate, cooperative organization, or other entity "that engages in offering or providing a consumer financial product or service," or any service-providing affiliate of such person, presumably applying to affiliates who provide products as well.[13] "Consumer financial product" will include: (1) consumer loans and credit; (2) loan servicing and brokering; (3) leases of personal or real property; (4) taking of deposits and

[11] *See id.*
[12] *See, e.g.*, 12 U.S.C. §§ 5514-5516 (2010).
[13] 12 U.S.C. § 5481(6), (19) (2010).

transferring or acting as custodian of funds or financial instruments; (5) stored value instruments (if the seller is a party to the stored-value contract); (6) check-cashing, -collection, or -guaranty services; (7) payments, or services related to facilitating payment; (8) financial advisory services other than those provided by a person regulated by the Securities Exchange Commission within their regulated capacity; (9) consumer reporting (credit scores); (10) debt-collection; as well as (11) "such other financial product or service as may be defined by the Bureau . . . [if] such financial product or service is . . . [1] entered into . . . to evade any Federal consumer financial law[,] or [2] permissible for a bank or for a financial holding company to offer or to provide under any provision of a Federal law or regulation applicable to a bank or a financial holding company, and has, or likely will have, a material impact on consumers."[14] However, modest limitations to the term "covered persons" may be forthcoming through Bureau rulemaking, as one of the Bureau's forty-five questions presented in its Advanced Notice of Proposed Rulemaking (the "ANPR") seeks input regarding whether "there [are] types of data holders that should not be subject to the access rights in section 1033," or if there are certain types of data holders that should be subject to modified rules relating to data access rights.[15]

II. ANALYSIS

This paper 1) analyzes stakeholder concerns regarding the potential rules or regulations to be promulgated by the Bureau pursuant to Section 1033 of the Act by reviewing a) the Bureau's actions to date regarding Section 1033, and b) the disparate impacts of regulatory regimes in other jurisdictions, while keeping the plain text of the statute in mind; and 2) identifies potential

[14] 12 U.S.C. §§ 5481(15)(A)(xi)(I)-(II); *but see*, 12 U.S.C. § 5481(15)(B)(i) (stating that certain products or services provided by affiliates of covered persons will not be included in subsection (A)(xi)(II) of this clause [(which discusses those permissible for a bank to offer)], including those used for identity authentication; "fraud or identity theft detection, prevention, or investigation"; document retrieval or delivery; public records information retrieval; and anti-money laundering activities).

[15] Advanced Notice of Proposed Rulemaking, 85 Fed. Reg. 71003, 71010 (Nov. 6, 2020).

pros, cons, and tradeoffs between potential regulatory regimes from the perspective of startup businesses in the Fintech industry, with particular focus on the potential designs' effects on cost of doing business, barriers to entry, and consumer choice and power.

A. Stakeholder Concerns Regarding Potential Design Choices

This paper first reviews the Bureau's official actions up to present, as well as the disparate impacts of unique regulatory regimes in other jurisdictions, in order to provide context for recommendations as to how the Bureau can best use its authority to promote data portability, competition, and innovation; we address each in turn, keeping in mind the plain-text statutory interpretation that will instruct any rulemaking.

1. The Bureau's Actions to Date Regarding Section 1033

a. The 2016 Request for Information and Subsequent Principles

In 2016 the Bureau solicited information from stakeholders in the financial services sector by publishing an official Request for Information in the Federal Register (the "2016 RFI") to better understand the benefits and risks to consumers associated with consumer-authorized data access, and to aid the Bureau in publishing principles to help market participants and policymakers develop practices and procedures to protect consumers, maximize the benefit consumers receive from safe access to their data, and boost innovation.[16] The Bureau received input from a wide range of stakeholders, including financial institutions (i.e., "banks" or "data holders"), data aggregators, data users (or "Fintechs" and, together with data aggregators, "third parties"), trade associations, consumers, and consumer advocates. The Bureau used this information to develop its 2017 report, "Consumer-authorized financial data sharing and aggregation: Stakeholder insights that inform the Consumer Protection Principles" (the

[16] Request for Information Regarding Consumer Access to Financial Records,81 Fed. Reg. 83806 (Nov. 22, 2016).

"Stakeholder Insights Report"), and its 2017 Consumer Protection Principles (the "Principles"). The Principles, as published, placed a priority on ensuring innovators in the data-aggregation market would safeguard consumer interests while the market continued to develop without direct regulatory intervention.[17]

In response to the feedback that the Bureau received to its 2016 RFI, it identified nine categories of concern that it deemed should each have a guiding principle.[18] The Bureau released principles for each of the nine categories, which were intended to reiterate consumer interests but did "not themselves establish binding requirements or obligations relevant to the Bureau's . . . authority."[19] This paper analyzes the seven of nine categories that have the potential to impact the scope of consumer-data portability and its methods of achievement, focusing on how the Principles were informed by the feedback received to the 2016 RFI. Those seven categories are: (1) access; (2) data scope and usability; (3) control and informed consent; (4) access transparency; (5) accuracy; (6) ability to dispute and resolve unauthorized access; and (7) efficient and effective accountability mechanisms.

(i). Access

Stakeholders agreed that consumers should have access to their own financial data, but data holders were split as to whether consumers should be able to authorize access to third parties.[20] Some data holders favored consumer-authorized access to third parties because they

[17] *See* Consumer Financial Protection Bureau, Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf (the "Principles"); Pratin Vallabhaneni, *CFPB Seeks Comments on Highly Anticipated Consumer Access to Financial Information Rulemaking*, WHITE & CASE TECH. NEWSFLASH (Nov. 3, 2020), https://www.whitecase.com/publications/alert/cfpb-seeks-comments-highly-anticipated-consumer-access-financial-information.

[18] Consumer Financial Protection Bureau, Consumer-authorized financial data sharing and aggregation: Stakeholder insights that inform the Consumer Protection Principles (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf, at 1 (the "Stakeholder Insights Report").

[19] The Principles, at 2.

[20] The Stakeholder Insights Report, at 4-5.

worried that restricting such data portability would limit their own ability to compete, while others disagreed due to concerns over consumer-data protection and the fact that, in their view, the Act does not mandate third parties be granted access to consumer data.[21]

The "access" Principle states that consumers are to have complete access to their financial data and that such access should be granted within a timely manner after consumer request.[22] The Principle also instructs that best practices consist of having financial account agreements that "support safe, consumer-authorized access, promote consumer interests, and do not seek to deter consumers from accessing or granting access to their information."[23] While this Principle does not require consumers to grant access to third parties they are "generally able to authorize ***trusted*** third parties to obtain such information from account providers to use [for consumer benefit]."[24]

The access Principle eliminates any concerns that consumers might be unable to authorize third parties to access their data. This Principle states that banks must provide consumers their data only after they request it; but since the Principles were published, stakeholders have recommended systems that could reduce friction and make consumer financial data constantly available to them while limiting third parties' ability to access the data.[25] This Principle creates ambiguity where it states "trusted" third parties may gain access to consumer

[21] The Stakeholder Insights Report; at 4; *compare* Letter from Stuart Rubinstein, Senior VP, Fidelity Investments, to Monica Jackson, Executive Secretariat, Consumer Financial Protection Bureau, at 2 (Feb. 21, 2017) (on file with the Bureau), *with* Letter from Joseph M. Gormley, Assistant VP and Regulatory Counsel, Independent Community Bankers of America, to Monica Jackson, Executive Secretariat, Consumer Financial Protection Bureau, at 2 (Feb. 21, 2017) (on file with the Bureau).
[22] The Principles, at 3.
[23] *Id.*
[24] *Id.* (emphasis added).
[25] Consumer Financial Protection 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, at 4-5 (the "Symposium Summary") (highlighting that many participants cited consumer-facing dashboards, which could reduce friction and delay between when consumers authorize the data sharing and when the data is ultimately shared).

financial data, as it is not clear who determines whether the third party is trusted; this Principle can reasonably be construed as intending that banks decide, but this could limit the consumers' autonomy over their own financial data and allow banks to withhold data for anti-competitive reasons.

(ii). Data Scope and Usability

Stakeholders were divided over data scope and usability in their responses to the 2016 RFI. Third parties generally advocated for access to unlimited data, while banks proposed a limit on data they deem extraneous.[26] Third parties expressed concern that banks could act in an anti-competitive manner by withholding data that could otherwise maximize the effectiveness of financial products and services.[27] Banks argued that aggregators may gain access to extraneous data that could increase the privacy risks consumers face, which could expose banks to legal liability and risks of loss of business.[28] Banks also expressed concern that if certain data they deem proprietary is shared, competitors and Fintechs could reverse engineer some of their products or services.[29] To address these concerns, banks proposed a limit on consumer-authorized access and use of data "to the express purpose for which the consumer has authorized that access."[30]

The Principle sets forth the type of data that may be made portable, which includes "any transaction, series of transactions, or other aspect of consumer usage; the terms of any account, such as a fee schedule; realized consumer costs, such as fees or interest paid; and realized consumer benefits, such as interest earned or rewards."[31] The data must be in a form readily

[26] The Stakeholder Insights Report, at 4-5.
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] The Principles, at 3.

usable by the consumer or the third party they authorized to use their data.[32] Authorized third parties can only access that data needed "to provide product(s) or service(s) selected by the consumer and only maintain such data as long as necessary."[33]

This Principle is ambiguous where it limits third-party access to data that is "necessary to provide product(s) or service(s) selected by the consumer and only maintain such data as long as necessary."[34] It is unknown who decides what data is necessary to provide certain products or services, and this lack of clarity has the potential to increase the cost of compliance that third parties face, as well as increase friction and slow down data sharing and portability in order to make time for close review to ensure that extraneous data is not being shared. "Use cases" are being developed to address this concern and will be discussed later in this paper.

(iii). Control and Informed Consent

Stakeholders generally agreed that consumers should have the power and control to grant authorization and revoke it at will.[35] Banks expressed concern that consumer-data-sharing agreements with data users will not provide adequate means of revoking access, or that multiple agreements between a consumer and different third parties will make it hard for the consumer to manage such agreements or comprehend the ways in which each agreement differs and how to invoke their rights under each separate agreement.[36]

The Bureau's Principle contemplates a system in which data users share responsibility in giving effect to consumers' intentions. The Principle states that sharing agreements with third parties should disclose terms of access (including frequency, data scope, and retention period),

[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] The Stakeholder Insights Report, at 5.
[36] *Id.*, at 6.

storage, use, and disposal in a way consumers understand and that are consistent with what a consumer would expect the terms to be when taking into account the product(s) or service(s) they are obtaining from the third party.[37] The Bureau provides clear direction under this Principle where it states data users are to be responsible for implementing consumer-initiated revocations in a "timely and effective manner," with such revocations "provid(ing) for third parties to delete personally identifiable information . . . at the discretion of the consumer."[38]

This Principle is straightforward, and it would likely only require modest effort for Fintechs to comply with the required contractual terms. While this Principle is non-binding, it points to potential rulemaking that would require Fintechs to delete data that has been revoked by consumers. This has the potential to place administrative costs on Fintechs including those incurred through ensuring proper deletion of data and moving to regain authorization. It may also affect potential legal liability for mistakes in carrying out consumer-data retention and deletion. In addition to the compliance costs Fintechs face, they may also face consumer dissatisfaction and loss of business if the need for reauthorization of data sharing leads to temporary service outages.

(iv). Access Transparency

The "access transparency" Principle is the Bureau's response to the widespread concern that not all consumers understand what data they are authorizing access to, the extent to which their data is used, what it is used for, and how long it is stored.[39] Consumer advocates argued that tools that would increase consumer understanding of their data sharing should be made available to them either by data holders or data users, but did not provide specific examples of

[37] The Principles, at 3.
[38] *Id*.
[39] The Stakeholder Insights Report, at 8.

tools they would like to see developed.[40] Data holders have proposed making multi-purpose dashboards available where consumers would be able to monitor all of the third-party sharing agreements they have entered into and modify or revoke those sharing agreements at will.[41] Data holders cite the importance of monitoring who can access their customers' data and what they will use it for as the reason why they should have such information centralized on their proposed platforms.[42] They also argue that such information would allow them to "vet third parties to whom consumers authorize access, suspend or terminate sharing arrangements if third parties breach . . . sharing agreement[s] or fail to meet security standards, comply with their regulatory obligations, and better protect consumers."[43] If banks were to become the prescribed provider of such dashboard they would gain a market advantage as this would be a tool that consumers eventually need and one that likely could be offered by a Fintech company. It would also serve as a barrier to communication between Fintech service providers and consumers when there are data-sharing issues between the two parties.

While the Bureau's published Principle does not appoint financial service providers as the exclusive provider of consumer-data-sharing dashboards, it does state that consumers must be informed of, or be able to determine, who is accessing or using their financial services data.[44] It also states that the security of the third party accessing their information, the specific data being accessed, the use of such data, and the frequency the data is accessed should be "reasonably ascertainable throughout the period [their] data [is] access, used, or stored."[45]

---

[40] *Id.*, at 9.
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] The Principles, at 4 ("[t]he identity and security of each such party, the data they access, their use of such data, and the frequency at which they access the data").
[45] *Id.*

(v). Accuracy

Stakeholders disagreed as to what is the most accurate and effective method for collecting data.[46] Screen-scraping is one option, in which third parties rely on consumers' login credentials to sign into their bank accounts and copy as much data as they choose. Most stakeholders agreed that screen-scraping has a higher likelihood of producing inaccurate or missing information, since the data that it captures consists of snapshots from specific points in time.[47] Another method that is becoming more widely adopted is the use of Application Programming Interfaces ("APIs"), which are intermediary software applications that allow other pieces of software to communicate with one another, allowing for custom arrangements between customers, banks, and third parties that base the types of data shared on what the data will ultimately be used for. Third parties argued against APIs' complete substitution of screen-scraping, stating that this could limit their ability to access data when they need it and to provide consumers with useful products and services.[48]

The Bureau promulgated the "accuracy" Principle in response to these competing concerns, which states that the data consumers receive or authorize to be shared should be accurate and current, and that if inaccuracies arise, consumers should have reasonable means to dispute and resolve them.[49] The Bureau avoided endorsing screen-scraping or APIs through this Principle and instead stated a Principle that no party would disagree with: data should be accurate and timely. However, the majority opinion among stakeholders in their responses to the 2016 RFI was that sharing through APIs is the more accurate, reliable, and timely way of sharing

[46] The Stakeholder Insights Report, at 9.
[47] *Id*.
[48] *Id*.
[49] The Principles, at 4.

consumer financial data.[50] The guidance or rules that the Bureau promulgates will determine if APIs are ultimately used to increase competition and innovation or if competition will be stifled; these issues are discussed later in this paper.

(vi)-(vii). Ability to Dispute and Resolve Unauthorized Access & Efficient and Effective Accountability Mechanisms

Further indication of a shift away from screen-scraping methods, which are still frequently used today despite the consensus that APIs are superior, are both the Bureau's Principle regarding the ability to dispute and resolve unauthorized access and its Principle regarding efficient and effective accountability mechanisms. The Principle regarding the ability to dispute and resolve unauthorized access states that "[p]arties responsible for unauthorized access are held accountable for the consequences of such access."[51] The Principle regarding efficient and effective accountability mechanisms states "[c]ommercial participants are accountable for the risks, harms, and costs they introduce to consumers. . . . [and that they] are likewise incentivized and empowered to prevent, detect, and resolve unauthorized access and data sharing."[52] This potential for liability may forecast a shift away from screen scraping toward APIs, since screen scraping necessarily leads to more unauthorized access. Even if APIs are adopted and exhaustive measures are taken to protect consumer data, unpreventable data breaches may occur due to rogue employees or hackers. Therefore, this Principle has the potential to increase the liability costs of all stakeholders.

b. The 2020 Symposium

Following the 2016 RFI, and the Bureau's publishing of the Stakeholder Insights Report and the Principles, the Bureau held a symposium in 2020 (the "Symposium") where each

[50] The Stakeholder Insights Report, at 9.
[51] The Principles, at 4.
[52] *Id*.

panelist made a pre-Symposium written submission. After the Symposium the Bureau published several documents, including a summary of the Symposium proceedings (the "Symposium Report") and the ANPR.

Participants at the Symposium largely agreed that the best method of transferring consumer financial data is through the use of API technology, and that screen scraping should be discontinued.[53] However, participants disagreed as to (1) the scope of data that consumers should be allowed to share, (2) the method by which consumers should both authorize such data sharing and revoke it, (3) how soon screen scraping should be abandoned, (4) who should bear the costs of retrieving and producing data, and (5) who should be liable in the event consumer financial data is breached. Participants were mostly supportive of the "market-led" development of technical API standards that is free of agency rulemaking,[54] which would allow industry stakeholders to develop their own API solutions—with no formal or compulsory government intervention—and at their own pace. Nonetheless, the differences in opinion among stakeholders on important issues—as well as the need for continued innovation—will likely necessitate at least some regulation, even if that regulation is limited to requiring participation in, and adherence to, certain stakeholder-led cooperative platforms and the standards they set (like the Financial Data Exchange).[55]

[53] The Symposium Summary, at 4.
[54] *Id.*, at 8.
[55] *See* Statement by James Reuter, President and CEO, FirstBank, for the Symposium, at 4 (Feb. 26, 2020) (on file with the Bureau) (discussing cooperation among stakeholders engaging with the Financial Data Exchange ("FDX"), which is a non-profit organization designed to facilitate API innovation and data access and sharing); Letter from Lila Fakhraie, Senior VP, Wells Fargo Bank, N.A., to William Wade-Gery and Gary Stein, Assistant Directors, Consumer Financial Protection Bureau, at 3-4 (Feb. 13, 2020) (on file with the Bureau) (emphasizing the superiority of stakeholder cooperation, including the FDX initiative, over binding regulations).

(i). Scope of Shareable Data

Fintech advocates and data aggregators stated in their pre- Symposium submissions that consumers should have ultimate control over their data and be able to grant broad access to third parties, even exceeding the minimum amount necessary to provide the goods or services they select.[56] Fintech stakeholders also advocated for exhaustive and continuous access to consumer financial data for certain products and services, such as cash-flow underwriting, which uses bank account information (including ongoing balance) to help provide access to credit for otherwise "credit-invisible" individuals.[57] Conversely, banks and consumer advocates argued for a system that would (1) limit data sharing to that data needed to provide the products or services that consumers purchase from Fintechs and (2) limit the amount of time it can be accessed to the amount of time it is being used to provide products or services.[58] However, there are some differences between the positions of banks and consumer advocates. Banks ultimately argue that API standards can be addressed through the FDX initiative while consumer advocates argue for rules that would (1) set boundaries prohibiting banks from withholding data in their APIs for anticompetitive purposes and (2) allow consumers to easily port all of their account information (including account numbers) to switch financial service providers seamlessly.[59] A further difference can be found in the parties' motives in minimizing data sharing; banks are incentivized to minimize data sharing to protect themselves from liability as well as protect their

[56] Symposium Summary, at 3; *see also*, Letter from John Pitts, Head of Policy, Plaid, to Kathy Kraninger, Director, Consumer Financial Protection Bureau, at 3, 7 (Feb. 19, 2020) (on file with the Bureau).
[57] *See* Written Statement of Petal Card, Inc., for the Symposium, at 3 (Feb. 12, 2020) (on file with the Bureau).
[58] *See* Letter from Dan Murphy, Policy Manager, Financial Health Network, to Kathy Kraninger, Director, Consumer Financial Protection Bureau, at 2 (Feb. 12, 2020) (on file with the Bureau); *see also*, Statement by Natalie R. Williams, Managing Director and Associate General Counsel, JPMorgan Chase, for the Symposium, at 7 (Feb. 26, 2020) (on file with the Bureau); *but see* Symposium Summary, at 6 (Fintechs worry that this could allow banks to limit access for certain Fintech firms if they provide a competitive threat.).
[59] *See* Letter from Chi Chi Wu, National Consumer Law Center, to Kathleen Kraninger, Director, Consumer Financial Protection Bureau, at 3 (Feb. 12 ,2020) (on file with the Bureau).

proprietary data, while consumer advocates are compelled by the mission of protecting consumers from fraud or security breaches.

(ii). Method for Authorizing and Revoking Access to Data

All stakeholders generally agreed that consumers should have a dashboard where they can share their data, track what entities have access to each field of their data, and revoke such access. Banks and data aggregators touted their current practice of signing bilateral agreements (between banks and data aggregators) that state the terms of third-party access.[60] Such agreements make it difficult for uniform data-sharing standards and conditions to emerge. Further, Fintechs expressed discontent with the status quo in their submissions, citing the lack of standardized APIs among banks, the lack of reliability of data using current practices, and expensive middlemen (presumably referring to data aggregators as well as banks' software service providers).[61] Banks suggested basing access to consumer data on a process where authorized parties can log on to the relevant API connection temporarily with tokenized access so long as the consumer has shared that data with that party.[62] This method of accessing information would be more in line with what Fintech companies would like to see, as Fintech advocates stated they would like a system that moves away from bilateral agreements and where they could link directly into the banks' APIs to pull consumer data (although there is disagreement as to the scope of data they would have access to once they logged in[63]).[64]

---

[60] *See, e.g.*, Statement by Natalie R. Williams, Managing Director and Associate General Counsel, JPMorgan Chase, for the Symposium, at 3 (Feb. 26, 2020) (on file with the Bureau); Letter from John Pitts, Head of Policy, Plaid, to Kathy Kraninger, Director, Consumer Financial Protection Bureau, at 2 (Feb. 19, 2020) (on file with the Bureau).
[61] Letter from John Pitts, Head of Policy, Plaid, to Kathy Kraninger, Director, Consumer Financial Protection Bureau, at 3 (Feb. 19, 2020) (on file with the Bureau).
[62] *See* Statement by Natali S. Talpas, Senior VP, PNC Bank, for the Symposium, at 9-10 (Feb. 26, 2020) (on file with the Bureau).
[63] *see supra* § II(A)(1)(b)(i).
[64] *See* Written Submission of Steve Boms, Executive Director, Financial Data and Technology Association of North America, for the Symposium, at 4 (Feb. 26, 2020) (on file with the Bureau); Written Statement of Petal Card, Inc., for the Symposium, at 3 (Feb. 12, 2020) (on file with the Bureau).

Consumer advocates praised the use of systems, like dashboards, where consumers can control their data sharing, and they added that the Bureau should consider a system that could allow financial institutions to condition access to third parties on their meeting certain certifications or safeguards, including those required under the Graham Leach Bliley Act.[65] Data aggregators argue that despite the Bureau's Principle stating that access be allowed for only "trusted" third parties, access should be granted to third parties unless that party is shown to provide a material risk and that data sharing should be "complete."[66] As discussed in section II(A)(1)(a)(i), *supra*, and section II(B), *infra*, a more consumer- and Fintech-friendly regulation would be one that requires independent third-party certification so that banks' interests do not taint their vetting processes.

(iii). How Soon Screen Scraping Should be Abandoned

Stakeholders disagreed as to how soon screen scraping should be abandoned, with Fintech advocates on one end of the spectrum arguing that they should not be substituted for APIs in the near future and consumer advocates arguing that they should be moved on from as soon as possible; this disagreement persists.[67] In addition to highlighting that API-powered platforms are prohibitively expensive for small banks to set up, third parties argued that API solutions could allow banks to limit data they share in an anticompetitive manner and that if API

[65] *See* Letter from Dan Murphy, Policy Manager, Financial Health Network, to Kathy Kraninger, Director, Consumer Financial Protection Bureau, at 3 (Feb. 12, 2020) (on file with the Bureau); *See* Letter from Chi Chi Wu, National Consumer Law Center, to Kathleen Kraninger, Director, Consumer Financial Protection Bureau, at 5, Attachment 1, at 20 (Feb. 12 ,2020) (on file with the Bureau).
[66] *See* Letter from John Pitts, Head of Policy, Plaid, to Kathy Kraninger, Director, Consumer Financial Protection Bureau, Appendix 1, at 6 (Feb. 19, 2020) (on file with the Bureau).
[67] *Compare* Written Submission of Steve Boms, Executive Director, Financial Data and Technology Association of North America, for the Symposium, at 3 (Feb. 26, 2020) (on file with the Bureau) (stating "[a]n overnight ban on screen scraping would result in tens of millions of Americans immediately no longer having the ability to take advantage of [financial] tools that help them"), *with* Letter from Chi Chi Wu, National Consumer Law Center, to Kathleen Kraninger, Director, Consumer Financial Protection Bureau, at 3 (Feb. 12 ,2020) (on file with the Bureau); *see also*, Written Statement of Petal Card, Inc., to the Consumer Financial Protection Bureau, in Response to the Advanced Notice of Proposed Rulemaking, at 10 (Feb. 4, 2021) (on file with the Bureau).

solutions are switched too abruptly, the drastic increase in restrictiveness compared to that of screen-scraping techniques would leave many consumers unable to utilize the financial products and services they currently rely on.[68] It is understandable why third parties might want to continue relying one one-time, credential-based access to continuously screen scrape broad data set, however, studies show that consumers are currently unaware of how much of their data is retained and used through such practices and that when they find out they do not feel comfortable with such practices.[69] Therefore, building a business model on this type of access can be prone to a significant loss of consumer data if consumers ever organize to restrict the continuous and unchecked access that comes along with screen scraping.

(iv). Who Should Bear Costs of Retrieving and Producing Data?

One bank participant and one Fintech participant raised the concern that data aggregators are receiving consumer data from financial institutions for free but charging Fintechs for that data, creating additional costs that are ultimately borne by consumers.[70] Fintechs proposed a rule that would allow them to plug into financial service providers' APIs directly as a way to solve this issue (presumably advocating for credential-based access).[71] Banks proposed a set of rules requiring third parties that transfer data to do so for free or at cost.[72]

---

[68] *See* Written Submission of Steve Boms, Executive Director, Financial Data and Technology Association of North America, for the Symposium, at 3 (Feb. 26, 2020) (on file with the Bureau); Statement by James Reuter, President and CEO, FirstBank, for the Symposium, at 5 (Feb. 26, 2020) (on file with the Bureau)

[69] *See* Statement by Natali S. Talpas, Senior VP, PNC Bank, for the Symposium, at 4-6 (Feb. 26, 2020) (on file with the Bureau).

[70] *See* Written Submission of Becky Heironimus, Managing VP, Capital One Financial Corp., for the Symposium, Appendix, at 19 (Feb. 18, 2020) (on file with the Bureau) (discussing "long chain of value additions"); *see also*, Written Statement of Petal Card, Inc., for the Symposium, at 3 (Feb. 12, 2020) (on file with the Bureau) (discussing "expensive middlemen").

[71] Written Statement of Petal Card, Inc., for the Symposium, at 3 (Feb. 12, 2020) (on file with the Bureau).

[72] Written Submission of Becky Heironimus, Managing VP, Capital One Financial Corp., for the Symposium, Appendix, at 19 (Feb. 18, 2020) (on file with the Bureau).

(v). Liability

Third parties did not raise the issue of who would be liable in the event of unauthorized transactions resulting from a data breach. However, banks proposed that data aggregators should be liable for any unauthorized transactions, and most banks are already attempting to accomplish such liability-shifting through bilateral agreements.[73] Consumer advocates also agreed that third parties may be liable for unauthorized transactions arising from data breaches, however, they stated that consumers should first be able to hold their banks responsible since they are in the best position to determine how the breach occurred.[74] Additionally, consumer advocates stated that third parties should have liability insurance so that if they are at fault, financial institutions can seek to be made whole and consumers wont be left without any recovery.[75]

c. ANPR and Stakeholder Responses

Most recently, the Bureau issued the ANPR to seek input from stakeholders that would help the Bureau develop regulations to implement Section 1033.

Responses to the Bureau's ANPR still see separate classes of stakeholders digging their heals in to certain of their self-serving positions, however, there seems to be a conscious effort to find common ground on certain issues in order to continue productive business operations while satisfying each party's requirements under Section 1033. For example, all parties seem to agree that data aggregators should be supervised by the Bureau going forward. Oversight could include meeting security standards, ensuring data is not stored beyond what consumers agreed to, limits on how consumer data is used, and confirming data aggregators have insurance. This is an

[73] *See* Letter from Lila Fakhraie, Senior VP, Wells Fargo Bank, N.A., to William Wade-Gery and Gary Stein, Assistant Directors, Consumer Financial Protection Bureau, at 3-4 (Feb. 13, 2020) (on file with the Bureau).
[74] Letter from Chi Chi Wu, National Consumer Law Center, to Kathleen Kraninger, Director, Consumer Financial Protection Bureau, at 5, Attachment 1, at 10-11 (Feb. 12 ,2020) (on file with the Bureau).
[75] Letter from Dan Murphy, Policy Manager, Financial Health Network, to Kathy Kraninger, Director, Consumer Financial Protection Bureau, at 5 (Feb. 12, 2020) (on file with the Bureau).

opportunity for banks to reduce risk of liability and shift some of the cost of doing business away from themselves and on to other stakeholders in the ecosystem, no doubt for competitive reasons. Large, established data aggregators also say they should be subject to Bureau oversight, and that if the Bureau cannot figure out a way to supervise all data aggregators in the near future, it should start by supervising the preeminent data aggregators.[76] However, if Bureau supervision becomes a prerequisite to directly tapping into financial institutions' APIs, Fintechs could be blocked from doing so. Consumer advocates argue that any firm tapping into financial institutions' APIs should be supervised by the Bureau and governed by the FTC Safeguards Rule under the Gramm-Leach Bliley Act.[77] Fintech stakeholders have not commented on whether the reach of the GLBA should be extended to third parties. However, as explained in section II(B), *infra*, the GLBA likely should be extended to third parties offering products or services that are financial in nature. This compliance would increase the cost of doing business for Fintechs, but it could also create a consumer base that has more trust in legitimate Fintech businesses and, therefore, is more likely to share data with such businesses.

Banks advocate for "use cases," which, through stakeholder-neutral cooperatives, define and set minimized data sets needed for specific uses.[78] Banks would like to see the Bureau regulate by supporting the development of standards through stakeholder cooperatives like the FDX and Akoya (which is a platform owned by The Clearing House and banks that operates as a centralized location for APIs and boilerplate data-sharing agreements), and data aggregators

[76] *See* Written Statement of Meredith Fuchs, General Counsel, Plaid, to the Consumer Financial Protection Bureau, in Response to the Advanced Notice of Proposed Rulemaking, at 2, 10 (Feb. 4, 2021) (on file with the Bureau).
[77] Written Statement of Chi Chi Wu, National Consumer Law Center Response, to the Consumer Financial Protection Bureau, in Response to the Advanced Notice of Proposed Rulemaking, at 2 (Feb. 4, 2021) (on file with the Bureau).
[78] *See* Written Statement of Ben Soccorsy, Senior VP, Wells Fargo & Co., to the Consumer Financial Protection Bureau, in Response to the Advanced Notice of Proposed Rulemaking, at 3, 5 (Feb. 4, 2021) (on file with the Bureau).

generally support this position; banks cite the fact that prescriptive rules that lock the ecosystem into using a certain type of technology could limit innovation in the future.[79] Fintechs and their advocates stand against use cases, as they do not want data limited, and this has contributed to their standing against Bureau endorsement of certain market-led initiatives (like FDX), since it could indirectly give big banks disproportionate influence.[80]

Banks argue data aggregators should need to request annual or regular authentication by customers or that there should be automatic expiration of permission to access their financial data once certain markers are reached.[81] Banks also request to be able to share costs with other stakeholders because they bear almost all the cost of building the infrastructure to be able to share consumer data.[82] This argument is weak, as third parties are investing in their own technological capabilities to be able to serve consumers, and any capital that banks have to invest in revamping their data-sharing software is warranted since they too have to contribute to a robust data-sharing ecosystem, or risk losing their own clients.

2. The Approach Other Jurisdictions Have Taken and How it Has Affected Data Portability

International regulatory regimes regarding consumer-financial-data portability generally fall into three categories: (1) mandated (i.e., regulatory driven), where the roll out of consumer-permissioned data sharing is prescribed in detail (including the stages in which specific classes of

[79] *Id.*; *see also*, Written Statement of Naeha Prakash, Senior VP and Associate General Counsel, Bank Policy Institute, to the Consumer Financial Protection Bureau, in Response to Advanced Notice of Proposed Rulemaking, at 4 (Feb. 4, 2021) (on file with the Bureau).
[80] Written Statement of Meredith Fuchs, General Counsel, Plaid, to the Consumer Financial Protection Bureau, in Response to the Advanced Notice of Proposed Rulemaking, at 19 (Feb. 4, 2021) (on file with the Bureau).
[81] Written Statement of Rob Morgan, Senior VP of Innovation and Strategy, American Bankers Association, to the Consumer Financial Protection Bureau, in Response to the Advanced Notice of Proposed Rulemaking, at 10 Feb. 4, 2021) (on file with the Bureau).
[82] Written Statement of Becky Heironimus, Managing VP, Capital One Financial Corp., to the Consumer Financial Protection Bureau, in Response to the Advanced Notice of Proposed Rulemaking, at 12 (Feb. 2, 2021) (on file with the Bureau).

data must be shared, with what parties that data should be shared, and certifications and standards third parties must meet); (2) market-led, where the government takes a hands-off approach and allows the various stakeholders in the consumer-finance industry to develop standards of consumer-permissioned data sharing[83]; and (3) guided, which lies between the regulatory- and market-driven approaches and sees government regulators providing non-binding guidelines aimed at encouraging stakeholders to collaborate in their technological development, resource-sharing, and innovative product and service offerings for consumers.[84]

a. Mandated/Regulatory-Driven

Jurisdictions that have embraced regulatory-driven approaches include the UK, the EU, and Australia. These jurisdictions have had quicker rollout of consumer-financial-data sharing, but in some instances have seen banks comply with the minimum API standards required by regulation due to competition concerns. For example, while the UK saw early adoption of open banking by its largest banks, that was only because the UK Competition and Markets Authority ("CMA") ordered those banks (the "CMA9") to create and pay for an entity aimed at establishing open banking.[85] This government-mandated approach initially served to hinder innovation because large banks enjoyed disproportionate influence compared to other stakeholders, and the CMA9 used that influence to delay robust API development that would otherwise have spurred data sharing and competition from Fintechs. This prompted a letter from

[83] *Open Banking Ecosystem and the Need for a New Connectivity Model*, KAPRONASIA, September 2021, at 6, available at https://www.kapronasia.com/research/reports/open-banking-new-connectivity-model-kapronasia-equinix.html. (last visited Apr. 30, 2022).
[84] *Id.*, at 6-7.
[85] *Corporate Report: Update on Open Banking*, COMPETITION & MARKETS AUTHORITY, Nov. 5, 2021, available at https://www.gov.uk/government/publications/update-governance-of-open-banking/update-on-open-banking. (last visited Apr. 30, 2022).

Tony Craddock of the Emerging Payments Association calling for the Implementation Entity to take action to uphold the spirit of open-banking laws in the UK.[86]

Since then, the open-banking ecosystems in the UK and EU have seen genuine efforts by banks to create workable API solutions to foster innovation and to remain competitive, especially after Covid-19 made it apparent that Fintech solutions are the way of the future.[87] The EU has served as an example of how a mandated approach can foster innovation and competition, by setting benchmarks that must be met by the industry and providing timelines. One way this competition manifested itself is in the wide variety of data aggregators that the EU enjoys. While the data-aggregation market in the U.S. is largely controlled by Plaid, the EU ecosystem has had multiple data aggregators to choose from, which can ultimately contribute to more competitive pricing for data-aggregation services that Fintechs rely on, as well as constant innovation.[88]

Australia provides an example of how a mandated approach can lead to a transformative change in data sharing. Australia opted to make its Treasury Department the lead agency of its Consumer Data Right policy ("CDR") and to ultimately extend consumers' rights to their data beyond the banking industry.[89] This is a regulatory-driven approach that seeks to enable consumer-data portability in its truest sense. This will allow Australian citizens to share all the

---

[86] *Payments community calls on Open Banking to do more to enable access for Fintechs*, THE PAYMENTS ASSOCIATION, August 13, 2018, available at https://thepaymentsassociation.org/article/payments-community-calls-on-open-banking-to-do-more-to-enable-access-for-fintechs/. (last visited Apr. 30, 2022).

[87] *The UK Open Banking ecosystem and the tension of innovation vs compliance*, OPEN BANKING EXCELLENCE, July 2, 2021, available at https://www.openbankingexcellence.org/blog/the-uk-open-banking-ecosystem-and-the-tension-of-innovation-vs-compliance/. (last visited Apr. 30, 2022).

[88] Pauline Brunel, *US vs. Europe: two visions of Open Banking and their impact on the market structure*, BLACKFIN TECH, March 6, 2020, available at https://medium.com/blackfintech/us-vs-europe-two-visions-of-open-banking-and-their-impact-on-the-market-structure-e0a18ac44b90. (last visited Apr. 30, 2022).

[89] *What is the Consumer Data Right?*, OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, available at https://www.oaic.gov.au/consumer-data-right/what-is-the-consumer-data-right#:~:text=The%20Consumer%20Data%20Right%20was%20introduced%20in%20the,and%20the%20Australian%20Competition%20and%20Consumer%20Commission%20%28ACCC%29. (last visited Apr. 30, 2022).

data they generate as consumers as they please (i.e., across industries), allowing for a better understanding of their finances, the development of more innovative products, and streamlining payment and financing options between banks and non-financial service providers.

b. Market-Led

Market-led approaches, like that in the U.S., seemingly allow for more competition among banks since they are able to develop data sharing and APIs as they individually see fit. However, the U.S. has served as an example of how free competition has been at least partially illusory. This is because, by allowing stakeholders to develop their own data-sharing schemes without regulation, incumbent financial institutions as well as large, influential data aggregators (like Plaid) are able to exercise disproportionate influence and strike their own bilateral agreements. This leaves consumer interests out of the equation, and it also leaves out smaller banks that do not have the resources to revamp their legacy software programs to support robust, API-driven data sharing. The latter issue is particularly troublesome in the U.S., as community banks make up 91% of the FDIC-insured financial institutions that consumers can choose to bank with.[90] Leaving these banks lagging behind would not only counter their customers' ability to access the most innovative financial technology, but cutting out this segment of the market would also limit the incentive for Fintechs to innovate. There has recently been one instance of private-equity investment in a community bank to modernize its technology and software so that Fintechs can innovate on its platform, but this was to address Fintech innovation generally; it does not help the many other community banks that do not have such funding or ambitious leadership.[91] In addition to the market consolidation that could take place under a market-driven

[90] *FDIC Quarterly*, FEDERAL DEPOSIT INSURANCE CORP., March 30, 2022, available at https://www.fdic.gov/analysis/quarterly-banking-profile/fdic-quarterly/index.html. (last visited Apr. 30, 2022).
[91] Kyle Wiggers, *Plaid co-founder's next venture is a bank to power fintech apps*, TECHCRUNCH, April 21, 2022, available at https://techcrunch.com/2022/04/21/plaid-cofounders-next-venture-is-a-bank-to-power-fintech-apps/.

approach, the lack of uniformity that it creates has the potential to cause friction if different stakeholders cannot agree on best practices, and it could also lead to disparate levels of cooperation among stakeholders.

c. Guided

Guided jurisdictions, such as Singapore, have seen regulatory agencies lead initiatives aimed at encouraging API adoption and innovation.[92] Singapore's initiatives have included publishing all open APIs in a centralized location, launching the API Exchange, which is an open-architecture platform aimed at allowing collaboration and innovation of new APIs, and SGFinDex, which is managed through the national identity platform, SingPass, and allows consumers to consent to data sharing in one, centralized location and then integrate that data into Fintech apps.[93] These initiatives are similar to the stakeholder-led initiatives in the U.S., FDX and Akoya, in that they develop and centralize best practices. However, they differ in that the government is leading the cooperative efforts in Singapore and therefore data-sharing platforms are much more robust and are genuinely based on the dual goals of consumer data portability and innovation, whereas the stakeholder-led initiatives in the U.S. center around producing standards for APIs, essentially performing the rulemaking of the Bureau, as opposed to innovating.

B. Potential Bureau Regulations and Pros, Cons, and Tradeoffs from the Perspective of Fintechs

Each different type of regulatory approach has its benefits and drawbacks. This paper argues for a hybrid approach that stays consistent with the Bureau's approach thus far in allowing market-led innovation and setting of certain best-practices, but that also puts concrete

(last visited Apr. 30, 2022) (discussing William and Annie Hockey's initiative in purchasing local bank to revamp its technological infrastructure and allow for Fintech partners to innovate on its platform).

[92] *Open Banking Ecosystem and the Need for a New Connectivity Model*, KAPRONASIA, September 2021, at 7, available at https://www.kapronasia.com/research/reports/open-banking-new-connectivity-model-kapronasia-equinix.html. (last visited Apr. 30, 2022).

[93] *Id.*

rules in place that will provide a foundation that fosters maximum innovation and stakeholder participation. This hybrid model is recommended, as opposed to a guided regulatory landscape like that in Singapore, because stakeholders in the U.S. have already proven to be less collaborative than stakeholders in Singapore, who are, *inter alia*, engaging in open-source API development.

Stakeholders have made certain concessions since the Bureau's 2016 RFI to find common ground and stay competitive with the financial products and services they offer. However, some unresolved disagreements remain, and the Bureau's pending response will dictate how innovative and competitive the U.S. financial-services ecosystem will be going forward. Disagreements that persist include the scope of data to be shared, with some Fintech's wanting exhaustive and constant access and other stakeholders endorsing minimizing sharing to data that is relevant; method of access, with most stakeholders opting for APIs, but with some Fintechs—and their advocates—arguing that screen scraping should not be abandoned too soon; whether third parties must meet certification standards to be able to access data or otherwise be deemed a "trusted" third party; and which group of stakeholders should bear the costs of retrieving and sharing data.

The Bureau should be cautious not to promulgate rules that would set prescribed limits to data sharing. Not only is the Bureau ill equipped to determine the unique data-set needs for each type of product or service, but it is also unable to forecast all the potential data-set needs for products or services that are yet to be developed. Instead, the Bureau should endorse the use of stakeholder cooperatives, like FDX and comparable platforms, that would serve as a place for knowledge-sharing, development of best practices, and a place where "use cases" can be discussed and decided upon. Further, the Bureau could launch its own platform so that it has

more control over the content available and so that users know that the information and standards are approved by a neutral party. A platform run by the Bureau could include some of the features made widely available in other jurisdictions. Singapore, for example, has a register of all public APIs, as well as the API Exchange, which allows open-source collaboration and innovation. A platform launched by the Bureau could include these features as well as other information, like "report cards" for financial institutions that assess the technology banks have in place to enable data sharing, their data-sharing policies, and their current API offerings. Such information would serve to align the incentives of financial institutions and Fintechs so that all parties have a sense of urgency in innovating and coming up with data-sharing solutions for different products and services. The innovation in data-sharing and API solutions that would result from such an open platform would obviate the need for screen scraping and make "use cases" more palatable, since input from a diverse range of stakeholders and transparency would likely lead to solutions that provide robust data sharing tailored to unique products and services. Creating an open-architecture platform with APIs and methods for consumers to authorize access to Fintechs directly could serve as the first step to eliminating "expensive middlemen."

While the Act does state that the Bureau may not promulgate rules that favor any type of technology over the other,[94] it is unclear how that implicates the Bureau's authority in regulating screen scraping. Screen scraping is not a novel technology; it merely relies on credential-based access to copy all the data from the account the user is logging in to. Therefore, the Bureau should issue rules that would finally begin the phasing out of screen-scraping, and it would likely be within its authority if it did so. Not only would consumers' data be more secure, but the inability of third parties to gain access to unlimited data would make it necessary for all

[94] Pub. L. No. 111-203 §§ 1033(e)(1)-(3), 124 Stat. 2008 (codified at 12 U.S.C. §§ 5533(e)(1)-(3) (2010)).

stakeholders in the ecosystem to commit to developing the most innovative and efficient API solutions and to take a cooperative approach. The Bureau could begin to phase out screen scraping by identifying services that still rely heavily on screen scraping and determining if their utility warrants a temporary waiver to enable Fintechs providing those services. For example, this can be done with Fintechs that use screen scraping to provide credit or loans to consumers that would not be able to take on debt if it were not for underwriters first having access to their cash-flow statements. This waiver period would allow stakeholders to come up with API-driven or alternative solutions to share the data necessary to power these products and services. The Bureau could then set a date at which screen scraping must be eliminated (except for those instances in which a waiver has been granted), and then set a date at which waivers expire. This type of regulation would not promote one type of technology over any other and would create an ecosystem built on sustainable data sharing, as it would be a system that builds consumer trust that their data is secure while simultaneously fostering innovation. As discussed above, having broad stakeholder cooperation on API development could serve to de-consolidate the current data aggregation industry and lower the costs of data for Fintechs.

The Bureau should use its authority to require independent third-party certification. As mentioned above, bank stakeholders have considered vetting third parties, but they should neither have to take on the cost of performing such due diligence nor should they be given the discretion to act in a potentially anti-competitive manner by being the ultimate decision maker of who is a trusted third party. Instead, the Bureau should publish a set of standards that data aggregators and Fintechs must meet to be certified third parties. In fact, the Bureau has recently taken the first step in being able to identify, track, and label third parties,[95] so the final step of

[95] Ayana Brown, Jeffrey P. Ehrlich, Brandi G. Howard, Kristin Lee, Heryka R. Knoespel, and Susan C. Rodriguez, *CFPB's New Interest in Examining Fintechs is Likely to Mean More Naming and Shaming by the Agency*, SUBJECT

promulgating standards they must meet to be certified would be relatively simple and would give third parties direction on how to become legitimate and certified to tap into consumers' banking data. One requirement that should be included for third parties to become certified is that they have third-party insurance. While this would add to the cost of doing business for Fintechs it is only right that customers are able to be made whole in the event of a data breach. Further, having third-party insurance will ensure banks they will not be responsible for third-party negligence, which will likely make banks more willing to share data. Another certification requirement that the Bureau should set through binding rulemaking is that third parties be subject to the GLBA requirements for consumer-data privacy. The Act states that the Bureau should work with other agencies to ensure uniformity as it relates to covered persons,[96] and the FTC has promulgated rules that state, for GLBA purposes, a covered person is one that engages in activity that is financial in nature or incidental to financial activity[97]. Here, Fintechs are, almost by definition, providing products and services that are at least incidental to financial activity and can even be deemed to be financial in nature. This is a necessary step even though it would increase compliance costs that could be a major hurdle for startup Fintechs. It would also increase transparency between Fintechs and consumers and, therefore, increase the frequency with which consumers engage with the Fintech market, increasing network effects.

III. CONCLUSION

While the recommendations this paper proffers would increase the cost of doing business in certain ways for Fintechs, they also eliminate certain other costs of doing business, as well as make the costs more predictable and less sensitive to competitor influence (i.e., from banks and

TO INQUIRY BY MCGUIREWOODS, April 28, 2022, available at https://www.subjecttoinquiry.com/2022/04/cfpbs-new-interest-examining-fintechs-likely-mean-more-naming-shaming-agency/. (last visited Apr. 30, 2022).
[96] Pub. L. No. 111-203 § 1033(e)(1), 124 Stat. 2008 (codified at 12 U.S.C. § 5533(e)(1) (2010)).
[97] *See* 16 C.F.R. § 313.3(k)(1).

large data-aggregators). Compliance costs are generally finite and forecastable, while insurance costs are merely a way to finance costs that likely will arise at some point in the future. In addition to the cost-shifting nature of these proposals, they are also aimed at reducing friction in innovation and data-sharing by aligning interests of separate stakeholders that are inherently in competition with one another. By giving stakeholders what they want—by adopting a market-led approach—and including novel features like a government-sponsored platform, report-card-like grading, a definitive time limit for abandoning screen scraping, third-party certification, and consumer-controlled authorization, stakeholder interests will begin to align and banks' efforts to modernize their capabilities will begin to be seen less as acts of benevolence and more as what they really are, necessary efforts to remain competitive. Finally, these recommendations aim to increase network effects by using open-architecture platforms as a way to include Fintech startups and community banks, which make up the majority of the financial institutions in the U.S.; this will broaden consumers' access to Fintechs and further incentivize Fintech innovation.