October 21, 2025

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

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

Re: Comments on Advance Notice of Proposed Rulemaking for Personal Financial Data Rights Reconsideration; 12 CFR Part 1033, Docket No. CFPB-2025-0037, RIN 3170-AB39

To Whom it May Concern,

Akoya LLC ("Akoya") appreciates the opportunity to provide comment on the Consumer Financial Protection Bureau's ("CFPB" or "Bureau") Advance Notice of Proposed Rulemaking ("ANPR") seeking input on the implementation of section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Section 1033" and "Dodd-Frank Act").

Akoya's mission is to empower consumers to take control of their finances by giving them control over their data. We help leading financial institutions and technology companies of all sizes provide secure data access for customers. Akoya's data access network connects over 4,600 financial institutions, fintechs, credit unions, and data aggregators. Our model is tokenized, permissioned, and pass-through: we do not store consumer credentials, engage in screen scraping, or harvest consumer data for monetization. Each month, our infrastructure facilitates over a billion secure data transmissions, enabling innovation while prioritizing security, privacy, and consumer control.

Akoya LLC. © 2025. All rights reserved.

Open banking (or open finance) in the United States has been market-led, with fintechs, financial institutions, and data aggregators developing data-sharing technologies and consumer-centric solutions. Section 1033 provides the necessary statutory framework to accelerate the industry's progress and ensure consistency, fairness, and consumer protection. The Bureau's Personal Financial Data Rights final rule ("PFDR Rule") was an important step in this direction, particularly in setting standards for security, data use and retention, and consumer consent. We support the Bureau's decision to revisit the PFDR Rule to refine key provisions and close gaps identified since its publication.

We believe the revised regulatory framework should rest on three mutually reinforcing principles, much like three legs of a stool. These three principles—qualified API access, prohibition on unsafe screen scraping, and a sustainable access fee framework—directly advance the Bureau's objectives of promoting access, security, and competition. **First, financial institutions should be required to build and maintain developer interfaces that are available to all qualified third parties, provided those third parties have fulfilled their own obligations under the rule (e.g., have obtained proper consumer authorization) and meet risk-management standards.** On this front, the PFDR Rule mostly gets it right. **Second, once such interfaces are available, the rule should prohibit reliance on credential-based screen scraping by third parties and aggregators.** Allowing screen scraping alongside APIs leaves a back door, imposing obligations on financial institutions while creating options for third parties—a structural imbalance that undercuts consumer protection. **Third, the rule should allow financial institutions to charge reasonable fees for data access.** Without a sustainable fee structure, open banking risks becoming a costly mandate rather than a durable ecosystem, and smaller institutions (and their customers) will be left behind. The PFDR Rule missed an important opportunity on these two latter points, and Akoya welcomes the Bureau's willingness to reconsider them in this rulemaking.

The rulemaking process initiated by this ANPR should build upon the consumer protection mechanisms introduced by the PFDR Rule and strengthen the requirements that allow consumers to safely and securely access their data. It is also crucial that the changes to the PFDR Rule do not limit consumer choice, innovation, and competition through unreasonable restrictions on who is entitled to access data on a consumer's behalf. **Consumers, not institutions, must remain at the center of the financial data ecosystem.** No consumer should face heightened risk because of institutional carveouts

Akoya LLC. © 2025. All rights reserved.

or outdated, unsafe practices like screen scraping. Time is of the essence in setting and enforcing compliance deadlines because consumers are at risk now. The Bureau should move quickly to finalize an enforceable framework, rather than allowing delays that enable unsafe practices to continue.

Our comments address how the Bureau can achieve these objectives while ensuring clarity, security, and competitive neutrality. Our letter includes the following points:

1. Screen scraping remains a systemic risk and should be banned outright.
2. Data providers should be able to charge reasonable fees to promote investment in expensive open banking infrastructure.
3. Consent, consumer control, and secondary use limitations should continue to be part of the PFDR Rule.
4. The term "representatives" under the PFDR Rule and Section 1033 should be interpreted to include commercial third parties, consistent with consumer expectations and market practice.
5. While compliance deadlines must be reasonable, a regulatory framework for open banking should be implemented with urgency.

I. Screen scraping remains a systemic risk and should be banned outright.

The PRDR Rule introduces important data security measures that Akoya believes will contribute to safe and secure data sharing. While the Rule took significant steps towards establishing meaningful requirements for third parties around information security, it failed to ban screen scraping outright, leaving the entire financial system unnecessarily exposed to vulnerabilities.

Screen scraping is the automated extraction of data from user interfaces. Consumers share their online banking credentials with third parties, who then use those credentials to log in to the financial institution's digital assets to access data. Consumers typically have limited visibility or control over how their log-in information is stored and how it is used after the initial authorization.

While the PFDR Rule promotes the establishment of API-based data access, it does not ban the practice of screen scraping even after API-based interfaces are made

Akoya LLC. © 2025. All rights reserved.

available by financial institutions. The Bureau clearly understood the risks associated with screen scraping when writing the PFDR Rule, stating that it "understands that credential-based screen scraping creates data security, fraud, and liability risks for data providers"[1] and noting the "inherent risks, such as the proliferation of shared consumer credentials and overcollection of data."[2] By leaving screen scraping as a viable option for accessing consumer financial data and failing to mandate API-only access under strict, uniform security standards, the PFDR Rule missed an important opportunity to protect consumers at scale and reduce unnecessary strain on the financial system.

In reassessing the PFDR Rule, the Bureau should implement a complete ban on credential-based access once data providers make developer interfaces available. This step would eliminate the need for consumers' log-in credentials to be stored by various market participants, a practice that introduces systemic risk into the financial ecosystem. API-based access, by contrast, establishes a consistent baseline for enhanced data security and consumer transparency. Over the years, as API-based data access continued to prove viable at scale, it created market incentives to move away from screen scraping and toward safer, standardized, consumer-permissioned data access. Akoya has always operated through APIs rather than credential-based methods, and our business model, along with overall progress in the industry, has proven it is not necessary for institutions to continue screen scraping once API-based data access is available.

Currently, third parties and other data holders store hundreds of millions of consumer login credentials outside of strictly regulated financial institutions. If these credentials are compromised via the work of bad actors, it could have wide-reaching effects both on consumers and on financial institutions. While screen scraping enables broad connectivity, particularly where secure APIs have not yet been established, it also introduces significant security, compliance, and user experience risks. Compromised credentials remain the most frequent attack vector for data breaches, with an average cost of $4.67 million per incident.[3] Retaining hundreds of millions of credentials across unregulated entities perpetuates a single point of potential failure across the financial system.

---

[1] Supplemental Information to the PFDR Rule at 89 Fed. Reg. 90,972 (https://www.federalregister.gov/d/2024-25079/p-1308)

[2] *Id.* at 89 Fed. Reg. 90,840 (https://www.federalregister.gov/d/2024-25079/p-96)

[3] IBM Security & Ponemon Institute, *Cost of a Data Breach Report 2025: The AI Oversight Gap* (2025), https://www.ibm.com/security/data-breach.

Akoya LLC. © 2025. All rights reserved.

Screen scraping is an obstacle to the actual adoption of secure, API-based interfaces for data access. Absent a complete ban, third parties effectively retain the option to avoid any regulatory requirements and data provider oversight that comes with these interfaces by continuing to screen scrape. This means that those who do not wish to prioritize consumer safety may continue to do so, while data providers are left with a mandate to build expensive infrastructure even as their customers remain exposed. At the same time, while data providers may wish to block screen scraping after making consumer data available through APIs, doing so can be prohibitively costly and complex, even for the most sophisticated institutions. With the advent of new AI tools, this becomes even more problematic, as data providers must grapple with autonomous AI agents and the accelerated development and deployment of workarounds to their attempts to block the practice. All of this shows that a screen scraping ban directed at third parties is the most effective way to shift the market away from outdated and unsafe methods to secure, API-based interfaces.

Because the PFDR Rule did not expressly prohibit credential-based access, screen scraping remains a de facto option even after APIs are available. As long as screen scraping remains viable, an insecure backdoor exists. At best, screen scraping as a method of access is outdated, and at worst it is a grave risk to consumers and the financial system. We urge the Bureau to use this new rulemaking process to require a full transition away from screen scraping and mandate APIs as the sole channel of access to covered data.

II. Data providers should be able to charge reasonable fees to promote investment in expensive open banking infrastructure.

Given Akoya's dual role as a service provider to financial institutions and operator of a data access network, we have a nuanced understanding of both the challenges related to accessing data to enable a business use case and the costs that financial institutions must bear to provide the proper infrastructure for safe and secure access. While any solution to the issue of fees must consider the impact on consumers and competition among financial service providers, financial institutions should be allowed to charge reasonable fees that support the continued maintenance, enhancement, and security of open banking infrastructure, thereby promoting its long-term sustainability for consumers and market participants alike. Without an ability to assess fees, open banking

Akoya LLC. © 2025. All rights reserved.

risks becoming a costly mandate rather than an effective driver of innovation, leaving many smaller institutions and their customers behind and undercutting the Bureau's goals of increasing consumer protection and fair competition.

Based on market feedback and discussions with multiple financial institutions, we believe that the Bureau, and many financial institutions themselves, underestimated both the initial and ongoing cost of supporting the required infrastructure outlined in the PFDR Rule. The largest financial institutions have invested millions of dollars to set up the required infrastructure over multiple years. These efforts include building APIs, implementing robust information security standards, and standing up third-party interfaces to enable integration. Additional millions of dollars are still needed to operate, support, and secure that same infrastructure. This involves ongoing support and maintenance, information security audits, network security services, cloud or onsite infrastructure, third party risk reviews, as well as executing and managing contracts with those third parties. While large financial institutions with data sharing infrastructure already in place will face lower initial implementation costs, they will still need to bear ongoing support and maintenance costs. Building and maintenance costs can easily range from multiple hundreds of thousands of dollars to a few millions of dollars per annum.

Regardless of size, banks and credit unions also bear costs that extend beyond building and maintaining a secure interface. Third parties derive inherent value from the numerous compliance obligations that these regulated entities are required to have in place to onboard consumers and maintain a banking relationship. For example, banks and credit unions invest significant resources in Know Your Customer (KYC) processes that establish and verify identity; this initial validation is then leveraged by third parties. Banks and credit unions also fund extensive fraud prevention and anti-money laundering (AML) programs. Third parties benefit from, and rely on, that validation when they process ACH transactions or other payment flows on behalf of the consumer. These regulation-based practices are foundational to the safety, soundness, and integrity of our financial system. They also provide quantifiable value to downstream actors who did not incur the initial cost.

Charging fees can help spur further data provider investment in data sharing and innovation after the initial implementation of required infrastructure. This is particularly important for small and medium-sized financial institutions, who otherwise may be challenged to maintain and improve the quality of service or user experience beyond the

Akoya LLC. © 2025. All rights reserved.

minimum requirements. For open banking to continue to evolve, it is important for all market participants to have an incentive to continue to invest and innovate.

Given the significant investment as well as potential legal, regulatory, and reputational risks that financial institutions must manage when participating in data sharing at scale, it is appropriate for commercial entities who benefit from the infrastructure that has been provided to pay reasonable fees to access it. We believe in an approach in which data providers are allowed to make a modest profit, provided that it is grounded in a defined standard of reasonableness and that these fees are not used to stifle competition. Private parties should have the flexibility to negotiate fees that reflect healthy market dynamics. We suggest a regulatory approach that is interested in policing and penalizing market abuses rather than mandating specific limits or formulas that may become outdated as the ecosystem changes.

A useful parallel exists in the healthcare sector, another highly regulated environment where data security and consumer safety are paramount. Under the Cures Act and related interoperability rules, covered entities may charge reasonable fees (which can include a reasonable profit margin) for the electronic exchange of patient information, provided those fees are based on objective, uniformly applied criteria and not conditioned on whether the party requesting the data is a competitor.[4] While the healthcare framework is not a perfect analogy to financial services, it illustrates that a fee structure can coexist with strong consumer protections when guided by clear principles of reasonableness and fairness.

A sustainable access fee framework is consistent with consumer protection. Properly designed, it ensures that those who benefit from secure, regulated infrastructure contribute to its maintenance, while safeguards against unreasonable or exclusionary pricing preserve innovation and competition. This is the balanced approach the Bureau should adopt as it revisits the PFDR Rule.

[4] 21st Century Cures Act: Interoperability, information blocking, and the ONC Health IT certification program (Final rule). 85 Fed. Reg. 25,642 (May 1, 2020); ONC, Cures Act Final Rule: Information Blocking Exceptions, April 2024 (https://www.healthit.gov/sites/default/files/2024-04/IB_Exceptions_Fact_Sheet_508_0.pdf)

Akoya LLC. © 2025. All rights reserved.

III. Consent, consumer control, and secondary use limitations should continue to be part of the PFDR Rule

The PFDR Rule represents a significant step forward in codifying consumer protection practices and addressing privacy risks. Akoya welcomes the Bureau's continued focus on these issues and offers several refinements to strengthen consent, control, and limitations on secondary use.

Consumer consent is a foundational element of a sound banking system, and as such we support the inclusion of clear, straightforward, and meaningful requirements for the delivery and content of disclosures, and consumer consent needed for data access. Akoya recommends that the Bureau clarify that meaningful consent includes clear disclosure of the **frequency, recurrence, and duration** of access authorized. Some use cases require only one-time retrieval; others involve recurring access over an extended amount of time. Providing this information at the point of consent enables consumers to make informed decisions and limits unexpected, unwanted ongoing data access.

Giving consumers ongoing control over their data is crucial to ensuring true consumer protection. Data providers should display, in real time, what type of data is being accessed and by whom. This would provide a deeper understanding of how data is being shared and processed, and whether a consumer wishes to continue providing it to the third party.

Data providers should also be able to provide simple tools for consumers to monitor, modify, or revoke access and prior consent. Providing such controls through the financial institution's digital banking interface would not displace third-party responsibilities. Rather, it would give consumers a single, trusted location to manage permissions. Currently under the PFDR Rule, a third party is required to provide a consumer with a method to revoke authorization that is as easy to access and operate as the initial authorization. A data provider on the other hand can only provide the consumer with the option to revoke consent completely, without the option to modify its scope (for example, by limiting access to particular accounts or data categories), which limits the ability of consumers to meaningfully manage who has access to their data and how. [5] Allowing data providers to enable this functionality through digital banking interfaces that

[5] 12 C.F.R. § 1033.331(e) and Supplemental Information to the PFDR Rule at 89 Fed. Reg. 90,838 90,909 (https://www.federalregister.gov/d/2024-25079/p-714)

Akoya LLC. © 2025. All rights reserved.

consumers trust would go a long way towards increasing control and visibility over financial data. It is also imperative that any revisions to the PFDR Rule preserve the provisions that address the consequences of revocation, under which third parties, subject to receiving a revocation request or notice of such a request, may no longer collect covered data and no longer use or retain covered data that was previously collected (12 C.F.R. § 1033.421(h)(2)). This contributes to true consumer choice and control by ensuring any use or retention of their data stops once their consent is withdrawn.

Lastly, Akoya believes it is crucial that the Bureau continues to support limitations on secondary uses by authorized third parties and data aggregators. As discussed in Section IV regarding the interpretation of "representative," Akoya's support for allowing commercial third parties to act as consumer representatives depends on these limitations, which ensure that representatives truly act "on behalf of" consumers. Covered data should only be used for purposes reasonably necessary to provide the product or service a consumer has requested. Allowing data aggregators or authorized third parties to use covered data for purposes like cross-selling, targeted advertising, or data sales would expose consumers to significant privacy and security risks and undermine informed choice. Even deidentified data can often be re-identified, a risk amplified by the proliferation of AI tools capable of correlating data sets. Opt-in or opt-out mechanisms are not sufficient to protect consumers who may lack the information necessary to give meaningful consent. The Bureau recognized these risks in the PFDR Rule and Akoya supports maintaining strict limits on secondary use to preserve consumer control and trust. If a third party has a use case that presents consumer benefits, it can be offered as a standalone product or service, with a dedicated disclosure and consent path that will allow the consumer to make an informed choice. Maintaining strong consent, revocation, and purpose-limitation standards will ensure that open banking operates on consumer trust, the essential foundation for lasting innovation.

IV. The term "representative" under the PFDR Rule and Section 1033 should be interpreted to include authorized commercial third parties, consistent with consumer expectations and market practice.

The Dodd-Frank Act defines a "consumer" as an individual or an agent, trustee, or representative acting on behalf of an individual. This definition in turn serves as the basis to determine who, besides the consumer themselves, may request access to covered

Akoya LLC. © 2025. All rights reserved.

data from a data provider under Section 1033. The ANPR focuses on how the term "representative" in the definition of "consumer" should be interpreted by the Bureau; in particular whether "representative" should be understood to mean an individual or entity with fiduciary duties, and whether this would limit consumers' ability to access data.

We believe that "representative" should be understood broadly to mean third parties, whether fiduciaries or otherwise, acting under consumer authorization through standardized, verifiable processes that incorporate clear guardrails such as consent, scope, use limitation, and information security. Nothing in Section 1033 limits the term "representative" to entities with fiduciary duties. To the contrary, the statute's inclusion of agents, trustees, and representatives as distinct categories indicates that "representative" encompasses a broader range of authorized actors. The PFDR Rule takes care to define "consumer," "third party," and "data aggregator" separately but does not define a "representative." We believe this intentional omission reflects the proper interpretation of a "representative" that is not limited to entities with fiduciary duties. For more than a decade, third parties—including data aggregators, fintechs, and service providers without fiduciary duties—have accessed consumer financial data through consent-based models. This reflects settled industry practice and consumer expectations.

Moreover, the PFDR Rule already imposes functional fiduciary-like duties—such as informed consent, data minimization, and use limitation—that collectively require that authorized third parties act in the consumer's interest. While there may be additional requirements that Akoya would like to see (see above), the framework introduced in the PFDR Rule is designed to ensure that any authorized third party that seeks to access consumer data must in fact be acting on behalf of that consumer and at their request for that access to be granted. It is through careful consideration of these requirements, rather than through limiting what constitutes a "consumer" for the purposes of Section 1033, that the Bureau can meaningfully increase consumer safety and data security, while continuing to enable meaningful access to financial data.

Importantly, Akoya's position that "representative" should include authorized third parties applies only where those parties act on behalf of the consumer and within the guardrails established by the PFDR Rule, particularly the prohibition on secondary use. Section 1033 allows representatives to access data solely for purposes that benefit the consumer who authorized the access. Any use of covered data for the representative's own benefit—such as product development, cross-selling, targeted advertising, data resale, or other secondary use—falls outside the scope of acting "on behalf of" the

Akoya LLC. © 2025. All rights reserved.

consumer and therefore outside the meaning of "representative." The secondary-use limitation is thus a critical safeguard that keeps commercial participation consistent with the statute's text and purpose.

Consumers have come to rely on widespread data access, expecting to be able to provide their data instantly, securely, and seamlessly across a wide variety of financial tools and applications. The development of open finance has enabled use cases across sectors such as banking, insurance, investments, lending, retail, healthcare, tax preparation, and more. The availability of standardized consumer data has led to an explosion of innovative financial products, while allowing consumers to have more control over their data and more insights into how it is utilized. According to the Financial Data Exchange, roughly 114 million customer connections are now made through APIs aligned to the FDX API Standard.[6] Over ten thousand fintechs operate in the US, a tenfold increase in only 12 years, largely due to the widespread adoption of open banking.[7] According to a consumer survey conducted by Visa, 87% of consumers have linked financial accounts to third party applications, with the average consumer connecting to more than four open-banking powered applications at any given time.[8] This illustrates how integral open banking has become to the financial sector.

It is our view that a narrow reading of the term representative, allowing only entities with a fiduciary duty to their customers to access data under the rule, would be detrimental to the continued development of the ecosystem and harmful to consumers. Section 1033 was introduced to facilitate access to financial data, enabling consumers to share it with providers of other services, including fintechs, of their choosing. A reading of Section 1033 that would require a fiduciary relationship for third parties would severely limit the utility of a consumer's data sharing rights, contrary to legislative intent and market-driven practice. Interpreting Section 1033 narrowly would also mean that third parties seeking consumer data would have to shoulder greater legal obligations than the financial

[6] Financial Data Exchange, "114 Million Reasons to Keep Moving Forward on Industry-Led Standard for Secure Data Sharing," Financial Data Exchange (Apr. 25, 2025), https://www.financialdataexchange.org/FDX/News/Press-Releases/114%20Million%20Reasons%20to%20Keep%20Moving%20Forward%20on%20Industry-Led%20Standard%20for%20Secure%20Data%20Sharing.aspx

[7] Statista, "Total number of fintechs and number of new fintechs founded in the United States from 2008 to 2024" (2025), https://www.statista.com/statistics/1476784/us-number-of-fintechs/

[8] Visa Inc., *The U.S. Open Banking Movement: How Consumers Are Driving U.S. Open Banking Innovation* (2023), https://corporate.visa.com/content/dam/VCOM/corporate/visa-perspectives/guides/documents/23a556e7-8cb6-43fa-b62b-f8af7e6212be.pdf

Akoya LLC. © 2025. All rights reserved.

institutions that currently hold that data, while also restricting the ability of even well-regulated banks to participate in data sharing as authorized third parties.

Meaningful data access requires that consumer choice and competition be preserved. That is why Akoya believes the best way towards a healthy open banking ecosystem is through secure, transparent, and seamless data access with robust controls rather than through limiting the types of entities that consumers can choose to provide them with financial products enabled by their data.

V. While compliance deadlines must be reasonable, a regulatory framework for open banking should be implemented with urgency.

A vast majority of American consumers already share their financial data with third parties—to make payments, qualify for loans, manage their money or access a broad range of other digital financial services. As adoption continues to grow, every day that compliance deadlines are extended is another day that consumer data is not adequately protected. Further delay only benefits those who have not yet invested in security infrastructure, leaving responsible actors and consumers to deal with the consequences.

Absent fundamental changes to the PFDR Rule, most large financial institutions already have the necessary infrastructure in place and will need only to refine their solutions and introduce appropriate policies and procedures. For small and medium sized data providers, more time may be needed, but that time should not exceed what is provided for currently under the PFDR Rule. Through Akoya's experience with providing services to financial institutions, we know the process can be completed effectively in the current timeframe, and further delays risk the safety of consumer data and the ongoing development of modern financial services based on technological innovation.

VI. Conclusion

Akoya supports the progress made towards facilitating secure and seamless data access for consumers through the PFDR Rule. At the same time, we urge the Bureau to improve the Rule, particularly by banning screen scraping and strengthening other security and consumer protection requirements.

Akoya LLC. © 2025. All rights reserved.

Should you have any questions or require additional information regarding this letter, please do not hesitate to contact me at courtney.robinson@akoya.com.

Sincerely,

/s/ Courtney Robinson

Head of Policy and Communications
Akoya LLC

Akoya LLC. © 2025. All rights reserved.