



February 4, 2021

Ms. Monica Jackson
Office of the Executive Secretary
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

Re: Advance Notice of Proposed Rulemaking Regarding Consumer Access to
Financial Records [Docket No.: CFPB-2020-0034]

Dear Ms. Jackson:

Financial Innovation Now (FIN)¹ appreciates the opportunity to comment on the Consumer Financial Protection Bureau's (CFPB or "Bureau") advance notice of proposed rulemaking (ANPR) regarding consumer access to financial records under section 1033 of the Dodd-Frank Act ("Section 1033").² Consumer-authorized data access and use of such data by a range of providers of consumer financial products and services (collectively, "Industry") can increase the accessibility of and breadth of innovative consumer financial services products and services available to customers.

FIN supports the CFPB's efforts, through the ANPR, to develop regulations that would "clarify the Bureau's compliance expectations and help to establish market practices to ensure that consumers have access to consumer financial data."³ FIN also supports the spirit of Section 1033 of the Dodd-Frank Act, that a bank or other consumer financial services provider, or "covered person," should "make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data...in an electronic form usable by consumers."⁴ FIN believes that regulation of consumer-authorized access is now necessary given the division among Industry participants. FIN further believes that establishing such regulations will address existing barriers preventing consumers from accessing their financial information and providing others access to this information. Addressing such barriers will facilitate consumer

¹ FIN is an alliance of technology leaders working to modernize the way consumers and businesses manage money and conduct commerce. We believe that technological transformation will make financial services more accessible, safer, and more affordable for everyone, and we promote policies that enable these innovations. Our member companies include Amazon, Apple, Google, Intuit, PayPal, Square, and Stripe. For more information regarding FIN's policy priorities and principles, please visit www.financialinnovationnow.org.

² 85 Fed. Reg. 71,003 (Nov. 6, 2020).

³ Id. at 71,009.

⁴ 12 U.S.C. § 5533.

access to financial products or services by empowering these consumers with choice and agency.

As discussed further below, our views on consumer-authorized data and access and use of such data are based on FIN's observations that:

- Consumers are using new applications and technologies that utilize consumer financial account data to empower themselves to make better-informed financial decisions; and
- Consumer-authorized access to consumer financial account data benefits both consumers and the broader financial services industry by promoting competition.

Based on these observations, FIN believes that consumers' interests will be promoted most effectively if:

- Consumers are empowered to permit access to consumer financial account data securely and easily, using appropriate secure application or technology, without charges or restrictions that unreasonably favor any one application or technology over another;
- The obligations and responsibilities of data aggregators, data holders, and data users are clearly delineated; and
- Industry-developed standards for consumer-authorized data access, which shall not mandate a specific type of technology, are required by regulation.

Consumers are using new applications and technologies that utilize consumer financial account data to empower themselves to make better-informed financial decisions.

The economic benefits of wide access to data to facilitate informed market choices are axiomatic. Simply put, more information enables better choices. One study estimates the potential value of wide access to data (or "open data") to the U.S. economy across seven sectors, including consumer finance, to be approximately \$1.1 trillion.⁵

This benefit ultimately accrues to consumers. Consumers can make better-informed decisions and benefit from lower costs for products and services. Open data also will promote efficient production and lead to more jobs and higher wages. All of these benefits collectively lead to higher standards of living. Today, the benefits of open data are manifesting themselves in many different aspects of consumers' lives, including with respect to consumer transactions, social networking, professional development, health care, and education. Transparency enabled by open data has, for example, allowed consumers to easily compare pricing for travel, health care, and other consumer products and services. Open data has also changed the way consumers travel, for example, by enabling improved navigation on mobile devices and public transportation reliability. Consumers are empowered to make use of this data increasingly through apps on mobile devices and in app

⁵ See McKinsey & Company, OPEN DATA: UNLOCKING INNOVATION AND PERFORMANCE WITH LIQUID INFORMATION 6 (2013), <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information>.

marketplaces, and these delivery mechanisms have dramatically lowered barriers to entry for thousands of entrepreneurs to innovate and create new services and new jobs.⁶

The area of consumer financial services, based in part on the extensive amount of data generated, provides some of the greatest opportunities for consumers and their households to benefit from open data. Currently, there are a range of tools for consumers to better manage their finances, including personal financial management and budgeting apps that enable consumers to view and manage consumer financial account information on a consolidated basis across accounts and financial institutions. These tools help consumers analyze account activity, make better-informed financial decisions, and become aware of, and ultimately avoid, unnecessary fees. Consumers also are using savings tools, informed by permissioned access to consumer financial account data, to help meet their savings goals, as well as apps that can educate and advise them on the range of financial products and services that may be available to them, including recommendations for credit and other financial products or services.

Consumer-authorized data access benefits consumers and the broader financial services industry.

Enabling consumer-authorized data access has the potential to make these and other tools more widely available and reliable. For example, open data can enable efficient and more reliable tools that provide verification of account ownership or loan application information. Account verification tools enable consumers to access other financial products and services, including peer-to-peer payment services, in real time rather than by delayed verification options, such as micro-transfers.

Importantly, consumer-authorized data access can be targeted to narrow data sets and designated for specific entities. Such tailoring enhances consumer control. Enabling consumers to permission access to financial account data for designated creditors, for example, can provide the designated creditors with a more complete picture of a consumer to assess creditworthiness. Among other things, consumer permissioned data can be used to promote financial inclusion, and serve as a basis for providing financial products and services to traditionally unbanked or underbanked populations.⁷ FIN believes that consumers should be permitted to authorize access to all data that a consumer's financial institution makes available directly to the consumer via paper statements or on the financial institution's website, provided that financial institutions may be permitted to block authorizations in clearly defined circumstances, such as in the event of a believed security risk, upon notice to the consumer.

Similarly, consumers should be permitted to authorize access to all payment data. To promote a more holistic understanding for all parties, consumers should also be able to disclose account payment information for funds moving within a single financial institution, rather than transferring of funds among different financial institutions. Permitting access to

⁶ See The App Association, State of the App Economy, (6th Ed. 2018), <https://actonline.org/2018/04/16/state-of-the-app-economy-report-highlights-american-leadership-in-the-950-billion-app-economy/>

⁷ Stefan Staschen and Ariadne Plaitakis, Open Banking: 7 Ways Data-Sharing Can Advance Financial Inclusion, May 7, 2020. ("Our early research indicates that when firms can access customers' financial data held by third parties, these firms create savings, credit and financial management products that are better suited to poor people than those traditional banks have to offer. These products are especially important today in a COVID-19 world.")

the foregoing data would empower consumers to provide creditors with a more complete understanding of the consumer's financial position and ability to utilize particular financial products or services.

Fundamentally, we believe that consumer-authorized data access is a core component of promoting the Bureau's statutory purpose to "ensur[e] that all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive."⁸ We also believe that it would help the Bureau achieve its objective of markets "operat[ing] transparently and efficiently to facilitate access and innovation."⁹

Consumers should be empowered to permission access to consumer financial account data securely and easily, using appropriate secure application or technology, without charges or restrictions that unreasonably favor any one application or technology over another.

In spite of strong consumer interest and the potential for significant consumer benefit, consumer-authorized access to consumer financial account data has, at times, been restricted. Some account-holding financial institutions have blocked access to permissioned entities (e.g., personal finance applications or aggregators) that the consumer directs to access consumer financial account data. In addition, sometimes account-holding financial institutions change data formats and URLs or online forms in ways that disrupt automated access to consumer financial account data by these permissioned entities acting on behalf of consumers.

To promote the greatest degree of flexibility for consumers and generate opportunities for industry to offer consumers the financial services and products they truly need, some in the industry are working together in constructive arrangements to facilitate greater consumer-authorized data access. For example, as the CFPB notes, some data aggregators and data holders have shifted toward the use of tokenized access through application programming interfaces (APIs). In such instances, mutual customers can provide consent for token-based access to financial account data. As with most third-party application providers, the consumer that permissions access to his or her financial data should also be empowered to revoke permission and to delete his or her account with the permissioned entity, at any point. We believe that open, standardized APIs can provide a secure and scalable method for consumers authorizing data access in a safe and secure manner.

While open, standard APIs should be the preferred method, until APIs become widespread and companies accessing those APIs can reach mutually acceptable terms conditioning access to those APIs, alternative methods for facilitating consumer-authorized data access, such as screen scraping, should be preserved. To mitigate the fraud, security, and compliance risks inherent to screen scraping, its deployment may be limited to cases where other methods of data access are not available. Moreover, industry participants engaging in screen scraping should provide consumers with information on how their data is being used, by whom, and for how long.

⁸ 12 U.S.C. § 5511(a).

⁹ *Id.* § 5511(b)(5).

Despite such arrangements, potential gaps for those consumers that are not customers of large financial institutions, as well as for third-party application providers that have built their applications with the consumer's broader financial picture in mind, continue to exist. FIN recommends that industry standards be developed and applied. Examples of such industry standards and best practices are those envisioned by the Center for Financial Services Innovation (CFSI)¹⁰ or those contemplated, albeit too slowly, within the Financial Services Information Sharing and Analysis Center (FS-ISAC). Industry standards, formal or informal, potentially based on the discussions at CFSI or FS-ISAC, would lead to a data-sharing ecosystem that is open to all, not only those who bank with the financial institutions that have entered into bilateral agreements. Fundamentally, these standards must include a focus on security and flexibility. Importantly, the CFPB should mandate the adoption of these Industry-developed standards, both because of Industry experience in preparing these standards and because such standards would encompass standards for a variety of technologies, rather than choosing a single technology over all other alternatives.

Principles for Consumer-Authorized Data Access

Classification. In any regulations, the CFPB should carefully distinguish data aggregators from financial institutions and third-party applications. Significantly, the activities engaged in by these classes of entities are not identical, and additional consents and security procedures may be required for the activities of data aggregators. For example, FIN members do not sell consumer data, whereas some data aggregators may do so. Data aggregators that sell consumer data would be required to obtain additional consumer consent for sharing consumer data for each third party to which the data aggregator provides the consumer data. In order to better protect and educate consumers, the CFPB may also consider imposing a time period limit on data aggregators' consumer-authorized data access where the consumer is not actively using the particular product or service, thereby making such consents time-limited and subject to periodic renewal during periods of product or service inactivity. Such distinctions will have a tangible impact on the obligations of, and affect the compliance procedures instituted by, entities operating as data aggregators, data holders, or data users.

Security. Realizing the benefits of consumer-authorized data access is dependent on robust security, all participants in the data access ecosystem agree that security is a shared goal and a shared responsibility. There are a growing number of approaches designed to share securely consumer-authorized data. However, FIN does not believe that new data security requirements need to be imposed by the CFPB in connection with Section 1033. The pre-existing regimes are sufficient for ensuring the protection of consumer-authorized data. Moreover, Industry participants have collaborated for years to progress on developing industry-wide standards and protocols for consumer data-sharing. As a result, the Industry has already taken significant steps toward developing a robust security framework; a new government-developed security framework would likely be either duplicative of the pre-existing Industry-developed standards or provide less security than the Industry-developed standards. Moreover, Industry is better positioned to rapidly address needed changes in the data security landscape to protect consumers.

¹⁰ See Jennifer Tescher, *One-off data-sharing deals aren't enough*, Am. Banker, Jan. 27, 2017, <https://www.americanbanker.com/opinion/one-off-data-sharing-deals-arent-enough>.

Allocation of Liability. Currently, data sources have significant discretion to prevent data aggregators and downstream data users from accessing information. As a condition of accessing APIs, data sources may seek to transfer substantially all liability to data aggregators, including for downstream users' actions that are outside the control of data aggregators. This liability framework is a substantial disincentive for aggregators to move to accessing data through secure APIs, which should be the preferred solution for all parties. Although an aggregator should be responsible for its actions, subject to appropriate risk-based liability caps, the liability framework proposed by some data sources cuts against the spirit of Section 1033, which seeks to make it easier for consumers to access and permission their data, without data sources playing an additional gatekeeping function. Third and fourth-party risk management obligations on data sources should not result in aggregators and downstream users being put in the inequitable position of assuming substantially all of the data source's risk in providing consumer-permissioned data through APIs. A combination of industry standards and consumer consent should dictate which entities can collect and use consumer-permissioned data, rather than the financial institution that serves as a repository of such information. Additionally, there should be some consistency in how liability is quantified and imposed on data aggregators, data users and data sources.

Privacy. Privacy is a fundamental human right which Industry participants are obligated to respect and safeguard. In the context of consumer-authorized data access, abiding by a robust security framework is essential to guaranteeing consumer financial privacy, and certain principles may be applied to further its protection. Such principles include, but are not limited to, utilizing encryption and tokenization to reduce sensitive data transmission, and providing consumers with the key information they need to make informed choices, including through granular, intelligible, and easily accessible notice. By granting customers control over their data and the information required to exercise that control, Industry participants help to satisfy their affirmative and continuing privacy obligations. FIN supports Congressional efforts to pass comprehensive national privacy legislation and believes Congress should raise the bar for all stakeholders.¹¹

Existing regulatory frameworks, namely the Gramm-Leach-Bliley Act ("GLBA") and the Fair Credit Reporting Act, as well as state laws including the California Financial Information Privacy Act, limit how financial institutions and service providers use and share consumer data, and for which purposes. This rulemaking should not include additional restrictions or limitations, as there are already multiple, disparate legal frameworks in place to regulate such data access and use. Despite FIN's strong desire for a comprehensive federal privacy law that strengthens consumer protections beyond those afforded by, for example, GLBA, Section 1033 does not grant the Bureau with broad authority to draft federal privacy or data protection rules.

Standards for consumer-authorized data access should be industry-led and should not box in current technology.

Individual partnerships enable certain consumers to benefit from consumer-authorized data access, but these partnerships cannot scale to all account-holding

¹¹ See FIN "To Senators Crapo and Brown: Raise The Bar for Everyone on Data Privacy," <https://financialinnovationnow.org/2019/03/15/fin-to-senators-crapo-and-brown-raise-the-bar-for-everyone-on-data-privacy/>

institutions or third-party application providers. Industry standards would empower a broad class of consumers to permit access to consumer financial account data, and would promote innovation. For example, Industry-developed standards would enable many small financial institutions to facilitate permissioned access to consumer financial account data, minimizing the need to negotiate bilateral agreements with every third-party application provider.

We believe that the CFPB should mandate through regulation the adoption of Industry-developed standards. The need for standards to evolve as technology evolves makes a regulatory approach to setting standards for permissioned access to consumer financial account data insufficiently flexible. This is not a role for a government regulator; standards development and maintenance must be Industry-led. Moreover, due to the variety of stakeholders, Industry-developed standards are likely to be better equipped to accommodate a variety of technologies in the standards with the nuance and precision that a government regulator likely would not have.

* * *

FIN applauds the CFPB's efforts to develop regulations implementing Section 1033 to ensure that consumers can efficiently and safely engage in the broad and complex data access ecosystem. This is a dynamic space for innovation and promises to deliver significant benefits to consumers by enabling them to make smarter financial decisions and gain access to a broader range of consumer financial products and services. These benefits will only be fully realized if consumers are empowered to permit access to consumer financial account data securely and easily, without charges that favor any one application or technology over another. To empower consumers, any regulations under Section 1033 should clearly delineate the possible classifications for entities and associated obligations. The regulations should further mandate the adoption of Industry-developed standards that promote security and flexibility.

FIN would be pleased to meet with the Bureau to discuss these issues or any other issues.

Respectfully submitted,



Brian Peters, Executive Director
Financial Innovation Now
1155 F Street NW
Washington, DC 20004
info@financialinnovationnow.org