American Bankers Association

Ryan T. Miller
Vice President & Senior Counsel
Innovation Policy
(202) 663-7675
rmiller@aba.com

October 21, 2025

The Honorable Russell Vought
Acting Director
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Via Federal eRulemaking Portal: https://www.regulations.gov

Re: Docket No. CFPB-2025-0037, ABA Letter responding to Advanced Notice of Proposed Rulemaking on Personal Financial Data Rights Reconsideration [RIN 3170-AB39]

Dear Acting Director Vought,

The American Bankers Association[1] (ABA) appreciates the opportunity to respond to the Consumer Financial Protection Bureau's (CFPB or Bureau)'s Advance Notice of Proposed Rulemaking (ANPR) on Personal Financial Data Rights (PFDR or Section 1033) Reconsideration published in the Federal Register on August 22, 2025.[2] ABA and our members have expressed significant concerns with several aspects of the current regulation and we are grateful that new CFPB leadership recognizes the need to make substantial revisions thereto.

The Bureau specifically requested feedback on the following issues: 1) the proper understanding of who can serve as a "representative" making a request to access data on behalf of the consumer; 2) the optimal approach to the assessment of fees incurred by a "covered person" in responding to a customer driven request; 3) the threat and cost-benefit picture for data security associated with Section 1033 compliance; and 4) the threat picture for data privacy associated with Section 1033 compliance. The CFPB also inquired about appropriate compliance dates.

[1] *The American Bankers Association is the voice of the nation's $25 trillion banking industry, which is composed of small, regional and large banks that together employ approximately 2.1 million people, safeguard $19.7 trillion in deposits and extend $13.1 trillion in loans.*
[2] https://www.federalregister.gov/documents/2025/08/22/2025-16139/personal-financial-data-rights-reconsideration

In addition to the areas specifically solicited, ABA is providing feedback on other aspects of the existing PFDR rule (codified at 12 CFR 1033),[3] including pay-by-bank[4], industry standard-setting,[5] and other matters of vital importance to our members.

The November 2024 PFDR rule was overbroad and built on a dubious legal foundation, ultimately picking winners (fintechs and data aggregators[6]) and losers (banks and consumers) in the process. The rule simply cannot stand, either as a matter of jurisprudence or policy. In order to help the CFPB with its crucial goal of correcting the PFDR rule in its re-proposal, ABA makes a number of recommendations throughout this letter.

Before launching into our substantive response, we wish to emphasize at the outset the urgency for the CFPB to take formal action to suspend the compliance dates of the November 2024 PFDR rule immediately. According to the effective version of the PFDR rule finalized in November 2024, the first tranche of compliance dates for banks that hold at least $250 billion in total assets is April 1, 2026[7] (although the Eastern District of Kentucky tolled this, and other compliance tiers, for a total of 90 days each during the now-stayed *Forcht Bank* litigation against the CFPB).[8] The CFPB has clearly stated its intention to revisit and revise the severely flawed 2024 PFDR rule, both in the aforementioned litigation and as evidenced by this ANPR.

This letter will go into greater detail regarding the appropriate compliance dates in Section VIII, but those dates will be for the amended PFDR final rule. Significant back-office work, costing time and resources (both in material and personnel), is currently being devoted to building a compliance regime for the November 2024 PFDR rule.

Candidly, the first tranche of data providers is being irreparably harmed and wasting monetary and human resources by having to take steps in the interim to comply with a regulation that is undergoing substantial revision. Yet data providers do not have the luxury of ignoring the flawed November 2024 PFDR rule even if the Bureau itself has no intention of engaging in enforcement, because state regulators and/or state attorneys general may elect to do so. Under Dodd-Frank, state regulators and attorneys general can bring proceedings against entities to

[3] https://www.ecfr.gov/current/title-12/chapter-X/part-1033

[4] For additional information about pay-by-bank, *see* https://www.federalreserve.gov/econres/notes/feds-notes/pay-by-bank-and-the-merchant-payments-use-case-benefits-20250707.html.

[5] https://www.federalregister.gov/documents/2024/06/11/2024-12658/required-rulemaking-on-personal-financial-data-rights-industry-standard-setting

[6] As used throughout this letter, the term "data aggregator" refers to those entities operating as intermediaries in the data sharing ecosystem for information concerning financial products and services (rather than for data more broadly).

[7] *Supra,* note 3 at 12 CFR 1033.121(b)(1), https://www.ecfr.gov/current/title-12/chapter-X/part-1033/subpart-A/section-1033.121. Moreover, although ABA represents banks, it is worth noting that the first tranche also includes nondepository institutions that generated at least $10 billion in total receipts in either calendar year 2023 or 2024. Therefore, this issue affects multiple stakeholder groups.

[8] *See* https://www.courtlistener.com/docket/69302685/forcht-bank-na-v-consumer-financial-protection-bureau/.

enforce Dodd-Frank or its implementing regulations, although in the case of national banks and federal savings associations they are limited to enforcing rules prescribed by the Bureau.[9]

As the CFPB has already clearly stated its intention to rewrite the Section 1033 rule and undertaking the rule writing process, the Bureau must end this unnecessary compliance risk by indefinitely postponing all compliance dates until a new PFDR rule is finalized in the Federal Register.

Accordingly, ABA urges the CFPB to suspend the current compliance dates as soon as possible through a publication of an interim final rule in the Federal Register. Under the Administrative Procedure Act, the Bureau may forgo notice and comment if it finds good cause—an exception ABA believes is justified in this situation given the current uncertainty and the significant burden on institutions weighing investments in implementing a rule in the midst of substantial revision. This path would offer legal clarity while preserving the CFPB's flexibility to make further adjustments. Informal methods outside of the Administrative Procedure Act do not have the adequate force of law given the role of states in enforcement matters as noted above.

I. ABA recommendations for the re-proposed rule made in this comment

This letter makes a number of recommendations to the CFPB as it reconsiders the PFDR rule. We believe inclusion of these concepts would make the re-proposed rule far more effective than the November 2024 version, which would mean a better result for consumers, stakeholders in the data sharing ecosystem, as well as the regulatory agencies.

For convenience, we are listing the recommendations here in no particular order. They also appear below in the relevant context along with the supporting rationale. To be clear, many of the issues that the PFDR rule attempted to address through rulemaking have been, and continue to be, solved by the competitive private market. Bilateral agreements are the cornerstone of a secure and innovative data-sharing ecosystem. Unlike rigid, one-size-fits-all regulations, agreements empower banks and fintechs to negotiate terms that directly address consumer needs, privacy, and security. They enable all parties to invest in robust infrastructure, set higher performance standards, and ensure responsible data use, ultimately protecting consumers from unnecessary risks and data misuse. By fostering collaboration and accountability, bilateral agreements drive market-driven innovation and competition, creating a dynamic environment where consumers benefit from safer, more efficient financial services tailored to their preferences.

- The CFPB must limit itself to its narrow statutorily-prescribed duties and allow the market to continue solving for other aspects of data sharing.

- The CFPB must consult transparently and coordinate with the federal banking agencies and the Federal Trade Commission (FTC) as required on safeguarding data shared

[9] 12 USC 5552, https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title12-section5552&num=0&edition=prelim.

pursuant to the PFDR rule to ensure all attendant issues are addressed. This may include the prudential regulators issuing appropriate activity-specific guidance to aid supervised entities with meeting compliance expectations, as the general Interagency Guidance on Third-Party Relationships: Risk Management[10] does not adequately address the issues presented by consumer-permissioned data sharing. The FTC has a role with its Safeguards Rule,[11] and can issue guidance for entities that do not fall under CFPB supervisory authority.

- The CFPB must not restrict data providers' ability to conduct risk management activities before, during, and after sharing data pursuant to consumer consent, to include conducting appropriate due diligence on data aggregators and data recipients prior to establishing connections.

- The CFPB should adhere to the text of Section 1033 in determining its scope. A logical reading of the statute requires the person requesting the information from the data provider to have themselves obtained the financial product or service. Further, the CFPB must not ignore the "acting on behalf of" language. While the statutory scope of 1033 is narrow, the permissioned data sharing market in the US is robust and thriving, and has been in the absence of CFPB rulemaking. The CFPB should avoid inserting itself into this functioning market at the peril of impeding progress and growth.

- If the CFPB interprets the definition of consumer more broadly, it should qualify the entities in scope to those that are engaging in financial activity.

- Data aggregators and larger fintechs must be subject to ongoing supervision. This is imperative for entities operating in the consumer-permissioned data sharing ecosystem. Supervision is necessary, among other things, to ensure consumer privacy preferences are respected and information security requirements for the shared data are complied with. ABA recently submitted several comment letters regarding the importance of the larger participant supervisory program.[12]

- Consumers must have access rights to information about consumer financial products and services held by all "covered persons," which as the statute directs should include banks, credit unions, fintechs, and data aggregators (however, entities regulated by the Securities and Exchange Commission or the Commodity Futures Trading Commission should be expressly excluded from the PFDR rule given the CFPB's lack of jurisdiction over them per plain language—see footnote 27). Further, any sharing of data must be expressly

[10] https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management.
[11] https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314.
[12] *See* https://www.aba.com/advocacy/policy-analysis/cfpb-letter-defining-larger-participants-international-money-transfer; https://www.aba.com/advocacy/policy-analysis/cfpb-letter-defining-larger-participants-consumer-reporting; https://www.aba.com/advocacy/policy-analysis/cfpb-letter-defining-larger-participants-auto-finance; https://www.aba.com/advocacy/policy-analysis/cfpb-letter-defining-larger-participants-consumer-debt-collection.

tied to the consent of the consumer and respecting the information security interests of the original data provider. Data aggregators or data recipients should not be permitted to re-share permissioned data; rather, it must be obtained from the original data provider pursuant to explicit consumer authorization (for example, by requiring the consumer authenticate identity directly with the data provider for each authorization). This is the only way to ensure appropriate degrees of protection for the data, in addition to ensuring the flow of liability corresponds with the data movement.

- Within a narrow, statutorily-bound rule, the CFPB must distribute obligations based on function versus form. To start, it should be clear that any entity offering financial products and services to consumers are data providers under the rule. Also, the confusing terminology of "third party" should be replaced with the more descriptive "data recipient." Further, the rule must impose substantially similar requirements on all covered persons. As things currently stand, the requirements in the November 2024 PFDR rule are too focused on data provider obligations; which, as written, will disproportionately impact banks as supervised entities. Instead, the regulation should be reworked emphasizing the obligations of data aggregators and data recipients to ensure:

  (1) consumer data is used for limited consumer-authorized purposes;
  (2) the data remains secure and protected; and
  (3) failure to meet these obligations will result in liability of the breaching party.

- Payment initiation information should be out of scope of the re-proposed PFDR rule.

- Pending or authorized status transaction information and upcoming bill information should be out of scope of the re-proposed PFDR rule.

- Rewards data should be out of scope of the re-proposed PFDR rule.

- The re-proposed rule must allow for a free and fair market by being silent on the question of fees—as is the 1033 statute.

- Screen scraping must be sunset and specifically designated as an Unfair, Deceptive, or Abusive Act or Practice (UDAAP) violation. To ensure compliance with the prohibition, data providers must be able to block screen scraping without fear of reprisal. The re-proposed rule must include clear timelines when the prohibition of screen scraping goes into effect, which could also serve as the compliance dates.

- The CFPB should remove the exemption for community banks and credit unions with assets of $850 million and less.[13] While we understand the noble motivation behind carving out small entities, according to the CFPB's own data it leaves over 74% of community banks and over 89% of credit unions out of the rule's reach for data

[13] *Supra*, note 3 at 12 CFR 1033.111(d), https://www.ecfr.gov/current/title-12/chapter-X/part-1033/subpart-A/section-1033.111.

providers[14] and will have the effect of perpetuating screen scraping, injecting additional risk into the ecosystem, creating inconsistent consumer experiences (and protections), and harming the competitiveness of community banks in an increasingly digital world. Allowing data providers to charge fees will alleviate the removal of the exemption for smaller depository institutions.

- To the extent any re-proposed rule regulates data sharing throughout the ecosystem it should include a clear liability framework requiring a responsible party to notify others of potential data breaches or unauthorized activities, with a methodology for restitution. Given the prudential agencies' and the FTC's responsibilities on safeguarding, the Bureau must coordinate with them in this matter. The re-proposed rule should establish safe harbor provisions and a clear liability framework. The principles underpinning this liability regime should be:

  (1) data providers are afforded a safe harbor when data misuse occurs downstream;
  (2) liability follows the data, with third party recipients liable for fraud, data breaches, or other misuse due to their own activities and data handling;
  (3) data providers should retain discretion to require liability and indemnification terms as a condition for access; and
  (4) data aggregators and data recipients should be required to certify that they are adequately capitalized and carry indemnity insurance to support their liability obligations.

- The CFPB should retain the general prohibition on secondary uses in its re-proposed PFDR rule, but should add examples of permissible and forbidden behavior under this framework, the latter of which must include "reverse engineering."

- Express informed consent is the appropriate principle governing activities using consumer-permissioned data. A model form should be included, use of which would provide a safe harbor.

- For purposes of the "keeping consumer informed" request, CFPB should amend the requirement to the "categories" of third parties rather than the specific "names."

- The number of provisions contemplated for industry standard-setting bodies must be limited. Only a format concerning standardized formats (i.e., API specs) would be of utility (incidentally, it is the only area that currently has a recognized industry standard setter—the Financial Data Exchange[15]). Moreover, the deference to the standardized

[14] https://www.federalregister.gov/documents/2024/11/18/2024-25079/required-rulemaking-on-personal-financial-data-rights; *see* Table 1.

[15] *See* https://www.consumerfinance.gov/personal-financial-data-rights/applications-for-open-banking-standard-setter-recognition/. Only one other application was posted for public comment—the Digital Governance Standards Institute. The CFPB took no action on this application, although it is noteworthy that ABA opposed recognition; *see* https://www.aba.com/en/advocacy/policy-analysis/letter-digital-governance-standards-institute-application.

format standard must be strengthened to a safe harbor instead of the ambiguous "indicia of compliance."

- The CFPB must suspend the current compliance dates immediately via publication of an interim final rule. The re-proposed PFDR rule must set a period of 2 years from the issuance of consensus standards for data formats.

II. Understanding the context of the PFDR rule is pivotal

A. Regulation as distinguished from the market

The entire consumer-permissioned data sharing ecosystem as it exists today in the United States is a product of the market. Every connection, every use case, every control has come into being well before the CFPB even commenced rulemaking with its 2020 ANPR, never mind compliance dates under the November 2024 PFDR rule.

A functional regulation sets the floor; anything implemented beyond that baseline is the result of an informed business decision that allows for competitive differentiation. Simply because something is not mandated does not mean it will cease to exist; instead, the market will solve for appropriate availability and terms. Consumer demand and competitive pressures would work far better than governmental directives in fulfilling the promise of permissioned data sharing in the United States—indeed, over 100 million consumer accounts are already safely sharing data through application programming interfaces following the Financial Data Exchange[16] (FDX) standard.[17] We must not confuse regulation, which concerns what banks are *required* to do, with the free market, which pertains to what businesses *choose* to do to meet consumer demand. This letter lays out our members' positions on regulatory compliance matters—not the market.

RECOMMENDATION: The CFPB must limit itself to its narrow statutorily-prescribed duties and allow the market to continue solving for other aspects of data sharing.

B. The 1033 statute predates the data sharing ecosystem and requires the CFPB to consult other regulators

As the CFPB has noted, the "statutory text of section 1033 is quite sparse and does not specifically address several important questions that arise from the rights it creates."[18] Indeed,

[16] https://www.financialdataexchange.org/.
[17] https://www.financialdataexchange.org/FDX/News/Press-Releases/114%20Million%20Reasons%20to%20Keep%20Moving%20Forward%20on%20Industry-Led%20Standard%20for%20Secure%20Data%20Sharing.aspx.
[18] *Supra,* note 2.

the entire law is brief enough to cite in its entirety in a footnote without taking up an undue amount of space.[19]

The consumer-permissioned data sharing ecosystem as it exists today (with a multitude of fintechs connecting with data providers by way of intermediary data aggregators) only came into existence after the passage of the Dodd-Frank Act in 2010. Accordingly, any regulation that attempts to retrofit the market into something that it was never intended to govern, will pick winners and losers in a manner that is both unfair and unlawful. If the CFPB exceeds its authority, it will in fact stifle innovation and increase risk to consumers. Conversely, the narrower approach the CFPB takes in its rulemaking, the less questions it will have to resolve because those issues will be addressed by the market.

There will be an inherent and enduring tension between any PFDR rule that demands sharing personal information and prudential expectations for banks to safeguard it. Indeed, the drafters recognized this and prescribed consultation between the CFPB and the Federal banking agencies

---

[19] **Consumer rights to access information**
(a) In general
Subject to rules prescribed by the Bureau, 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, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data. The information shall be made available in an electronic form usable by consumers.
(b) Exceptions
A covered person may not be required by this section to make available to the consumer-
(1) any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors;
(2) any information collected by the covered person for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct;
(3) any information required to be kept confidential by any other provision of law; or
(4) any information that the covered person cannot retrieve in the ordinary course of its business with respect to that information.
(c) No duty to maintain records
Nothing in this section shall be construed to impose any duty on a covered person to maintain or keep any information about a consumer.
(d) Standardized formats for data
The Bureau, by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers under this section.
(e) Consultation
The Bureau shall, when prescribing any rule under this section, consult with the Federal banking agencies and the Federal Trade Commission to ensure, to the extent appropriate, that the rules-
(1) impose substantively similar requirements on covered persons;
(2) take into account conditions under which covered persons do business both in the United States and in other countries; and
(3) do not require or promote the use of any particular technology in order to develop systems for compliance. [12 USC 5533, https://uscode.house.gov/view.xhtml?req=(title:12%20section:5533%20edition:prelim)%20OR%20(granuleid:USC-prelim-title12-section5533)&f=treesort&edition=prelim&num=0&jumpTo=true].

as well as the FTC prior to issuing any re-proposed rule.[20] The CFPB should engage in such consultation in a transparent manner so that stakeholders can be satisfied on this front.

Furthermore, the prudential agencies might consider issuing appropriate activity-specific guidance given the unique questions consumer-permissioned data sharing presents that will remain true whether such activities occur due to market forces or regulatory compliance.

RECOMMENDATION: The CFPB must consult transparently and coordinate with the federal banking agencies and the FTC as required on safeguarding data shared pursuant to the PFDR rule to ensure all attendant issues are addressed. This may include the prudential regulators issuing appropriate activity-specific guidance to aid supervised entities with meeting compliance expectations, as the general Interagency Guidance on Third-Party Relationships: Risk Management[21] does not adequately address the issues presented by consumer-permissioned data sharing. The FTC has a role with its Safeguards Rule,[22] and can issue guidance for entities that do not fall under CFPB supervisory authority.

RECOMMENDATION: The CFPB must not restrict data providers' ability to conduct risk management activities before, during, and after sharing data pursuant to consumer consent, to include conducting appropriate due diligence on data aggregators and data recipients prior to establishing connections.

III. The Scope of the PFDR rule should be governed by the statute

A. The meaning of "consumer" in Section 1033 is narrow

A central question of the *Forcht Bank* litigation that has not yet been resolved and is featured prominently in the ANPR is the meaning of "consumer" in the context of the 1033 statute. The entirety of the statute, cited in footnote 19, discusses only "consumer" and does not go into detail on the nuances of the wider data sharing ecosystem. Indeed, the text reads as too simple to possibly contemplate the massive issues native to such activity. While online banking for consumer accounts and availability of electronic information are ubiquitous today, in 2010 they were not. Fintechs or data aggregators did not exist at scale, and the term "open banking" is not a concept found in the statutory text or Congressional record because it only developed a few years after the enactment of Dodd-Frank. Similarly, novel applications of technology such as agentic AI acting on behalf of consumers were certainly not considered by lawmakers as those are very recent developments.

Importantly, if the CFPB scales back the definition of "consumer" ecosystem, limiting "consumer" to its proper scope will not halt the thriving data-sharing ecosystem; consumer demand and market competition will ensure its continued growth and momentum. It is simply a question of what conduct the Bureau can and cannot mandate under the color of law.

[20] *Id.* at 12 USC 5533(e).
[21] *Supra*, note 10.
[22] *Supra*, note 11.

Another section of Dodd-Frank defines "consumer" as meaning "an individual or an agent, trustee, or representative acting on behalf of an individual."[23] However, within Section 1033, "consumer" must be narrowly read based on a logical reading of the plain text of the statute. Section 1033(a) only requires that covered persons make available data "concerning the consumer financial product or service that the consumer obtained from" the covered person, and "the consumer" must refer to the actual individual who did, in fact, obtain such product or service (this could conceivably encompass agents, trustees, and representatives acting on behalf of the consumer such as conservators, executors, guardians, and similar roles). Data aggregators and data recipients are not seeking information about the products or services *they* obtained from the data provider, but rather those of a consumer held in common with the data provider.

Additionally, Section 1033(a) mandates that covered persons must make certain data "available in an electronic form usable by consumers." Section 1033(d) then states that the Bureau must prescribe standardized formats for this data. The most logical reading of these provisions is that "usable by consumers" refers to the data formats banks employ to provide individuals with their own data for their own use. This points to data format standards such as CSV and PDF, which are useful for individual consumers to get financial data in the same format from all of their banks. Nothing in Section 1033 suggests that Congress contemplated APIs and data transmission to third parties in addition to the individual consumer. Additionally, the legislative history for Section 1033 confirms that it is meant to cover data requests from individuals only.[24]

Even if the general definition of "consumer" in Dodd-Frank (inclusive of agents, trustees, and representatives acting on behalf of) were to apply to Section 1033, fintechs and data aggregators cannot qualify given their relationships to consumers. It seems unlikely (and it would be disingenuous) for data aggregators or fintechs to hold themselves out as agents or trustees. In any case, legal precedent supports the argument that data aggregators do not qualify as agents, trustees, or otherwise play a fiduciary role under Section 1033. The roles of agent and trustee require relationships of trust, loyalty, and control, which data aggregators and data recipients typically lack. At common law, the fiduciary obligations of "agents" and "trustees" arise only in relationships marked by extraordinary trust and a duty of loyalty to the principal. See, e.g., Restatement (Third) of Agency § 1.01 (2006); Restatement (Third) of Trusts § 2 (2003). In *Varity Corp. v. Howe*, the Supreme Court emphasized that fiduciaries, including trustees, must act "solely in the interest of the participants and beneficiaries" and owe an unwavering duty of loyalty to their beneficiaries. 516 U.S. 489 (1996). Similarly, in *NLRB v. Amax Coal Co*., the Supreme Court explained that trustees of employee benefit funds must act with "complete loyalty to the beneficiary of the trust, to the exclusion of the interests of all other parties." 453 U.S. 322 (1981).

---

[23] 12 USC 5481(4), https://uscode.house.gov/view.xhtml?req=(title:12%20section:5481%20edition:prelim)%20OR%20(granuleid:USC-prelim-title12-section5481)&f=treesort&edition=prelim&num=0&jumpTo=true.

[24] *See, e.g.*, S. Rep. No. 111-176, at 173 (2010) (Section 1033 "ensures that consumers are provided with access to their own financial information. This section requires the Bureau to prescribe rules requiring a covered person to make available to consumers information concerning their purchase and possession of a consumer financial product or service, including costs, charges, and usage data.").

Third-party data aggregators generally do not meet the criteria for agents, trustees, or fiduciaries because their relationships with individuals lack the hallmarks of fiduciary duties. For instance, in *Wanna v. RELX Group, PLC*, the Eighth Circuit found that an information broker lacked actual or apparent authority to act as an agent for a data provider, as their relationship was limited to arm's-length transactions without fiduciary obligations. 142 F.4th 1102, 1106 (2025).

Because data aggregators and data recipients cannot be agents or trustees, the outcome would hinge on them operating in the capacity of "representative acting on behalf of an individual." Following the Supreme Court's *Loper Bright Enterprises v. Raimondo*, 144 S. Ct. 2244 (2024) decision, the CFPB is not entitled to deference in interpreting the statutory terms "representative acting on behalf of [a consumer]."

Importantly, the term "representative" is accompanied by the additional qualifier of "acting on behalf of an individual." Certainly, this narrows the meaning of the phrase beyond mere authorization. Fintechs, data aggregators, and other data recipients are commercial entities engaged in business transactions with individuals that are governed by contractual obligations. They cannot reasonably be viewed as acting on behalf of or in the best interests of individual consumers. In *National Carbide Corp. v. C.I.R.*, the Supreme Court held that the mere transfer of profits or benefits to another party does not establish an agency relationship unless the agent is genuinely acting on behalf of the principal. 336 U.S. 422 (1949). Data aggregators (which in the vast majority of cases are the entities actually collecting personal information from the data provider) have even less of a claim here because they are intermediaries selected by fintechs and other data recipients, not the consumers themselves.

Given the misalignment of interests, fintechs, data aggregators, and other data recipients are not acting on behalf of consumers. Therefore, access to consumer financial data at scale by these third parties should occur via negotiated data access agreements that ensure the covered person providing the data can contractually require minimum data security and data privacy practices as a condition for getting access to consumer data.

Notwithstanding the above, if the CFPB nonetheless permits third-party access, it must be narrowly tailored:

(1) access should be limited to the specific data necessary to fulfill the consumer-authorized purpose;
(2) there must be clear and conspicuous disclosures detailing the scope, frequency, and duration and planned use of the data and any *n*th parties the data may be shared with in order to deliver the requested product or service; and
(3) secondary uses of the data by data aggregators and data recipients must remain prohibited.

Regardless of *who* can access the data, there must be a limitation based on *why*. Any rights pursuant to the PFDR rule must be restricted to consumer's use in obtaining consumer financial products and services only. The current rule, however, appears to require that a data provider make covered data available to third parties for almost any purpose, which creates significant

risks given the wide array of entities outside of the financial sector that could potentially request the data and are not subject to the same regulatory oversight.

RECOMMENDATION: The CFPB should adhere to the text of Section 1033 in determining its scope. A logical reading of the statute requires the person requesting the information from the data provider to have themselves obtained the financial product or service. Further, the CFPB must not ignore the "acting on behalf of" language. While the statutory scope of 1033 is narrow, the permissioned data sharing market in the US is robust and thriving, and has been in the absence of CFPB rulemaking. The CFPB should avoid inserting itself into this functioning market at the peril of impeding progress and growth.

RECOMMENDATION: If the CFPB interprets the definition of consumer more broadly, it should qualify the entities in scope to those that are engaging in financial activity.

B. Covered persons of all types should be subject to the rule's requirements

While sparse, the 1033 statute does require that any implementing regulations "impose substantively similar requirements on covered persons" to the extent appropriate.[25] Similarly, the right of access is applied to covered persons, not banks as a class.[26] A "covered person" is defined as:

> (A) any person that engages in offering or providing a consumer financial product or service; and
> (B) any affiliate of a person described in subparagraph (A) if such affiliate acts as a service provider to such person.[27]

Included in the definition of "financial product and services" is "[p]roviding financial data processing products or services by any technological means, including processing, storing, aggregating, or transmitting financial or banking data, alone or in connection with another product or service, where the financial data processing is not offered or provided by a person who, by operation of 12 U.S.C. 5481(15)(A)(vii)(I) or (II), is not a covered person."[28]

---

[25] *Supra*, note 19 at 12 USC 5533(e).
[26] *Id.* at 12 USC 5533(a).
[27] 12 USC 5481(6), https://uscode.house.gov/view.xhtml?req=(title:12%20section:5481%20edition:prelim)%20OR%20(granuleid:USC-prelim-title12-section5481)&f=treesort&edition=prelim&num=0&jumpTo=true.

However, the Bureau should note that, per plain language in the Dodd-Frank Act the "Bureau shall have no authority to exercise any power to enforce this title with respect to a person regulated by the [Securities and Exchange] Commission" or "the Commodity Futures Trading Commission. Therefore, these entities may not be "covered persons" under any PFDR rule. *See* 12 USC 5517(i) and 5517(j); https://uscode.house.gov/view.xhtml?hl=false&edition=prelim&req=granuleid%3AUSC-prelim-title12-section5517&f=treesort&num=0&saved=%7CKHRpdGxlOjEyIHNlY3Rpb246NTUxMyBlZGl0aW9uOnByZWxpbSkgT1IgKGdyYW51bGVpZDpVU0MtcHJlbGltLXRpdGxlMTItc2VjdGlvbjU1MTMp%7CdHJlZXNvcnQ%3D%7C%7C0%7Cfalse%7Cprelim.
[28] 12 CFR 1001.2(b), https://www.ecfr.gov/current/title-12/chapter-X/part-1001/section-1001.2.

Based on these sections, entities offering consumer financial products or services (including data aggregation) are covered persons and must be subject to the scope of the rule for data access to responsive information within their control or possession. When asked about this issue in a recent survey, 76% of respondents agreed that the "general requirement to share information should apply equally to every company or organization that holds consumer data."[29] Further, it is critical that these entities be subject to substantially similar requirements for privacy, information security, and risk management. Finally, to ensure appropriate protection and treatment of consumers' personal information, responsibilities for protecting consumers' data and the liability for any misuses or breaches of such data must flow with the receipt of such data and follow the transfer throughout the ecosystem.

A major flaw of the November 2024 PFDR rule is that it disproportionately imposed obligations on data providers, with very little affirmative obligations falling on the third parties. At the same time, it was insufficiently clear that fintechs are themselves data providers to the extent they offer covered financial products and services. Many of these entities wrongly viewed themselves purely as data recipients; education efforts and compliance materials provided by the CFPB and geared towards smaller fintechs could help in this regard.

Relevant to the above and as we have done previously on numerous occasions,[30] ABA urges the CFPB to commence larger participant rulemaking under 12 CFR Part 1090 to directly supervise data aggregators. The Bureau should also create a supervisory framework for larger participants in the fintech nonbank space to ensure regulatory parity. This is crucial given the massive presence of data aggregators and fintechs in the consumer-permissioned data sharing ecosystem.

Equivalent levels of supervision are especially important given the amount of sensitive personal information that aggregators handle. Without effective oversight, it becomes impossible to ensure the data is adequately safeguarded, and that it is not reverse engineered or used to train the aggregators' proprietary products, or otherwise impermissibly shared or misused.

RECOMMENDATION: Data aggregators and larger fintechs must be subject to ongoing supervision. This is imperative for entities operating in the consumer-permissioned data sharing ecosystem. Supervision is necessary, among other things, to ensure consumer privacy preferences are respected and information security requirements for the shared data are complied with. ABA recently submitted several comment letters regarding the importance of the larger participant supervisory program.[31]

---

[29] *Morning Consult*, National Tracking Poll #2509133, conducted October 01-06, 2025 at Question ABA5a_4.
[30] *See* American Bankers Association, et al., Joint Trades' Petition for Rulemaking Defining Larger Participants of the Aggregation Services Market (Aug. 2, 2022), https://www.regulations.gov/document/CFPB-2022-0053-0001; *see also* American Bankers Association, Response to Outline of Proposals and Alternatives Under Consideration for Required Rulemaking on Personal Financial Data Rights, https://www.aba.com/advocacy/policy-analysis/letter-to-cfpb-on-data-sharing-rules; *see also* American Bankers Association, Response to Request for Comment on Proposed Rule for Personal Financial Data Rights, https://www.aba.com/en/advocacy/policy-analysis/letter-to-the-cfpb-on-proposed-rule-for-personal-financial-data-rights.
[31] *Supra*, note 12.

RECOMMENDATION: Consumers must have access rights to information about consumer financial products and services held by all "covered persons," which as the statute directs should include banks, credit unions, fintechs, and data aggregators (however, entities regulated by the Securities and Exchange Commission or the Commodity Futures Trading Commission should be expressly excluded from the PFDR rule given the CFPB's lack of jurisdiction over them per plain language—see footnote 27). Further, any sharing of data must be expressly tied to the consent of the consumer and respecting the information security interests of the original data provider. Data aggregators or data recipients should not be permitted to re-share permissioned data; rather, it must be obtained from the original data provider pursuant to explicit consumer authorization (for example, by requiring the consumer authenticate identity directly with the data provider for each authorization). This is the only way to ensure appropriate degrees of protection for the data, in addition to ensuring the flow of liability corresponds with the data movement.

RECOMMENDATION: Within a narrow, statutorily-bound rule, the CFPB must distribute obligations based on function versus form. To start, it should be clear that any entity offering financial products and services to consumers are data providers under the rule. Also, the confusing terminology of "third party" should be replaced with the more descriptive "data recipient." Further, the rule must impose substantially similar requirements on all covered persons. As things currently stand, the requirements in the November 2024 PFDR rule are too focused on data provider obligations; which, as written, will disproportionately impact banks as supervised entities. Instead, the regulation should be reworked emphasizing the obligations of data aggregators and data recipients to ensure:

(1) consumer data is used for limited consumer-authorized purposes;
(2) the data remains secure and protected; and
(3) failure to meet these obligations will result in liability of the breaching party.

C. Payment initiation information should be out of scope and pay-by-bank should be market-driven

Pay-by-bank is a use case that is being evaluated by the market (for more information on pay-by-bank, please see footnote 4). However, as explained above in Section II(A), there is a vast divide between the market meeting a demand versus the government mandating an outcome. Any data field required to be shared must be rooted in the statutory language.

The 1033 statute only references information in the control or possession of the covered person concerning the consumer financial product or service that the consumer **obtained** [emphasis added]."[32] The plain meaning of "obtained," its use as a past participle indicating completed actions, and statutory interpretation principles collectively support the argument that the Section 1033 statute limits the CFPB's authority with regard to retrospective data. Courts have consistently emphasized the importance of adhering to the plain meaning of statutory language unless ambiguity exists. In *Argus Leader Media v. U.S. Dep't of Agric*., 740 F.3d 1172 (2014), the Eighth Circuit concluded the term "obtained" refers specifically to information already

[32] *Supra*, note 19 at 12 USC 5533(a).

acquired, not information that could be acquired. The court stated, "When the statute says 'obtained' it means 'obtained,' not 'can be obtained.'" *Id*. at 1176. Argus underscores the retrospective nature of the term, focusing on completed actions rather than future possibilities. Similarly, in *Drapich v. Donovan*, the Ninth Circuit rejected an expansive definition of "obtained" that would include future acquisitions or processes. 693 F.2d 1296, 1299 (9th Cir. 1982). The court adopted a narrower interpretation, equating "obtained" with "purchased" and emphasizing its compatibility with congressional intent. *Id*. *Drapich* thus supports the argument that "obtained" in Section 1033 should be understood as referring to past transactions or data already in possession.

The distinction between past and present tense in statutory language further supports the retrospective interpretation of "obtained." In *FlightSafety Def. Corp. v. United States*, the Court of Federal Claims analyzed the term "obtained" as a past participle, indicating a completed action. 173 Fed. Cl. 699 (2024)). The court noted that "the past participle indicates a completed action" and contrasted it with the present tense "obtain," which implies active effort to acquire something. *Id*. at 710.

Similarly, information that has not yet occurred is out of scope of any PFDR rule. This includes, among others, "information to initiate payment to or from a Regulation E account"[33] because the payment initiation is future-oriented activity. Section 1033 was created as a way for consumers to "access information," not to mandate specific functionality. Indeed, the CFPB should carefully reconsider the covered data definition in the November 2024 PFDR rule and ensure banks and other covered persons are not compelled to make any data available to third parties unless it is expressly authorized by the statute. For example, "credit limits" are not "information relating to any transaction, series of transactions," or the "costs, charges and usage data."[34]

Different use cases in data sharing have varying degrees of risk, but data sharing does not carry as much risk as money movement. Pay-by-bank has not, to date, solved for risk or liability. While ABA has long argued that liability should flow with the data[35] and former Director Chopra stated he endorsed this view,[36] the November 2024 PFDR rule did not address liability at all, nor did it touch on important issues regarding the application of Regulation E to third parties.

In its re-proposal the CFPB must strike those portions of the regulation that could facilitate the initiation of payments, such as the requirement to provide the data field "information to initiate payment to or from a Regulation E account."[37] That is not to say pay-by-bank will not occur in

---

[33] *Supra,* note 3 at 12 CFR 1033.211(c), https://www.ecfr.gov/current/title-12/chapter-X/part-1033/subpart-B/section-1033.211.
[34] *Id*. at 12 CFR 1033.211; *Supra*, note 19 at 12 USC 5533(a).
[35] *See* American Bankers Association, Response to ANPR of Proposed Rulemaking Regarding Consumer Access to Financial Records, https://www.aba.com/advocacy/policy-analysis/cfpb-anpr-consumer-access-to-financial-records.
[36] Testimony of Rohit Chopra, House Financial Services on CFPB Semi-Annual Report to Congress, November 29, 2023 ("We're trying to figure out under which of our statutes can we make sure absolutely clear that it's the receiving institution that really bears, you know, is responsible for handling that data").
[37] *Supra,* note 3 at 12 CFR 1033.211(c), https://www.ecfr.gov/current/title-12/chapter-X/part-1033/subpart-B/section-1033.211.

an environment tailored to market demand and featuring all due risk mitigants, only that the CFPB should not put its proverbial finger on the scale. It is possible a mitigant the market will adopt will be a larger role for tokenized account numbers (TANs). Stakeholders are currently working to create a network for warranties and dispute resolution. As things currently stand, the consumer protection regimes and operating standards in place for more established payment networks (such as debit and credit cards) are not yet there for pay-by-bank. Thus, the impact will not only be on businesses but their customers as well.

It is no accident that companies focusing on crypto and agentic artificial intelligence have suddenly joined the fray.[38] The purveyors of these innovative technologies wish to piggyback on the November 2024 PFDR rule's payments provisions.

However, this confluence is fraught with peril. For example, agentic AI could exacerbate existing problems with disputes around money movement (think of all the points of failure when consumers deputize an AI agent to consummate a deal on the condition that the price for an item reaches X dollars—what if the consumer alleges an error with the authorization, or the purchase itself, etc.). Similarly, the rules of the road for blockchain transactions (such as payment stablecoins) have not yet been written (rulemaking required by the GENIUS Act is currently a live exercise).

Even now, an established fintech is working to incorporate agentic AI into payments, noting that "agents are going to be buying and paying on our behalf."[39] This is all the more reason for the CFPB to avoid all references to payments initiation information in its re-proposed rule and allow the market to solve for these issues.

RECOMMENDATION: Payment initiation information should be out of scope of the re-proposed PFDR rule.

D. Pending or authorized status and upcoming bill information should be out of scope

Based on the above rationale regarding the meaning of "obtained," "pending or authorized status" transaction information and "upcoming bill information[40] should also be struck from the re-proposed rule, as they are future activities and accordingly beyond the reach of Section 1033.

RECOMMENDATION: Pending or authorized status transaction information and upcoming bill information should be out of scope of the re-proposed PFDR rule.

---

[38] *See* https://www.ftassociation.org/fintech-crypto-main-street-business-trades-urge-president-trump-to-uphold-open-banking-rule-amid-anti-competitive-moves-from-nations-largest-banks/; *see also* https://www.ftassociation.org/business-leaders-urge-president-trump-to-oppose-exorbitant-consumer-data-access-fees/.

[39] John Adams, "Inside Stripe's push into agentic artificial intelligence," *American Banker*, https://www.americanbanker.com/payments/news/stripe-adds-agentic-ai-tools-for-payments-stablecoins.

[40] *Supra,* note 3 at 12 CFR 1033.211(a) https://www.ecfr.gov/current/title-12/chapter-X/part-1033/subpart-B/section-1033.211.

E. Rewards data should be out of scope

Sharing rewards and rewards program data[41] is problematic as it may be commercially sensitive and/or encroach on the rights of third-party merchants/partners that share rewards data with a data provider. Further, sharing of this data may also put data providers in breach of preexisting contractual obligations with these third parties where sharing is impermissible. Such shared data should not be in scope of the re-proposed PFDR rule. Rewards program information is "confidential commercial information" and must be recognized as such.[42]

RECOMMENDATION: Rewards data should be out of scope of the re-proposed PFDR rule.

IV. Access fees are permissible under the statute, which the rule must reflect

As a threshold matter, the costs data providers incur to enable data access under a revised 1033 rule will depend greatly on how the CFPB defines "consumer." If the CFPB defines "consumer" narrowly, the status quo will likely persist with consumers enjoying free access to their own financial data, whereas fintechs and data aggregators will obtain access to such data via negotiated data access agreements.

Regardless, ABA strongly supports the ability for data providers to charge a fee given the service they are affording to data aggregators and data recipients. Despite what is alleged, it is not the data itself that is being charged for but rather developing and maintaining a costly system for access, refinement, monitoring, updates, and safeguarding of the data. Those who will use the API are not the consumers, but other companies who will provide a product/service based on the data they ingest, so it is reasonable they pay market value for such access.

There is a reason fintechs find bank data so valuable when they could easily obtain it from the consumer directly—data providers have already conducted the data hygiene, data lineage, and compliance work for them. In addition, the data is presented in a certain format that minimizes the amount of refinement the data recipient must do. This represents a convenience, and paying for convenience is well established in the market for a variety of products and services (e.g., using out-of-network ATMs, buying airfare via telephone, purchasing movie tickets online).

If Congress had intended for information under Section 1033 to be made without the ability to charge fees, it would have said so expressly. Congress makes clear when it wishes to forbid providers from imposing fees. See, e.g., 15 USC. 1681c-1(a)(2)(B) (Fair Credit Reporting Act requirement that consumer reporting agencies must provide to consumers all required disclosures "without charge to the consumer"). Compellingly, this practice is reflected elsewhere in Dodd-Frank. See *id*. at 1691(e)(4) (Creditors shall provide copies of written appraisals or valuations "at

[41] *Supra,* note 3 at 12 CFR 1033.211(a) and (d), https://www.ecfr.gov/current/title-12/chapter-X/part-1033/subpart-B/section-1033.211.
[42] *Id*. at 12 CFR 1033.221(a) and 12 CFR 1033.221(e), https://www.ecfr.gov/current/title-12/chapter-X/part-1033/subpart-B/section-1033.221.

no additional cost to the applicant."). Similarly, Dodd-Frank requires creditors to provide a copy of certain appraisals "without charge." *Id*. at 1639h(c).

However, the 1033 statute does not explicitly address fees, nor does its text imply that fees are impermissible. Notwithstanding the lack of Congressional delegation, the November 2024 PFDR rule prohibited fees:

> "[a] data provider must not impose any fees or charges on a consumer or an authorized third party in connection with: (1)…[e]stablishing or maintaining the interfaces required by paragraph (a) of this section; or (2)…[r]eceiving requests or making available covered data in response to requests as required by this part").[43]

This action was taken despite the strong evidence that Section 1033 does not prohibit fees. See, e.g., *W. Va. Univ. Hosps. v. Casey*, 499 U.S. 83, 87-88 (1991) (omission of "expert fees" from a provision authorizing recovery of "attorney's fees," where other statutes the same Congress had enacted addressed those categories separately, rendered expert fees unavailable).

Even more so, after *Loper Bright*, the delegation of authority in Section 1033 does not include the authority to prohibit charging fees. Section 1033 delegates rulemaking authority only with respect to subjects addressed in the statute itself. For example, the Bureau may clarify what qualifies as "confidential commercial information"[44] or specify the format in which data must be made available.[45] But that grant of authority is limited: it does not give the Bureau license to regulate matters outside the statute, such as setting fee restrictions that Congress never addressed.

The fee prohibition in the November 2024 PFDR rule, which only applies to data providers, is unlawful and ignores the very real costs associated with building and maintaining the developer interfaces required by the PFDR rule, which were severely underestimated in the CFPB's analysis. Consumers understand the inherent unfairness of this situation. In a recent survey, 70% of respondents agreed that "since data recipients and data aggregators are monetizing the data obtained from banks, they should be expected to share in the operating costs."[46]

Moreover, the APIs *create* value that is used for profit by entities in the chain. In essence, the November 2024 PFDR rule compels data providers under penalty of noncompliance to subsidize the business models of data aggregators and third parties seeking to monetize the information. It represents nothing less than a forced transfer of value imposed by the federal government, which is especially egregious given the fact that aggregators charge fintechs and other clients for access to consumer financial data and related services. These charges—which include both fixed and variable costs —underscore a critical asymmetry in the regulatory framework in that aggregators

---

[43] *Supra*, note 3 at 12 CFR 1033.301(c), https://www.ecfr.gov/current/title-12/chapter-X/part-1033/subpart-C/section-1033.301.
[44] *Id*. at 12 USC 5533(b).
[45] *Id*. at 12 USC 5533(d).
[46] *Morning Consult* at Question ABA5a_1; *supra*, note 29.

are monetizing data that originates from financial institutions yet face no similar regulatory constraints on the fees they may impose.

Fees are necessary to create an environment supporting rational behavior. For example, a transaction-based price sheet (like that used by the Social Security Administration for its Electronic Consent-Based SSN Verification Service, also known as the eCBSV, or the FTC's Do Not Call Registry) illustrates the sound policy of using scaling costs to induce reasonable access frequency. In other words, the ability to charge fees results in a more satisfactory outcome. Permitting data providers to treat the APIs like the services they are, and charge accordingly will ultimately result in superior performance while ensuring sensitive consumer personal information is adequately safeguarded. Fees can also offset the costs of fraud, which includes not only conducting investigations but also ongoing authentication protocols.

The vast majority of data providers will be reliant on third-party service providers (such as core processors) to stand up and maintain their API. Given this model, more connections and a greater number of API calls would result in more costs for data providers.

Upfront costs for data providers can vary dramatically. There are manifold cost centers that must be accounted for, either by the data provider itself or on the data provider's behalf by the selected third-party service provider. These include:

(1) technology costs- e.g., API architecture, software development and updates, screen scraping monitoring tools;
(2) cybersecurity costs- e.g., defensive and offensive tools to fend off bad actors or vulnerabilities;
(3) fraud costs- e.g., to verify consumer identity or due to unauthorized activity, particularly with payment use cases;
(4) operational costs- e.g., the cost of maintaining the system and the attendant workstreams, including the compliance function;
(5) third-party risk management costs- e.g., due diligence of those seeking direct connections to the API in addition to downstream parties; and
(6) other costs- e.g., investigation costs for customer complaints made to the bank but caused by the data recipient (or upstream/downstream parties). Payment use cases significantly elevate the inherent risk and necessitate additional parties in the chain.

Additionally, data providers must hire and train staff, build workflows, implement policies and procedures, and so on. Costs may fluctuate based on numerous factors, and providing access to additional data aggregators beyond the largest handful, or direct connections to certain data recipients, could increase cost exposure.

API call volume also impacts the fees—in the current state of the market, these costs can accrue rapidly and quickly become prohibitive. Monthly subscription-style pricing models are common and it is difficult to forecast how things will scale. Members have reported the volume of APIs doubling on a monthly basis in recent times compared to 2023, 90% of instances in which the consumer is not explicitly requesting the information. According to an ABA analysis of Juniper Research's Global Open Banking APIs Market: 2025 – 2029 dataset, API call volume ranged

from 1.3 billion pings to 1.5 billion pings in 2024. By 2029, call volume is projected to grow to 15.1 billion pings.[47] Instantaneous and continuous access to data by third-party companies is costly and supporting such access would be expensive and could greatly impact the cost of providing APIs. A tiered fee structure, like that found in the eCBSV, helps to shape sustainable conduct.

RECOMMENDATION: The re-proposed rule must allow for a free and fair market by being silent on the question of fees—as is the 1033 statute.

V. As written, the rule creates significant information security risks

Perhaps the most disappointing aspect of the November 2024 PFDR rule is its failure to end the scourge of screen scraping. This is despite the preamble acknowledging its inherent dangers to consumer privacy and financial institutions' information security programs.[48] Screen scraping significantly raises the specter of fraud and significantly heightens risks of consumer harm. The primary objective of any PFDR rule should be to banish screen scraping.[49]

Left to their own devices, data aggregators and many fintechs (which are not subject to prudential supervision under Title V of the Gramm-Leach-Bliley Act,[50] or GLBA, instead falling under the enforcement authority of the FTC's Safeguards Rule[51]) will never halt screen scraping entirely as long as it is permissible. The largest data aggregator by volume admitted that at least 20% of its traffic is screen scraped, and suggested it will persist until APIs access is universal.[52] However, even when APIs are available data aggregators often endeavor to include screen scraping as a fallback option in data access agreements. The CFPB's re-proposed rule must sunset the practice of screen scraping across the entire ecosystem by placing affirmative obligations on all covered persons, including data aggregators.

While sunsetting screen scraping may impose a burden on data aggregators and data recipients, they are the right parties to bear the costs because they are the entities *choosing* to offer financial

---

[47] ABA analysis of Global Open Banking APIs Market: 2025-2029 data provided by Juniper Research. Juniper Research reports API data across seven segments: payments, underwriting, account aggregation and personal finance management, investments, lending, identity, and mortgages. The total number of open banking-related API calls per year was calculated using the number of users at year-end and the average number of consumer open banking API calls per year. Juniper Research also reports its own total number of open banking API calls per year; this value and the ABA-calculated value represent the low and high ends of the estimate range.

[48] *Supra*, note 14.

[49] As a great (to the 100th or so generation) grandson of Cato the Elder might say, "screen scraping *delenda est* [must be destroyed]."

[50] 15 USC 6805, https://uscode.house.gov/view.xhtml?req=(title:15%20section:6805%20edition:prelim)%20OR%20(granuleid:USC-prelim-title15-section6805)&f=treesort&edition=prelim&num=0&jumpTo=true.

[51] https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314.

[52] Penny Crosman, "JPMorganChase reaches deal to charge Plaid for customer data," *American Banker*, https://www.americanbanker.com/news/jpmorganchase-reaches-deal-to-charge-plaid-for-customer-data.

products and services to consumers and accordingly should be expected to cover their own operating expenses as well as pay for services rendered.

The dangerous practice of screen scraping is anathema to the financial sector's information security as well as consumer privacy. Consumers deserve a system that protects their sensitive log-in credentials and limits disclosure of their personal information to what they authorize. In the absence of an outright ban, data providers' significant investments in APIs will be for naught. Moreover, mere availability of APIs will not cause screen scraping to wither on the vine as the treasure trove of data for little effort is too much of a carrot for data aggregators to ignore.

A return to screen scraping would be especially risky for consumers given the advance of AI. As touched on above in Section III(C), this technology has the potential to take screen scraping to a new and concerning level of sophistication. For example, the advent of third-party AI agents that have the capability to log into consumer accounts as if they were that consumer and have the ability to take actions on that account dramatically increases the likelihood of risks already present in screen scraping. A future where undetectable AI agents are used widely and cannot be trusted to act as intended would create a new and significant threat to consumers. AI accessing consumer financial data demands significant governance and oversight to be enabled thoughtfully and in the best interests of consumers. A banking system that is compelled to open consumer financial accounts to unsupervised AI agents is less secure.

Whether or not the CFPB prohibits screen scraping, data providers must be able to block screen scraping without fear of reprisal. If there is a functional developer interface in place that shares data pursuant to consumer consent (with appropriate exceptions in place), screen scraping should be prohibited with blacklisting of entities engaging in the activity permissible. This should be true even for product types and markets not covered by the PFDR rule. Such an outcome would be consistent with text in the November 2024 PFDR's preamble,[53] although a place in the regulatory text itself would render it far more impactful.

Liability for continuing to screen scrape should fall on data aggregators or those data recipients with direct connections. A legal basis for such a ban would be tying it to the information security requirements of the GLBA,[54] as data sharing via screen scraping is inherently unsafe and dangerous to privacy/security. Any entity engaging in screen scraping at this late stage, despite knowing the risks to information and security, has amply demonstrated its lack of concern with safeguarding consumer personal information. Therefore, all data providers would have a clear risk management basis to block this entity from connecting to its interface.

---

[53] *Supra*, note 14.

[54] 15 USC 6801(b), https://uscode.house.gov/view.xhtml?hl=false&edition=prelim&req=granuleid%3AUSC-prelim-title15-section6801&f=treesort&num=0&saved=%7CKHRpdGxlOjE1IHNlY3Rpb246NjgwNSBlZGl0aW9uOnByZWxpbSkgT1IgKGdyYW51bGVpZDpVU0MtcHJlbGltLXRpdGxlMTUtc2VjdGlvbjY4MDUp%7CdHJlZXNvcnQ%3D%7C%7C0%7Cfalse%7Cprelim.

On the other side of the coin, affirmative obligations for the entities seeking to connect to data providers would provide the necessary stick. The existing risk management denial section[55] could be rewritten to encompass these concepts, and the prudential agencies may have a role here as well.

As addressed in Sections II(B) and III(B) above, the information security risks present in the consumer-permissioned data sharing ecosystem are a direct function of the disparity in oversight. While banks undergo supervision to ensure compliance with safeguarding requirements, non-traditional entities such as data aggregators, fintechs, and data recipients outside the financial sector do not. As a result of this gap, ABA is deeply concerned that information security concerns will not be taken seriously unless the CFPB coordinates closely with the prudential banking agencies in clearly laying expectations for the ecosystem. This is all the more reason why it is necessary for the Bureau to limit the purposes for which the data is shared and supervise data aggregators and larger fintechs as part of the PFDR rule.

For example, unleashing personal information throughout the ecosystem introduces heightened risk of data breaches. While these are rooted both in prudential regulation for banks as well as by operation of state law for other entities (see this database of applicable state law compiled by the law firm Perkins Coie), a requirement that downstream entities notify the data provider of a potential breach scenario in addition to the impacted consumers would go a long way to establishing baseline standards of behavior. This concept exists in other areas of the law as well; for example, the Fair Credit Reporting Act requires resellers to notify credit reporting agencies if they are reselling the consumer report, to which entity the report is going, and confirming that entity has permissible purpose.[56] This would necessitate concepts such as "traceability" into the rule, which would lead to more advanced data governance (and thereby information security) programs. However, this would still not be sufficient without shifting liability and indemnification by the parties in the best position to mitigate risks—i.e., data aggregators and data recipients.

The very nature of digitally sharing personal information about a consumer through a network of third parties carries a degree of fraud risk. The "consumer" granting permission could be impersonating the actual subject, or the data recipient could be the bad actor. According to an ABA analysis of Juniper Research's Global Open Banking APIs Market: 2025 – 2029 dataset, 57% of permissioned data sharing API calls were associated with account aggregation and personal finance management and 23% of open banking API calls were associated with identity verification.[57] One can easily imagine how a fraudster or other financial criminal could take advantage of these tools. Banks continue to have several contemporaneous requirements, such as monitoring for illicit finance. Mandating the sharing of personal information via an expansive rule exacerbates these risks, and will scale as the market increases in size.

---

[55] *Supra*, note 3 at 12 CFR 1033.321, https://www.ecfr.gov/current/title-12/chapter-X/part-1033/subpart-C/section-1033.321.

[56] 15 USC 1681e(e), https://uscode.house.gov/view.xhtml?req=(title:15%20section:1681e%20edition:prelim)%20OR%20(granuleid:USC-prelim-title15-section1681e)&f=treesort&edition=prelim&num=0&jumpTo=true.

[57] ABA analysis of Global Open Banking APIs Market: 2025-2029 data provided by Juniper Research; *supra,* note 47.

Another key shortcoming of the November 2024 PFDR rule is its restrictive approach to data access denials. By permitting banks to deny access only in narrowly defined circumstances (i.e., "[d]irectly related to a specific risk of which the data provider is aware," "[a]pplied in a consistent and non-discriminatory manner[,]" and pertains to specific "laws and regulations regarding risk management"[58]) rather than a flexible framework the rule limits banks' ability to proactively protect consumers. This approach also conflicts with interagency guidance on third party risk management issued by the prudential agencies, which requires institutions to manage risks broadly, including potential and emerging risks, across all operational areas.[59] Banks should have the right to terminate access based on ***anticipated*** risk concerns. This authority should be grounded in GLBA language, specifically Section 501(b), which requires administrative, technical, and physical safeguards to:

(1) ensure the confidentiality of customer records and information;
(2) protect against ***anticipated threats or hazards*** to the security or integrity of such records;
(3) prevent unauthorized access or use that could result in substantial harm or inconvenience to customers.[60]

To better support consumer protection, the re-proposed rule should clearly permit data providers to evaluate third-party risk management practices before approving data sharing. It should also affirm that denying access for valid risk concerns—beyond data security and consistent with interagency third-party risk management guidance[61]—is *per se* reasonable.

Consumers understand that sometimes data providers will need to deny access if it means safeguarding their information. In a recent survey, 80% of respondents agreed "companies and organizations should be able to withhold a consumer's information if they have reason to believe sharing will result in a high degree of risk, such as unauthorized activity or data breaches."[62]

Additionally, the current rule allows authorized third parties and data aggregators to share consumer data with additional downstream parties—often without the knowledge of the customer or the original data provider. To enable data providers to properly assess the risks associated with data sharing, the rule should require third parties to disclose to data providers the following information prior to accessing any data:

(1) the specific authorized use case;
(2) their role in the transaction (e.g., aggregator, end-user); and
(3) whether any additional downstream entities (i.e., fourth, fifth, or *n*th parties) will access or use the data.

---

[58] *Supra*, note 3 at 12 CFR 1033.321, https://www.ecfr.gov/current/title-12/chapter-X/part-1033/subpart-C/section-1033.321.
[59] *Supra,* note 10.
[60] *See* the Interagency Guidance applying to banks of various charter types that operationalizes this requirement, https://www.ecfr.gov/current/title-12/chapter-I/part-30/appendix-Appendix%20B%20to%20Part%2030,
[61] *Supra*, note 10.
[62] *Morning Consult* at Question ABA5a_3; *supra*, note 29.

RECOMMENDATION: Screen scraping must be sunset and specifically designated as an Unfair, Deceptive, or Abusive Act or Practice (UDAAP) violation. To ensure compliance with the prohibition, data providers must be able to block screen scraping without fear of reprisal. The re-proposed rule must include clear timelines when the prohibition of screen scraping goes into effect, which could also serve as the compliance dates.

RECOMMENDATION: The CFPB should remove the exemption for community banks and credit unions with assets of $850 million and less.[63] While we understand the noble motivation behind carving out small entities, according to the CFPB's own data it leaves over 74% of community banks and over 89% of credit unions out of the rule's reach for data providers[64] and will have the effect of perpetuating screen scraping, injecting additional risk into the ecosystem, creating inconsistent consumer experiences (and protections), and harming the competitiveness of community banks in an increasingly digital world. Allowing data providers to charge fees will alleviate the removal of the exemption for smaller depository institutions.

RECOMMENDATION: To the extent any re-proposed rule regulates data sharing throughout the ecosystem it should include a clear liability framework requiring a responsible party to notify others of potential data breaches or unauthorized activities, with a methodology for restitution. Given the prudential agencies' and the FTC's responsibilities on safeguarding, the Bureau must coordinate with them in this matter. The re-proposed rule should establish safe harbor provisions and a clear liability framework. The principles underpinning this liability regime should be:

(1) data providers are afforded a safe harbor when data misuse occurs downstream;
(2) liability follows the data, with third party recipients liable for fraud, data breaches, or other misuse due to their own activities and data handling;
(3) data providers should retain discretion to require liability and indemnification terms as a condition for access; and
(4) data aggregators and data recipients should be required to certify that they are adequately capitalized and carry indemnity insurance to support their liability obligations.

RECOMMENDATION (REPRISE): The CFPB must not restrict data providers' ability to conduct risk management activities before, during, and after sharing data pursuant to consumer consent, to include conducting appropriate due diligence on data aggregators and data recipients prior to establishing connections.

VI. As written, the rule adequately addresses privacy risks but could be improved

The "reasonably necessary" standard in the November 2024 PFDR rule[65] is for the most part satisfactory to ABA members. Sale of data should continue to be prohibited, even in

[63] *Supra*, note 3 at 12 CFR 1033.111(d), https://www.ecfr.gov/current/title-12/chapter-X/part-1033/subpart-A/section-1033.111.
[64] *Supra*, note 14 at Table 1.
[65] Supra, note 3 at 12 CFR 1033.421, https://www.ecfr.gov/current/title-12/chapter-X/part-1033/subpart-D/section-1033.421.

anonymized/aggregated/deidentified form. Data aggregators have never adhered to strong privacy protections such as those outlined in the November 2024 PFDR rule. Importantly, consumers are not "choosing" to do business with a given data aggregator. Data aggregators only exist in the ecosystem as service providers to the companies that consumers *do* engage with; as such, they should face more stringent requirements for handling the data.

While ABA members were conceptually comfortable with the general "reasonably necessary" approach to privacy[66] in the November 2024 PFDR rule, the relevant sections would benefit from additional limitations, clarifications, and examples. Examples should include both permissible and forbidden activities. For instance, permissible activity might be informing customers about high-yield savings accounts generally as part of a personal budgeting tool; forbidden activity should include reverse engineering of bulk consumer data to indirectly obtain confidential commercial information.

While fintechs and data aggregators fervently wish to expand permissible secondary uses, the current allowances for legal compliance, fraud prevention, and product/service fulfillment are sufficient.[67] Due to the presence of the "on behalf of" qualifier in Dodd-Frank, the broadest possible reading of Section 1033 would mean the right only exists when the representative is acting in the consumer's interests. Any secondary use beyond the above should be forbidden; otherwise, the data should only be used in accordance with the consumer's specific, express consent.

In a recent survey, 80% of respondents agreed that "data recipients and data aggregators should NOT be able to use consumer data they obtain from banks to train AI models or develop new products and services without getting explicit consent from the consumer."[68]

Activities using consumer-permissioned data could and should be governed by appropriate informed consent pursuant to the following general principles with an appropriate audit trail:

(1) the data collected pursuant to the consumer's specific authorization should be limited to no more than what is reasonably necessary to deliver the core product or service the customer requested;
(2) data recipients must use clear and conspicuous language to explain what data will be accessed, how often, by whom (including upstream and downstream parties), for how long, and in what way;
(3) the consumer has granted permission and established the parameters for access and usage;
(4) data access must be limited in time to what is needed to deliver the requested product or service (e.g., there is no basis for ongoing access to consumer information unless imperative for the use case);
(5) for data aggregators acting in middleman roles, this should mean that they cannot keep copies of consumer financial data after passing the data onto the data recipient. Data

[66] *Id.*
[67] *Id.*
[68] *Morning Consult* at Question ABA5a_2; *supra*, note 29.

aggregators should not be allowed to continue monetizing consumer financial data without consumers' explicit consent;
(6) revocation must be as easy to effectuate as the initial consent and the data recipient must notify the data provider (the data provider should also be allowed to maintain a revocation mechanism); and
(7) once such revocation occurs, the data recipient must safely dispose of the permissioned data as soon as possible outside of legal necessity.

The current 1033 rule's disclosure framework can also be improved to aid consumers. As written, there is a probability that consumers would not fully understand the current authorization disclosures given the technical and legalistic requirements set forth in the November 2024 PFDR rule. This is especially true if the fintech or other data recipient is seeking permission for multiple use cases since this experience would likely need to involve so many screens that the consumer is overwhelmed with information. The CFPB should reconsider the authorization framework in the current rule and require a process that is more intuitive for and comprehensible to consumers. Indeed, the CFPB should consider including a model form in the re-proposed rule.

Collection and use of data directly by first parties is fundamentally different than a third party retrieving the consumer's data from a financial institution pursuant to the consumer's authorization. The latter scenario is a distinct subset of financial activity and accordingly should have tailored obligations for the collection, use, and protection of personal information.

Therefore, data providers should continue to be permitted to obtain their own consumer authorizations prior to sharing data with third parties, as well as conduct adequate due diligence before any data is shared, to include: the specific authorized use case; the entity's role in the transaction (e.g., aggregator, end-user); and whether any additional upstream or downstream parties will access or use the data.

Finally, the following section would benefit from revision: "[n]ames of parties with which the covered data was shared…[t]he names must be readily understandable to the consumer."[69] A more practical approach would be to require disclosing ***categories*** of third parties, which would align with the standard contained in many comprehensive state privacy laws (for example, the California Consumer Privacy Act of 2018, as amended).[70] This would recognize the operational challenges and risks associated with identifying specific entities and instead focus on transparency through categorical disclosures.

RECOMMENDATION: The CFPB should retain the general prohibition on secondary uses in its re-proposed PFDR rule, but should add examples of permissible and forbidden behavior under this framework, the latter of which must include "reverse engineering."

[69] *Supra,* note 3 at 12 CFR 1033.421, https://www.ecfr.gov/current/title-12/chapter-X/part-1033/subpart-D/section-1033.421.
[70] https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5; *see* Section 1798.110(a)(4).

RECOMMENDATION: Express informed consent is the appropriate principle governing activities using consumer-permissioned data. A model form should be included, use of which would provide a safe harbor.

RECOMMENDATION: For purposes of the "keeping consumer informed" request, CFPB should amend the requirement to the "categories" of third parties rather than the specific "names."

VII. Industry standard setting should be limited to data formats

The CFPB took the unusual step of finalizing a portion of the PFDR rule in June 2024, which created a process for recognition of industry standard setters to provide an indicia of compliance with substantive portions of the regulation.[71] During the previous round of rulemaking, ABA urged the CFPB to leverage the API spec issued by the FDX[72] so that the ecosystem didn't have to start from scratch. The CFPB found a way to do this, albeit in a disjointed process fraught with uncertainty (e.g., the CFPB "may" publish the application, "may" seek public input).[73] The CFPB recognized FDX for standardized data formats in January 2025,[74] an outcome advocated by ABA in an October comment letter.[75]

While a consensus standard for standardized formats is highly sensible, in general the November 2024 PFDR rule simply delegated too much. The re-proposed rule should not call for industry standard setting in the following areas:

(1) notice and amount of scheduled downtime;
(2) commercial reasonableness of the developer interface performance and response time;
(3) access caps;
(4) reasonable denials;
(5) reasonableness of data provider revocation methods;
(6) sufficiency of developer interface documentation to enable third party access and use;
(7) listing data fields;
(8) examples of policies and procedures regarding accuracy; and
(9) reasonableness of reauthorization requests.[76]

RECOMMENDATION: The number of provisions contemplated for industry standard-setting bodies must be limited. Only a format concerning standardized formats (i.e., API specs) would

[71] *Supra*, note 5.
[72] https://www.financialdataexchange.org/FDX/About/About-FDX.aspx?WebsiteKey=deae9d6d-1a7a-457b-a678-8a5517f8a474&hkey=dffb9a93-fc7d-4f65-840c-f2cfbe7fe8a6&a315d1c24e44=8#a315d1c24e44.
[73] *Supra,* note 3 at Appendix A to Part 1033—Personal Financial Data Rights Rule: How to Apply for Recognition as a Standard Setter, https://www.ecfr.gov/current/title-12/chapter-X/part-1033/appendix-Appendix%20A%20to%20Part%201033.
[74] https://www.consumerfinance.gov/about-us/newsroom/cfpb-approves-application-from-financial-data-exchange-to-issue-standards-for-open-banking/.
[75] https://www.aba.com/advocacy/policy-analysis/letter-to-cfpb-on-1033-rule.
[76] *Supra*, note 3.

be of utility (incidentally, it is the only area that currently has a recognized industry standard setter—the Financial Data Exchange[77]). Moreover, the deference to the standardized format standard must be strengthened to a safe harbor instead of the ambiguous "indicia of compliance."

VIII. Compliance dates for the re-proposed rule should be at least 2 years after new consensus standards for data formats are issued

As discussed above, because the current rule is effective and the CFPB is working to revise it, the compliance dates should be suspended immediately to avoid unnecessary expenditure of time and resources.

If the Bureau continues to delegate to industry standard-setters, the triggering of any compliance runway should be tied to these entities. Simple recognition is not sufficient, as in many cases the issuance of the consensus standards themselves occurs later. The first compliance date under the re-proposed rule should occur no sooner than 2 years after the publication of a consensus standard for data formats under the re-proposed PFDR rule.

ABA members generally supported a tiered structure based on asset size or total receipts; however, compliance dates should apply broadly to all covered persons operating in the ecosystem and not be limited to data providers only. Another possibility would be to also incorporate specific milestones for each tranche so that full compliance is not mandated on Day One. Realistically, data aggregators and data recipients will have to negotiate or amend bilateral agreements to address liability, and will need to conduct development and testing before moving to production. In short, the compliance dates should be a compliance *phase*.

Moreover, many banks will be reliant on service providers to maintain any developer interfaces on their behalf. However, the market is not currently tailored to any re-proposed rule. These service providers should be consulted by the CFPB for when *they* will be ready, as this will flow down to data providers.

As peppered throughout this comment, the CFPB should also take steps to supervise data aggregators and larger fintechs under the re-proposed PFDR rule, and they must also be given adequate time to come into compliance.

RECOMMENDATION: The CFPB must suspend the current compliance dates immediately via publication of an interim final rule. The re-proposed PFDR rule must set a period of 2 years from the issuance of consensus standards for data formats.

Conclusion

ABA and our members greatly appreciate the CFPB revisiting the deeply flawed November 2024 PFDR rule. We have shared our perspective on the specific areas requested in the Bureau's

[77] *Supra*, note 15.

ANPR as well as other matters that are key to a re-proposal's success, and have made a number of relevant recommendations in those areas. We look forward to continuing our engagement with the CFPB on this critical rulemaking.

If you have any questions about this comment, please contact Ryan T. Miller (rmiller@aba.com) at (202) 663-7675.

Respectfully submitted,

Ryan T. Miller
Vice President & Senior Counsel, Innovation Policy