Data Access Network

JANUARY 25, 2023

6 Liberty Square #2381, Boston, MA 02109 USA | akoya.com

Submitted electronically: Financial_Data_Rights_SBREFA@cfpb.gov

Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Comments on Small Business Review Panel for Required Rulemaking on Personal Financial Data Rights – Outline of Proposals and Alternatives Under Consideration

Dear Sir or Madam:

Akoya[1] appreciates the opportunity to provide comments on the Consumer Financial Protection Bureau's ("CFPB") Outline of Proposals and Alternatives Under Consideration for the Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights (the "SBREFA Outline"). Akoya believes it has a unique perspective to offer the CFPB as it seeks to implement Section 1033 of the Dodd-Frank Act. Akoya is a pro-consumer small business that believes that there should be competitive options for consumer data access.

Akoya applauds the efforts to date of the CFPB with respect to implementation of Section 1033 and looks forward to a Section 1033 final rule in the not-too-distant future. The CFPB's 2017 Principles for Consumer-Authorized Financial Data Sharing and Aggregation ("Principles") have provided valuable guidance to the financial services industry. We anticipate that a final rule on Section 1033 will significantly advance open banking in the United States if it is consistent with the Principles and coordinated with other federal financial services regulators to avoid conflicting regulatory positions.

Akoya is transforming the way consumers access their financial data by ensuring that data access and sharing is done in a secure and transparent manner. We aim to make accessing consumer financial data as easy and safe as possible by helping the industry move authorized data access (commonly referred to as "data aggregation") from credential-based data access (commonly referred to as "screen scraping") to access through an application programming interface ("API"). The Akoya network enables financial institutions to conduct consumer-authorized data sharing in a secure standard API format that aligns with the Principles, including informed explicit consent, transparency and control, and data minimization. Akoya is available to work with banks and other data providers of all sizes.

Akoya believes that data access has been a key driver of innovation in the financial services industry, yielding many benefits for consumers. For more than two decades, consumers have been using online services and financial technology applications to

[1] Originally created within Fidelity Investments, Akoya was developed to eliminate the risks associated with credential-based data access. In February 2020, realizing the value Akoya brought to the entire financial services industry, The Clearing House coordinated 11 of its member banks, including Bank of America, Capital One, Citi, Huntington Bank, JPMorgan Chase, KeyBank, PNC Bank, TD Bank, Truist, U.S. Bank, and Wells Fargo, to become equal owners of the now independent company alongside FMR LLC (the parent company of Fidelity Investments).

consolidate their financial information, whether it be for financial planning, budgeting, applying for loans, investing, tax preparation, or other essential financial tasks. Consumers value these products and services, and data access has enabled their development. Many of these applications have also facilitated access to products and services for many previously underserved communities.

While data access provides real benefits to consumers, it also comes with risks for consumers. Akoya believes that the best way to enhance the benefits of data access is to ensure that such access is provided in a safe, secure, and transparent manner. We believe that the CFPB's rulemaking to implement Section 1033 of the Dodd-Frank Act can and should help ensure that data access is provided in a safe, secure, and transparent manner. This letter includes four recommendations, which touch on a number of specific questions raised in the SBREFA Outline, for the CFPB to consider as it proposes a rule to implement Section 1033 of the Dodd-Frank Act.

1. The CFPB should prohibit screen scraping.

Screen scraping is neither secure nor transparent for consumers and needs to end. Often, consumers do not understand the scope or duration of access they are providing to data recipients and data aggregators. In fact, many consumers are unaware that their login information and financial data are stored by the data aggregator instead of, or in addition to, the data recipient. Screen scrapers also often access more data than is necessary to provide the service the consumer wants. Moreover, screen scrapers may continue to access consumer data even when a consumer no longer uses the service provided by the data recipient because there is not a clear and simple process for consumers to revoke the screen scraper's ongoing access to their data without consumers having to change their login credentials at their financial institution. This can result in third parties holding consumer login credentials and continuing to access a consumer's financial data for an indefinite period, unbeknownst to the consumer, which poses a significant privacy risk.

There is also a significant security risk with screen scraping. This risk is exacerbated by the common practice of consumers to use the same login credentials across multiple web services. This leaves consumers' accounts vulnerable to "credential stuffing" – a type of cyberattack where bad actors obtain stolen consumer login credentials and use them repeatedly across several sites until they find a match. In a September 2020 notification, the Federal Bureau of Investigation ("FBI") highlighted that "[c]redential stuffing attacks accounted for the greatest volume of security incidents in the financial sector at 41 percent of total incidents from 2017 through 2019, according to a 2020 cybersecurity firm report."[2] Given the risks associated with stolen consumer credentials, it is not surprising that a 2018 report from the United States Department of the Treasury found that "there was universal agreement among financial services companies, data aggregators, consumer fintech application

[2] FBI Cyber Division, *Private Industry Notification – Cyber Actors Conduct Credential Stuffing Attacks Against US Financial Sector* (Sept. 10, 2020), https://www.documentcloud.org/documents/7208239-FBI-PIN-on-credential-stuffing-attacks.html.

providers, consumer advocates, and regulators that the sharing of login credentials constitutes a highly risky practice."[3]

Screen scraping is also fragile and prone to disruptions that slow or stop the flow of data between data providers and data recipients. For example, data access fails when consumer financial accounts require two-factor or multi-factor authentication and can break down when data providers change or update the technology related to the user experience. The practice is also subject to fluctuations in internet traffic — if systems are too busy during an uptick in usage of a data provider's online services, data aggregators are often impacted first. When these factors come into play, the flow of data decelerates, the consumer's user experience deteriorates, and the costs for data providers to support screen scraping increase.

Given technological advances such as APIs, it is increasingly not necessary to rely on screen scraping. APIs act as software intermediaries that allow applications to communicate with one another – and in this case, provide access to data. API-based data access can be used by data providers to authenticate and authorize consumers directly, thus eliminating the need for login credentials to be held and stored externally by a data aggregator or data recipient. This significantly mitigates the privacy and security risks stemming from screen scraping. In addition to being more secure, APIs can also enable increased transparency and control for consumers.[4] Moreover, ending screen scraping will ultimately benefit small data providers, as they will be less likely to suffer losses from unauthorized transactions that result from consumer credentials being stolen from data aggregators or data recipients.

Akoya believes that the CFPB should be explicit in prohibiting screen scraping, although we understand that this may require time and priority setting as we progress toward that goal.[5] However, the CFPB should not prescribe the method of authorized data access that data providers must adopt. Rather, the CFPB should permit data providers to choose and direct the methods that data aggregators and data recipients may use to access consumer financial data held in data provider systems. Data providers are both large and small companies, with varied financial and operational resources and technological capabilities. Some data providers may wish to develop their own APIs and integrate directly with data aggregators and data recipients. Others may wish to integrate with a data access network, such as Akoya, that will serve as a single point of access to the data provider for all data aggregators and data recipients. Yet others may wish to rely on a core back-end service provider to facilitate API connections with data aggregators and data recipients or to connect to a data access network. The CFPB should offer data providers this flexibility because it will minimize the burden on small data providers without undermining the fundamental objective of ending screen

---

[3] U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities – Nonbank Financials, Fintech, and Innovation* (July 2018), https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf.

[4] APIs are central to safe and secure open banking, and it is important that the CFPB take no action that would limit the use cases in which data providers and authorized third parties may use APIs to achieve the full breadth of open banking.

[5] The CFPB has asked whether data providers should be required to permit screen scraping when a data provider's method of access (e.g., its API) experiences a service interruption. In our view, whatever minimal disruption occurs when a data provider's method of access is inoperable is not sufficient to justify screen scraping and the serious risks that it involves.

scraping. Also, it will allow each data provider to use the technological and operational solution that is best for it. Similarly, the CFPB should allow each data recipient and data aggregator to choose the approach that is best for it to receive data that is made accessible by a data provider. For example, for a data recipient, this may mean a direct connection to a data provider, working through a data aggregator, connecting to a data access network, etc. Moreover, given that technology is constantly evolving, it is important that the CFPB avoid being too proscriptive in defining data access standards.

Akoya acknowledges that not all data providers currently have third party access portals. We also believe that eliminating credential sharing is of the utmost importance to protect consumers and our financial system and it is important to make substantial progress toward this goal. Thus, Akoya does support the CFPB's thought process of giving certain classes of data providers a finite amount of time to stand up their third-party access portal. Moreover, to move towards a safer, more secure, and more transparent means of data access, Akoya believes the CFPB should work collaboratively with industry standard setters such as FDX to end screen scraping, speed up the adoption of third-party access portals, and define industry standard use cases.

2. **The CFPB should require that data recipients enable consumers to monitor access to their data on an ongoing basis and provide a means for consumers to revoke access to their data at any time.**

As discussed above, many consumers neither understand the full scope of access they are providing nor the parties to whom they are providing access. Accordingly, to protect and empower consumers, the CFPB should require that data recipients display to consumers the types of data that they are accessing on behalf of the consumer and that they are storing and the associated data provider from which the data is or was accessed. This information will help consumers understand their data footprint and make better decisions about the data recipients they use. Also, the CFPB should require data recipients to provide a mechanism for the consumer to easily monitor and revoke the access.

3. **The CFPB should require that data recipients obtain explicit and informed consent from consumers to access their data and limit data recipients' access only to data necessary to the service they are providing unless consumers have provided specific consent to access additional data.**

Consumers are typically seeking to use the applications of data recipients and are permitting access to their data for that purpose. They generally are not intentionally providing access for other purposes. Accordingly, data recipients should obtain explicit and informed consent from consumers to access their data. Moreover, data recipients should limit consumer data access only to data that are necessary to provide the service requested by the consumer. If it wants to access additional data, then a data recipient should have to obtain specific consumer consent for that additional data. Also, data recipients should limit the duration of consumer data storage to no more than is necessary to provide the requested service. Terms and conditions presented in multi-page documents to consumers should not include open-ended language stating that consumer financial data can be used for "any legal

purpose," "for any purpose including…" or other similar disclaimers. Accordingly, the CFPB should develop clear standards for collection, use, and retention of consumer information by data recipients and develop model language for the consents to be obtained by data recipients.

4. **The CFPB's rulemaking to implement Section 1033 should cover data providers that hold consumer account information and not only financial institutions as defined in Regulations E and Z.**

The SBREFA Outline contemplates that the CFPB's rulemaking to implement Section 1033 would apply to financial institutions as defined in Regulations E and Z. Akoya believes that this is inconsistent with the statutory text, would harm consumers, and would create an unlevel playing field among industry participants.

Section 1033 provides that "a covered person shall 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 . . ." A covered person is defined as "any person that engages in offering or providing a consumer financial product or service." There are a number of companies (e.g., credit bureaus, payment applications, digital wallets, cryptocurrency, etc.) that offer or provide consumer financial products or services that are not financial institutions as defined by Regulations E and Z. If the CFPB defines data providers as contemplated in the SBREFA Outline, it would be inconsistent with the statutory text. Such a distinction would be particularly harmful for small banks and credit unions that compete with companies that would not be covered by the rulemaking. Moreover, by limiting the number of institutions subject to the rule, the CFPB would harm consumers by enabling screen scraping to continue for numerous consumer financial accounts.

* * * * *

A thoughtful 1033 rule will ensure that consumers have access to their financial information in a seamless manner with due regard to data privacy and security considerations while fostering the growth of open banking in a safe and sound manner. We look forward to sharing our views with the CFPB as it works through this important rulemaking process so that the agency may benefit from our experiences at the center of the open banking movement. Should you have any questions or require additional information, please do not hesitate to contact me at anil@akoya.com.

Sincerely,

Anil Mahalaha
Vice President and Chief Evangelist
Akoya LLC
6 Liberty Square #2381
Boston, MA 02109