December 29, 2023

Submitted electronically: https://www.regulations.gov

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

Re: Comments on Required Rulemaking on Personal Financial Data Rights, Docket No. CFPB-2023-0052, RIN 3170-AA78

Dear Sir or Madam:

Akoya LLC ("Akoya") appreciates the opportunity to provide comments on the proposed rule issued by the Consumer Financial Protection Bureau ("CFPB") to implement Section 1033 of the Consumer Financial Protection Act of 2010 (the "Proposed Rule"). Akoya supports the issuance of the Proposed Rule, which would take important steps toward implementing Section 1033. This comment letter offers suggestions to enhance the consumer-focused approach the CFPB has taken through this rulemaking process while promoting a secure, fair, open, and competitive data access ecosystem.

Akoya optimizes security and transforms the way consumers access their financial data in two primary ways. First, the Akoya data access network allows an authorized third party or data aggregator to access consumer-permissioned data from multiple financial institutions of all sizes in a secure standard application program interface ("API") format. Akoya's network is unique because it is API-only. We do not access data by using a consumer's online banking login credentials and do not "screen scrape." The Akoya network was designed and built upon values that align with the Proposed Rule, including informed explicit consent, transparency and control, and data minimization.

Second, Akoya acts as a service provider to data providers that use Akoya to build and maintain developer connections with multiple third parties, including authorized third parties and data aggregators. In this capacity, Akoya can work with any data provider that seeks a third-party service provider to offer and manage its developer interface.

In sum, Akoya's mission is consumer-focused, with no screen scraping, no secondary-use monetization of data, and an emphasis on consumer consent, transparency, and control.

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 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 and even facilitated access to products and services for many previously underserved communities. However, data access comes with risks for consumers. Akoya believes that the best way to mitigate the risks is to ensure that data access is provided in a safe, secure, and transparent manner, and the Proposed Rule will go a long way toward achieving this objective.

This letter includes the following recommendations to sharpen and expand certain consumer protections in the Proposed Rule and promote fair and open competition among participants in the market:

1. The CFPB should enhance security measures by banning screen scraping and promoting tokenized account numbers when Regulation E accounts are used for payments.

2. The CFPB should enhance consumer control by refining the necessary content for consumer authorization disclosures, strengthening revocation requirements, and permitting only narrowly circumscribed secondary data uses.

3. The CFPB should take steps to promote choice for consumers' authorized third parties by requiring data aggregators and service providers to adhere to qualified industry standards that enable portability.

4. The CFPB should clarify the role of industry standard-setting bodies ("SSBs") by recognizing the Financial Data Exchange ("FDX") at the time of publication of the final rule and creating a safe harbor for compliance with qualified industry standards.

5. The CFPB should clarify the definitions of "covered consumer financial product or service" and "data provider."

1) The CFPB should enhance certain security measures.

a) The CFPB should prohibit "screen scraping."

The preamble of the Proposed Rule acknowledges that there is "nearly universal consensus that developer interfaces should supplant screen scraping."[1] The CFPB discusses the role that screen scraping has had in the development of the open banking

[1] 88 Fed. Reg. 74796, 74798 (Oct. 31, 2023).

industry but also rightly highlights the risks associated with its continued use. For example, the CFPB states that "screen scraping may pose risks to consumers' data privacy and security by capturing and storing consumer credentials and potentially capturing more data than are reasonably necessary to provide the requested product or service."[2] The preamble also estimates that only about half of third-party data access currently happens through APIs and the bulk of the balance is done through screen scraping.[3] The Proposed Rule, however, only takes a first step towards phasing out screen scraping. We recommend that the CFPB go further to close the door on this risk to consumers.

We recommend a two-step approach to mitigating the harm to consumers from screen scraping now to ensure access to covered data goes through secure developer interfaces. First, the CFPB should prohibit an authorized third party or data aggregator from using and storing consumer credentials to access covered data that are available through a data provider's developer interface once that developer interface is available for access. Consumer credentials and historical data that were stored prior to the availability of the developer interface should be deleted. Second, the CFPB should require data providers to make reasonable efforts to block access to covered data from a third party through the use of credentials once the data provider has made its developer interface available. We recognize that blocking screen scraping is technically complex and that no blocking methodology can prevent screen scraping entirely. We believe, however, that obligating data providers to undertake at least reasonable efforts to block screen scraping is not unfairly burdensome or costly.

At least three reasons support this change.

- First, the continued storage of consumer credentials by data aggregators represents a significant ongoing data security risk for consumers. Third parties that hold consumer credentials have unfettered access to all capabilities at the financial institution, including making payments and changing profile information. And large pools of consumer credentials are a potential target for criminals and wrongdoers.

- Second, data aggregators' legal ability to continue to screen scrape threatens the uptake of developer interfaces. Absent a ban on screen scraping, authorized third parties and data aggregators effectively will have an option either to access covered data through a developer interface or to continue to screen scrape.

- Third, banning screen scraping after a developer interface is available will enhance competition among data aggregators, which will benefit authorized third parties and consumers. Currently, a data aggregator's willingness to engage in screen scraping provides it with a bargaining chip, since data providers may

[2] Id. at 74799.
[3] Id. at 74798.

prioritize commercial agreements under which those data aggregators voluntarily agree to end the practice. By banning screen scraping, the CFPB will remove an inherent advantage held by large incumbent screen-scraping data aggregators, providing more competition among data aggregators and choice for authorized third parties. More choices for authorized third parties among their respective service providers ultimately will benefit consumers on whose behalf they act.[4]

b) The CFPB should continue to promote tokenization of payment credentials when Regulation E asset accounts are used for payments.

"Covered data" under the Proposed Rule includes information to initiate a payment to or from a consumer's Regulation E account. The Proposed Rule would allow a data provider to make available a tokenized account and routing number instead of, or in addition to, a non-tokenized account and routing number. Tokenization substitutes random digits for actual account numbers when making a payment. The randomized "token" facilitates a specific payment transaction, but it has no independent value and is not sensitive. And even if compromised, the token can be deactivated.

Tokenized account numbers offer numerous advantages to consumers. They put consumers in control of their sensitive data, allow consumers to revoke the tokenized number immediately when consumers revoke consent for an application that is utilizing a tokenized number, and prevent consumers from having to set up new accounts or receive new cards in instances of fraud. In the Proposed Rule, the CFPB acknowledges that tokenized account numbers are in use today and have benefits throughout the ecosystem, such as mitigating fraud risk to consumers and data providers.[5] We support the use of tokenized account numbers as much as possible and therefore encourage the CFPB to promote their use for open banking. The CFPB should promote interoperable, tokenized account numbers to be used for Regulation E accounts when used for payments.

---

[4] We encourage the CFPB to expressly recognize and permit one use of consumer credentials that is distinguishable from screen scraping and does not pose the same consumer risk. Often, to facilitate access to a consumer's financial data through the data provider's API, an authorized third party or data aggregator may provide a portal that redirects the consumer to the data provider's website on which the consumer enters credentials and enables access to the financial data that subsequently flows back through the portal to the third party. This structure differs from screen scraping, because the consumer does not give credentials to the third party itself to use to access the consumer's data from the data provider. Instead, through the portal arrangement, the consumer uses the credentials directly at the data provider to authenticate himself or herself and to authorize the data transfer, with the third party merely serving as a conduit to connect the consumer and data provider. Although Akoya's understanding is that this arrangement is already permitted under the Proposed Rule, Akoya encourages the CFPB to clarify expressly that this type of arrangement is permitted and does not constitute prohibited use of a developer interface with credentials.

[5] 88 Fed. Reg. at 74811.

2) The CFPB should take certain steps to enhance consumer control over data.

a) The CFPB should refine the required content of the consumer authorization disclosure to include information about the frequency, recurrence, and duration of data access.

Consumer consent should be a foundational element of a sound open banking system. We applaud the CFPB for including in the Proposed Rule clear, straightforward, and meaningful requirements for both the delivery and content of the consumer disclosure and consent to permit data access. We note that consumers will benefit from clarity around the what, who, how, and why of sharing their data before providing consent.

We suggest that the CFPB refine the Proposed Rule by adding a requirement that the consumer consent include a clear and accurate description of the frequency, recurrence, and duration of the authorized third party's data access. Authorized third parties that seek to verify account ownership, for example, may only require a single instance of data access. Other authorized third parties seek to access a consumer's data much more often, in some cases multiple times each day during the consent period. Consumers should be aware of these differences at the time they choose to consent to data access so they can properly consider whether to share their information with a particular company.

b) The CFPB should facilitate simple revocation by requiring that data providers display information about where data are going and offer a revocation mechanism.

Revocation is the necessary partner of consent: for consent to be truly effective, it must be possible to withdraw it. Again, we applaud the Proposed Rule's section 1033.331(e), which provides for a mechanism to revoke third party authorization to access covered data. That section permits a data provider to make available to a consumer a reasonable method to revoke any third party's authorization to access all of a consumer's covered data.

We believe the CFPB should go further to empower consumers by also requiring data providers to enable revocation from their own digital banking platforms.

Currently, some financial institutions' digital platforms display to consumers the third parties with which they are sharing data and allow consumers to "toggle off" sharing for specific third parties from that platform, without visiting the third-party site or application. This enhances consumer control. Without such information, some consumers might forget that they provided a third party with permission to access their data or might mistakenly believe that the third party would access their data for a limited time when the data collection in fact is ongoing. In either case, the consumer would not think to check with the third-party application, meaning that the data collection could

continue without the consumer's awareness. Data providers that provide consumers with transparency and visibility about where their data are going and empower consumers to turn off such sharing greatly mitigate these consumer risks.

c) The CFPB should permit narrowly circumscribed secondary data uses by authorized third parties but only with enhanced consumer disclosure requirements, and should prohibit other third parties from any secondary uses including of deidentified data.

The Proposed Rule imposes limitations on third parties with respect to their collection, use, and retention of consumer data, including doing so only as "reasonably necessary to provide the consumer's requested product or service." Akoya generally supports the CFPB's approach to this issue. We recognize, however, that authorized third parties may have the ability to use the covered data it collects to offer other products or services to the consumer or to improve their models or systems, which could benefit consumers.

Any provision in the final rule allowing such limited secondary data uses should include stringent consumer consent requirements. Akoya supports principles articulated by the Financial Technology Association for engaging with consumers, including (1) full transparency regarding data collection and use, (2) consumer control of personal data, (3) provider use of data for stated and transparent purposes, (4) plain language disclosures, and (5) non-discrimination.

We are concerned, however, that consumers *when initially consenting to allow third parties to access their data for a particular product or service* may be distracted and may not be in the best position to fully assess choices related to their data. Consumers signing up for a product or service might not take the time to fully review terms and conditions that include broad permission for secondary data uses when their primary interest is in completing the transaction. We therefore are skeptical that merely increasing the number of disclosures at that point in time will improve a consumer's ability to provide informed consent for secondary data uses. We offer three suggestions to optimize consumer control over the use of related data:

- The CFPB should prohibit authorized third parties from encouraging consumers to "opt in" to secondary uses of their data (i.e., uses beyond what is reasonably necessary to provide the product or service requested) at the time the third parties are obtaining express, informed consent to access covered data on the consumers' behalf.

- If the CFPB allows authorized third parties to seek permission for secondary uses of data, we recommend that the "opt in" consent for that use be obtained on a separate occasion from the origination authorization, product enrollment, or account opening.

- Permitted secondary uses should be limited to offering additional products or services to the consumer and to making improvements to models or systems used as part of the product or service initially requested by the consumer.

Finally, we suggest that only the authorized third party should be permitted to seek these limited secondary data use rights. Other third parties, including data aggregators, should be permitted to use data strictly as reasonably necessary to develop and provide the consumer's requested product or service.

3) The CFPB should take steps to promote choice for consumers' authorized third parties by requiring data aggregators and service providers to adhere to qualified industry standards that enable portability.

Third-party service providers to both data providers and authorized third parties are likely to play a key role in the open banking ecosystem after publication of the final rule. On the data provider side, there are over 9,000 financial institutions in the United States, a substantial majority of which are mid-sized and small regional and local banks and credit unions. Many of these institutions, some of which have made little progress with open banking, may look to service providers to assist them in building and operating developer interfaces. For authorized third parties, many of which are early-stage fintech companies, it may be easier to rely on data aggregators as service providers to access consumer financial data than to establish connections with dozens and potentially hundreds of developer interfaces.

Akoya commends the CFPB for recognizing in the Proposed Rule that these third-party services will play an essential ongoing role in supporting both smaller financial institutions (as data providers) and fintech companies (as authorized third parties).

The CFPB should encourage competition among data aggregators to benefit consumers and provide access to a greater number of products and services from a wider range of authorized third parties. When an authorized third party, acting on behalf of a consumer, can choose freely from multiple data aggregators, it can select a data aggregator that best serves the consumer based on the criteria relevant to the specific use case (e.g., speed, security, or value-added services).

Fostering competition among data aggregators includes facilitating the ability of an authorized third party to switch data aggregators. The Proposed Rule goes a small measure in this direction by acknowledging that an authorized third party may access data through a data aggregator that it retains after a consumer has completed the required authorization procedures, which could include changing from one data aggregator to another.

We believe that the CFPB should do more to facilitate the ability of an authorized third party to switch data aggregators. Currently, data aggregators use proprietary APIs to interface with authorized third parties, which may require bespoke connections from authorized third parties. This makes changing data aggregators difficult for authorized third parties, because of the additional technical resources required to connect to a new data aggregator's API. The CFPB should require uniform standards for the connections between data aggregators and authorized third parties, as defined by an SSB. This would lower the cost of authorized third parties to change from one data aggregator to another, and thereby drive business to the most competitive data aggregators, all to the ultimate benefit of consumers.

4) The CFPB should clarify the role of SSBs.

Akoya applauds the CFPB for drafting a Proposed Rule that references qualified industry standards on various issues. SSBs, with input from all participants in the open banking ecosystem, are best positioned to develop standards that are fair, practical, and representative of the current state of the industry. In effect, the CFPB wisely "future proofs" open banking regulation by incorporating qualified industry standards in the Proposed Rule.

We suggest the CFPB make two revisions to the Proposed Rule on this topic.

a) The CFPB should recognize FDX at the time of the initial publication of the final rule.

First, in the final rule, the CFPB should either formally recognize a specific SSB or commit to doing so in a very short time frame after publication. The purpose of this suggested revision is to avoid competing standards that will cause confusion in the industry and inhibit interoperability and innovation. As currently drafted, the Proposed Rule describes characteristics of an effective SSB, but does not recognize one or more than one. This creates the possibility of a long time period after publication of the final rule during which there is no recognized SSB. There could be several organizations that work towards recognition as an SSB during that time period, each developing its own potentially contradictory standards that it would propose to be utilized as qualified industry standards. This could create confusion and paralysis in the industry, as no participant in the ecosystem would have confidence that any particular standard would achieve recognition. The CFPB can avoid this situation by recognizing an SSB at the time of publication of the final rule.

Akoya suggests that the CFPB should recognize FDX as an SSB. FDX is a nonprofit organization dedicated to establishing a common, interoperable, and royalty-free standard for the secure access of user-permissioned financial data called the FDX API. FDX already provides data format standards, guidelines, and best practices for UX, security, and communication protocols. FDX also should develop a certification program to track adherence to standards. However, FDX should not set data security or third-

party risk management standards nor should FDX manage an accreditation program for third parties.

b) The CFPB should create a safe harbor for compliance with qualified industry standards.

We also urge the CFPB to create a compliance safe harbor for data providers, data aggregators and authorized third parties that adhere to qualified industry standards with respect to the elements of the Proposed Rule that reference qualified industry standards. Many participants in the ecosystem will no doubt adhere to qualified industry standards in designing and operating their infrastructure. Under the Proposed Rule, where indicated, this will be indicia of compliance. But the clear and reasonable negative inference to be drawn from this approach is that the CFPB may in its discretion decide that an industry participant is in violation of the final rule notwithstanding the participant's strict adherence to qualified industry standards. We believe that this is an unfair approach. If the CFPB references qualified industry standards in the final rule (which is a thoughtful way to draft regulations that govern a nascent industry), then adherence to those standards should result in the same certainty of compliance as adherence to specific requirements that are codified in the final rule. This predictability is essential for businesses to develop new and innovative open banking services for consumers.

5) The CFPB should clarify the definitions of "covered consumer financial product or service" and "data provider" to empower consumers with a more complete view of their finances.

The CFPB proposal covers Regulation E accounts, Regulation Z credit cards, and products or services that facilitate payments from a Regulation E account or a Regulation Z credit card. The CFPB indicates that payment data from these products and services support common beneficial consumer use cases today, including transaction-based underwriting, payments, and comparison shopping for bank and credit card accounts.[6] The CFPB proposal should expressly include all consumer financial products and services that are commonly described as "digital wallets," "payment apps," "funds transfer apps," or "person-to-person payment apps." These product and services are provided by neobanks, digital wallet providers, and similar nondepository entities and should qualify as covered data providers. Providers of consumer financial products and services delivered through these digital applications help consumers to make a wide variety of consumer payment transactions. A more specific definition will help avoid creating unintentional loopholes as the market evolves.

* * * * *

[6] Id. at 74803.

Akoya appreciates the effort that the CFPB has put into the Proposed Rule. We anticipate that the final rule from the CFPB 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. Should you have any questions or require additional information regarding this letter, please do not hesitate to contact me at behram.panthaki@akoya.com or Anil Mahalaha, Vice President and Chief Evangelist, at anil@akoya.com.

Sincerely,

Behram Panthaki
Chief Operating Officer
Akoya LLC
6 Liberty Square #2381
Boston, MA 02109