October 21, 2025

Via Electronic Delivery

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

Re: Advance Notice of Proposed Rulemaking on Personal Financial Data Rights Reconsideration (CFPB Docket No. CFPB–2025–0037)

Dear Acting Director Vought,

The Consumer Bankers Association (CBA) [1] appreciates the opportunity to respond to the Consumer Financial Protection Bureau's (CFPB) advance notice of proposed rulemaking (ANPR) entitled "Personal Financial Data Rights Reconsideration" (1033 ANPR)[2], which is meant to inform the CFPB's ongoing reconsideration of the Personal Financial Data Rights final rule (PFDR Rule)[3] that implemented section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act)[4] under the prior Administration. CBA supports consumers having access to their own personal financial information, but believes the PFDR Rule severely missed the mark, extending well beyond the statutory requirements, and failed to incorporate much of the critical feedback provided by industry through the comment period, resulting in a final rule that did not reflect market, technological, and practical realities.

As a more time-sensitive matter, the PFDR Rule compliance dates remain in effect, even though the CFPB is currently reconsidering the rule. As discussed later in this letter, this puts data providers in the position of having to make decisions now in anticipation of complying with the existing PFDR Rule—even though they are aware that significant changes may be forthcoming. Data providers should be building their systems based on what the final version of the PFDR Rule will be, rather than on the version issued under the prior Administration. To support this, the CFPB is empowered to either extend the PFDR Rule's compliance dates by at least one year, or suspend them altogether, pending the finalization of the CFPB's re-proposal of the rule, inclusive of a final resolution of the

[1] The CBA is a member-driven trade association, and the only national financial trade group focused exclusively on retail banking—banking services geared toward consumers and small businesses. As the recognized voice on retail banking issues, CBA provides leadership, education, research, and federal representation for its members. CBA members operate in all 50 states. They include the nation's largest bank holding companies as well as regional and super-community banks. Eighty-three percent of CBA's members are financial institutions holding more than $10 billion in assets.
[2] Personal Financial Data Rights Reconsideration, 90 Fed. Reg. 40986 (Aug. 22, 2025), *available here*.
[3] Required Rulemaking on Personal Financial Data Rights, 89 Fed. Reg. 90838 (Nov. 18, 2024), *available here*.
[4] 12 U.S.C. § 5533.

litigation regarding the rulemaking.[5] Additionally, while this ANPR does not pose questions regarding the types of data that should be shared under the PFDR Rule, CBA reiterates its opposition to the sharing of payment initiation information. As CBA has previously stated, sharing payment initiation information without adequate safeguards can significantly increase the risk of fraud and result in tangible losses to both consumers and data providers.[6] Further, the data sharing ecosystem is functioning well today, with millions of consumers already sharing their data safely through APIs offered by banks in arrangements governed by freely-negotiated bilateral agreements. These agreements have allowed banks, fintechs, and data aggregators to address privacy and security concerns while promoting consumers' ability to share their data. The CFPB should not impede the ability of market participants to negotiate contracts that enable innovation and competition, to the ultimate benefit of the consumer.

To assist the CFPB in its reconsideration of the PFDR Rule, CBA recommends that the CFPB specifically re-examine several areas including:

- ***Consumer and Representative***: The CFPB should conclude that third parties and data aggregators are not "consumers" under section 1033 of the Dodd-Frank Act because they are not "representative[s] acting on behalf of an individual" due to the fact they are operating with the consumer in a business relationship, one often premised on monetizing that consumer's data, rather than a fiduciary relationship.

- ***Costs & Fees***: The PFDR Rule incorrectly prohibited data providers from imposing fees on third parties and data aggregators accessing consumer data, and the CFPB should reverse this decision to permit all market participants in the data access ecosystem to charge fees as part of their business model, should they choose to do so.

---

[5] Some stakeholders may argue that, as an alternative to extending the compliance timelines, the CFPB could announce that it will not prioritize enforcement or supervision actions with regard to any penalties or fines associated the PFDR Rule, and instead will keep its enforcement and supervision resources focused on pressing threats to consumers. The CFPB has previously made similar announcement in connection with the Payday, Vehicle Title, and Certain High-Cost Installment Loans Regulation and the applicability of Regulation Z to "Buy Now, Pay Later" products. However, it will take significant time for the covered persons subject to the rule to appropriately design, implement, and test the systems necessary to comply with the rule's requirements. Further, even if the CFPB commits to withhold from enforcement or supervisory activity, state regulators would still be able to seek actions, and develop relevant case law, under the CFPB's new rule.

[6] *See* CBA, *Letter re: Docket No. CFPB-2023-0052 – Required Rulemaking on Personal Financial Data Rights* (Dec. 29, 2023), *available here* ("The sharing of information for initiating a payment to or from a Regulation E account, particularly the sharing of non-tokenized account and routing numbers, will make third parties an increased target for data breaches. Compromised credentials could be used to initiate fraudulent transactions, which would not only harm consumers, but also drastically expand the liability that will rest with either data providers or with consumers. Beyond the concerns outlined later in this letter regarding liability, the liability risk related to this specific covered data is magnified because of the differences for liability allocation under the NACHA Rules compared to Regulation E." (internal citations omitted)).

- ***Information Security:*** Any reconsidered PFDR Rule should explicitly prohibit screen scraping and bank data providers should be afforded clearer guidance on third-party risk management practices under the PFDR Rule that aligns with expectations of their prudential regulators.

- ***Data Privacy:*** The CFPB should maintain its secondary use limitations for third parties, but also provide clarity on the consumer consent and revocation process, as well as limit data aggregators' access to and practices with consumer data.

- ***Compliance Dates***: The CFPB is the only agency able to immediately delay the PFDR Rule compliance dates, as they are imminently approaching. Data providers must make decisions and resource allocations now in anticipation of complying with the current PFDR Rule, even though the CFPB intends to revise it. As such, CBA respectfully requests that the CFPB extend the compliance dates for the current PFDR Rule a minimum of one year following finalization of any re-proposal, inclusive of a final resolution of the litigation regarding the rulemaking, or suspend the compliance dates altogether.

Please find below CBA's more specific responses to certain questions in the Dodd-Frank Act 1033 ANPR.

* * *

Consumer and Representative (Questions 1-8)

Q1. What is the plain meaning of the term "representative?" Does the PFDR Rule's interpretation of the phrase "representative acting on behalf of an individual" represent the best reading of the statutory language? Why or why not?

The plain language of section 1033 of the Dodd-Frank Act is fundamentally centered on a *consumer's* access to information:

> "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*."[7]

[7] 12 U.S.C. § 5533(a) (emphasis added).

While ongoing litigation in connection with the PFDR Rule has raised concerns over whether the term "consumer" refers solely to an individual customer rather the definition found under the Dodd-Frank Act,[8] and indeed the CFPB itself has recognized the PFDR Rule's interpretation of the term "stretches the definition of 'consumer' past its breaking point,"[9] even under the Dodd-Frank Act definition, fintechs and other third parties are not "consumers" because they are not "representatives acting on behalf of an individual."

A "consumer" under the Dodd-Frank Act is defined as "an individual or an agent, trustee, or representative acting on behalf of an individual."[10] As the CFPB itself notes in the Dodd-Frank Act 1033 ANPR, the PFDR Rule "interpreted the phrase 'representative acting on behalf of an individual' to include third parties that access consumers' data pursuant to certain authorization procedures and substantive obligations."[11] This interpretation was flawed. In common law, the terms "agent" and "trustee" denote a fiduciary relationship that requires trust and confidence, as well as a duty of loyalty to act for the principal's benefit.[12] The proximity of the term "representative" relative to "agent" and "trustee" suggests that "representatives" should bear a similar fiduciary relationship with a duty of loyalty to act for the consumer's benefit.[13] The addition of the phrase "acting on behalf of an individual" after the word "representative" in the Dodd-Frank Act strengthens the fact that these terms are associated with fiduciary-like duties. These definitions invoke familiar, deeply rooted legal arrangements and do not capture the casual, and often short-lived, arm's-length commercial relationship between a customer and a data aggregator or service provider.

Fintechs and other third parties do not qualify as "consumers" then because they are not "representative[s] acting on behalf of an individual." In the data access ecosystem context, these are commercial entities engaged in business transactions with individual consumers that are governed by contractual obligations. Moreover, the primary business practices of these commercial entities are not premised on offering fiduciary-like services to consumers, but utilizing those consumers' data for other, self-interested purposes and services, such as research on future products the consumers sharing their data may not want, further demonstrating they are not truly acting on behalf of consumers.

---

[8] *See* Pl. ['s] Mot. for Summ. J. at 14-15, Forcht Bank, N.A. v. Consumer Fin. Prot. Bureau, No. 5:24-cv-304-DCR (E.D. Ky. May 30, 2025), *available here.*

[9] Def. Mem. in Supp. of Mot. for Summ. J. at 8, Forcht Bank, N.A. v. Consumer Fin. Prot. Bureau, No. 5:24-cv-304-DCR (E.D. Ky. May 30, 2025), *available here*.

[10] 12 U.S.C. § 5481(4).

[11] Personal Financial Data Rights Reconsideration, *supra* note 2, at 40987.

[12] *See* Personal Financial Data Rights Reconsideration, *supra* note 2, at 40987. S*ee also* Pl. ['s] Mot. for Summ. J., *supra note 8* at 16.

[13] The term "representative" need not bear every hallmark of an "agent" or "trustee," relationships with their own unique legal prerequisites, duties, and associations. Instead, "representative" captures other relationships that may not match the strict definitions of agency or trusteeship, but are likewise characterized by delegated authority, control, and loyalty.

Data aggregators do not act on behalf of consumers; rather, they serve as intermediaries selected by authorized third parties to facilitate the sharing of data. Data aggregators exist to facilitate data sharing and often do so without the consumer's awareness that their data may be stored and utilized by that data aggregator. Consumers generally do not have the ability to choose whether to use a data aggregator to benefit from the services from an authorized third party. As such, fintech and other third parties do not meet the definition of "representative" because they are operating with the consumer in a business relationship rather than a fiduciary relationship, and data aggregators are not "representatives" because they are merely data sharing intermediaries rather than an entity a consumer has a tangible fiduciary-like relationship with.

Q3. Does the statutory reference to an "agent, trustee, or representative" indicate that "representative" is intended to encompass only those representatives that are serving in a fiduciary capacity? If a "representative" under 12 U.S.C. 5481(4) is interpreted to be an individual or entity with fiduciary duties, what are the distinctions between an "agent" and a "representative" for purposes of section 1033?

As indicated in response to Q1, the proximity of the term "representative" relative to "agent" and "trustee" suggests that "representatives" should bear a similar fiduciary relationship with a duty of loyalty to act for the consumer's benefit. The addition of the phrase "acting on behalf of an individual" after the word "representative" in the Dodd-Frank Act strengthens the fact that these terms are associated with fiduciary-like duties.

Q4. In seeking the best reading of the statutory language, what evidence or interpretive principles should the Bureau consider with respect to the term "representative?"

As indicated in response to Q1, consistent with the linguistic canon of construction *noscitur a sociis*,[14] the proximity of the term "representative" relative to "agent" and "trustee" suggests that "representatives" should bear a similar fiduciary relationship with a duty of loyalty to act. The addition of the phrase "acting on behalf of an individual" after the word "representative" in the Dodd-Frank Act strengthens the fact that these terms are associated with fiduciary-like duties.

Q5. If a "representative" under 12 U.S.C. 5481(4) is interpreted to mean an individual or entity with fiduciary duties, to what extent would it limit customers' ability to transfer their transaction data to third parties under section 1033 or the ability of financial technology and other third-party service providers to compete with incumbent market participants?

When evaluating customers' ability to transfer their transaction data to third parties and competition within the data access ecosystem, it is important that policymakers,

[14] Latin phrase meaning "a term known by its associates." *See* Strauss et al., GELLHORN AND BYSE'S ADMINISTRATIVE LAW CASES AND COMMENTS 135 (12th ed. 2018).

including the CFPB, be mindful of the distinction between what the CFPB is statutorily permitted to prescribe and what the market has already independently adopted.

Covered persons are required to make information available in an electronic form usable by consumers.[15] Consequently, individual consumers today can download their data in machine-readable formats and then share that data themselves with fintechs and other third-party providers at their discretion. This process allows consumers to have true control over which of their data is shared, regardless of how the term "representative" is interpreted. Through online banking and these machine-readable formats, it could even be argued that many banks are already complying with the statutory language of section 1033.

The market has evolved independently of statutory requirements, as banks originated innovations almost a decade ago that created a safe, secure data access ecosystem with the development of application programming interfaces (APIs). Consumers in the marketplace have shared their data with thousands of third parties through this framework even without a regulatory mandate under a section 1033 rulemaking. Fintechs and other third-party providers now compete with banks by building experiences that enable consumers to share their financial data directly. Alternatively, they may collaborate with banks through bilateral agreements that include appropriate data security and privacy protections for individuals. A faithful interpretation of the requirements of section 1033 mandates that fintechs and other third-party providers access consumer financial data via these channels. Consumers can also share account categories beyond those covered by the PFDR Rule—such as brokerage[16] account information—and do so willingly with entities not covered by the PFDR Rule. Importantly, these advancements are a result of the free market, which enables parties to innovate, compete, and offer compelling products and services, allowing consumers to choose which data to share. CFPB has the ability to ensure any final rule enables the free market to continue to develop and thrive, instead of imposing counterproductive regulatory barriers.

Q6. Does the requirement in section 1033 for the Bureau to prescribe standards promoting the development and use of standardized formats for information made available under section 1033 illuminate the types of entities that should be considered "consumers" or have any other implications for how "representative" under 12 U.S.C. 5481(4) should be interpreted?

---

[15] *See* 12 U.S.C. § 5533(a).

[16] Any supervision by the CFPB in connection with brokerage accounts under the scope of a section 1033 final rule should be performed on data providers already subject to supervision by the CFPB. To the extent that an entity offering brokerage accounts is registered with the Securities and Exchange Commission (SEC), such entity should not be subject to the CFPB's supervisory authority following the finalization of this rulemaking. However, the foregoing does not limit the ability of the SEC itself to supervise any such SEC-registered entity.

As summarized in response to Q1, the term "consumer" refers to an individual customer, and fintechs and other third parties fail to meet the definition of "consumer" because they are not "representatives acting on behalf of an individual." Under the statutory text, banks are required to make certain data "available in an electronic form usable by consumers,"[17] and the CFPB "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."[18] Taken together, these two provisions can be read as referring to data formats banks employ to provide individuals their own data, such as CSV files or PDF file, that consumers can then share with third parties. This interpretation also aligns with the reality that consumer-permissioned data sharing and open banking, as they exist today, emerged after the enactment of the Dodd-Frank Act. This suggests that Congress did not intend for the statute to apply to third-party data sharing, as such practices were not contemplated in the same way at the time. It should also be noted that, while nothing in section 1033 of the Dodd-Frank Act itself references APIs, open authorization (OAuth), or other aspects of the data access ecosystem, these elements have emerged based on banks' investment in the data access ecosystem and are continuing to grow in utilization even absent a formal rulemaking.

Q7. If a "representative" under 12 U.S.C. 5481(4) is interpreted not to be required to have fiduciary duties, what elements are required in establishing that the individual is a "representative" acting on behalf of the consumer?

As summarized in response to Q1, the proximity of the term "representative" relative to "agent" and "trustee" suggests that "representatives" should bear a similar fiduciary relationship with a duty of loyalty to act. Nevertheless, even *if* the term "representative" is interpreted not to be required to have formal fiduciary duties, it is imperative that such fintechs and other third-party providers granted a regulatory right to access consumer data are truly "acting on behalf of" the consumer, particularly because many of these entities' primary business practices are centered on utilizing consumers' data for other purposes. These entities should have clear obligations inspired by agency and fiduciary principles, including that third parties must:

- Provide *clear and conspicuous disclosures* for every authorization of use of an individual consumer's data, with documentation that the consumer is requesting their data be transferred to such third parties to provide one or more specific products or services. The disclosures must also provide consumers with a clear explanation for what consumer data will be accessed, how often, by whom – including any fourth parties – for how long, and in what manner. Such disclosures must be readily apparent to the consumer;

- *Collect, use, and retain data for the consumer only as necessary* to provide the

[17] 12 U.S.C. § 5533(a).
[18] 12 U.S.C. § 5533(d).

product or service as request, and may not use data for purposes beyond accomplishing that consumer's requested service except for fraud and product improvement uses;

- *Not engage in any secondary uses* of the consumer's data, including when such data is anonymized or aggregated with other data;

- Keep the customer's information *confidential and secure*; and

- *Assume liability* for any misuse or compromise of consumer's data, as well as be *adequately capitalized* to make good on these liability obligations.

The assumption of liability and requirement for third parties and data aggregators to be adequately capitalized to make good on their liability obligations[19] is particularly pertinent given that, if the CFPB does not adjust the categories of data that are to be shared by data providers with authorized third parties and data aggregators, sensitive information will be shared that can supercharge fraudulent payments activity. As CBA has explained:

> "The sharing of information for initiating a payment to or from a Regulation E account, particularly the sharing of non-tokenized account and routing numbers, will make third parties an increased target for data breaches. Compromised credentials could be used to initiate fraudulent transactions, which would not only harm consumers, but also drastically expand the liability that will rest with either data providers or with consumers… the liability risk related to this specific covered data is magnified because of the differences for liability allocation under the NACHA Rules compared to Regulation E."[20]

It is vital that *if* fintechs and other third-party providers are entitled by a new PFDR Rule to access consumer data through APIs that they (i) are truly acting on behalf of consumers, and (ii) they then have adequate agent and fiduciary-inspired obligations to protect those consumers.

---

[19] CBA has previously recommended that, as part of the certification statement provided as part of the authorization disclosure by a third party, the third party should certify that (i) third parties and data aggregators agree to accept potential liability for when consumer credentials are misused by a third party or data aggregator, or are compromised in a data breach then subsequently used to initiate a fraudulent transaction, and (ii) third parties and data aggregators are adequately capitalized and carry indemnity insurance to make good on their liability obligations. *See* CBA, *supra* note 6.

[20] *See* CBA, *supra* note 6. Even beyond payment initiation information, the CFPB should carefully review the list of required data elements that comprise "covered data" and only mandate the sharing of data authorized by section 1033. For example, credit limits are currently included as "covered data", but this data is not reasonably part of the "[i]nformation relating to any transaction, series of transactions, or to the account including cost, charges and usage data" required to be shared in the statute.

Costs & Fees (Questions 9-18)

Q9. Does the PFDR Rule's prohibition on fees represent the best reading of the statute? Why or why not?

No, the PFDR Rule's prohibition on fees is not the best reading of the statute because it (i) goes far beyond the intent and plain reading of the statute, (ii) will disincentivize investment in the market, ultimately negatively impacting consumers, and (iii) risks creating an anticompetitive imbalance in the market.

Statutory Intent: The PFDR Rule's prohibition on fees was done in excess of the statute. Nothing in the language of section 1033 of the Dodd-Frank Act indicates that fees are impermissible,[21] and nothing suggests that Congress intended to authorize the CFPB to force data providers to develop and maintain APIs to facilitate data sharing with third parties and data aggregators for free, while those same entities can profit off of this information sharing. This is in contrast to Congress's historic practice of explicitly delineating when it seeks to prohibit fees. As CBA previously stated:

> "Congress has historically been very clear when it wants fees to be treated in a certain manner and when it is empowering a regulator to set fees related to consumer finance. For example, the Fair and Accurate Credit Transactions Act amended the [Fair Credit Reporting Act (FCRA)] to provide consumers with a right to receive one free credit report every year. Similarly, the Credit Card Accountability Responsibility and Disclosure Act amended the Truth in Lending Act to, among other things, outline requirements related to late fees and prohibit certain types of fees, such as double-cycle billing and penalties for on-time payments. Section 1033 contains no analogous language relating to fees, suggesting that Congress did not view Section 1033 as empowering the Bureau to prohibit fees in connection with the consumer access to data."[22]

Disincentivize Investment: As further discussed in Q10, data providers reinvest amounts from fees into technological investments that lead to innovation and useful financial products and services that benefit consumers. Investment in innovation is not static, but instead is an ongoing activity as banks continue not just to innovate to offer new products, but also protect their consumers from continually evolving threats. Without the ability to charge fees, data providers will necessarily be able to dedicate fewer resources toward these investments that, ultimately, benefit and protect consumers.

Anticompetitive Imbalance in the Market: A prohibition on data providers being able to charge fees can also result in an anticompetitive windfall for certain market participants at the expense of a competitive market and all other participants in the data access ecosystem. Under the PFDR Rule, data providers would be prohibited from charging

[21] *See* 12 U.S.C. § 5533.
[22] CBA, *supra* note 6 (internal citations omitted).

any fees to third parties designed to recover costs associated with developing and maintaining the necessary frameworks for facilitating the data sharing envisioned by the rule. However, data aggregators remain able to charge fees, and to the extent that data aggregators do so, third parties that pay data aggregators are likely to pass on those fees to the consumer. The net result is the one-sided fee prohibition is a windfall to data aggregators at the expense of data providers and consumers. This imbalance would be partially offset if data providers are likewise allowed to charge fees for accessing the developer interface. Further, as discussed more in response to Q10, limiting data providers' ability to charge fees will limit their ability to invest in technological innovation to the same degree that third parties and data aggregators will be able to, further distorting competition in the market.

Q10. Was the PFDR Rule correct to conclude that permitting fees "would obstruct the data access right that Congress contemplated"? Why or why not?

No, the PFDR Rule was not correct to conclude that permitting fees "would obstruct the data access right that Congress contemplated."[23] As summarized in the response to Q9, the CFPB does not have the authority to prohibit fees and the decision could result in an anticompetitive market. Moreover, the CFPB's logic in prohibiting data providers from charging is equally as applicable to the very real fees that data aggregators charge to third party fintech apps, banks, and others. The CFPB in its notice of proposed rulemaking to implement section 1033 of the Dodd-Frank Act (1033 NPRM) reasoned that fee restrictions on data providers are permissible because "prolonged negotiations about fees could delay or obstruct third parties being granted access expeditiously to data providers' developer interfaces, in turn undermining the core consumer data access right."[24] This reasoning applies just as much to the fee negotiation between data aggregators and third parties, a concern which the CFPB dismissed in the PFDR Rule, claiming that "data aggregators are service providers chosen by authorized third parties, who can select a different aggregator for price reasons—or connect to the data provider directly. As a result, competition should naturally put downward pressure on fees that aggregators charge third party clients."[25] The CFPB's conclusion is anything but natural, as differently sized data providers and third parties will have different levels of bargaining power vis-à-vis large data aggregators.

Moreover, the PFDR Rule failed to consider that fees for APIs are a necessary attribute for innovation, maintenance, data security, and fraud prevention. Without the ability to charge fees for the development and maintenance of APIs, data providers will be unable to make the same level of technological investments that lead to innovation and useful financial products and services. For years, banks have had the right to charge fees to data aggregators in their mutually agreed upon contracts; however, banks decided not to

[23] Required Rulemaking on Personal Financial Data Rights, *supra* note 3, at 90884.
[24] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74814 (Oct. 31, 2023), *available* here.
[25] Required Rulemaking on Personal Financial Data Rights, *supra* note 3, at 90838.

as a *business decision* as the industry evolved to incentivize the use of APIs instead of screen scraping. However, choosing not to exercise a right at particular point in time does not mean an entity loses that right, and it would be unreasonable for any industry to premise their business model on other entities offering a good or service for free in perpetuity.

Further, the marketplace itself has demonstrated in practice that data providers can charge reasonable fees to data aggregators while still ensuring all relevant parties maintain appropriate access to data.[26] Such arrangements have not obstructed consumers' access to their data or data sharing arrangements with third parties. A recent, first-of-its-kind negotiation between one large data provider and one large data aggregator –two of the most complex participants in the data access ecosystem – lasted for only two months,[27] during which data sharing was not disrupted. Future negotiations between equally or less complex parties based on this model will likely take less time. Moreover, if that negotiation was not accompanied by any obstruction of access to data, it is unlikely that future negotiations would cause such obstructions.

Q11. What is a reasonable range of estimates regarding the fixed costs to "covered persons" of putting in place the standards required by sub-section D of section 1033 and the operational architecture to intake, document, and process requests made by consumers, including natural persons and persons acting on behalf of a natural person (i.e., an agent, trustee, or representative)? How do these estimates vary by the size of the covered financial institution?

As a threshold matter, Congress has traditionally been explicit when it wants a government agency to engage in price controls.[28] It has not done so in section 1033 of the Dodd-Frank Act. Moreover, fixed costs to "covered persons" are not the correct lens through which fees for data access should be assessed. It is rare for any business to price their services at cost. Indeed, the value of data access is set by the competitive market, driven by the actions and pricing of third parties and data aggregators accessing consumer data. The value of data access is also influenced by the degree to which data providers can offer secure, reliable, always accessible, quick access to customer data;

---

[26] *See, e.g., JPMorganChase and Plaid announce an extension to their data access agreement for sharing of consumer permissione*d data, Press Release, JPMORGANCHASE (Sept. 16, 2025), *available* here.

[27] *See Plaid and JPMorgan Reach Customer Data Sharing Agreement*, PYMNTS (Sept. 16, 2025), *available here* ("The agreement comes a little more than two months after JPMorgan announced it would begin charging FinTechs to access customer banking information.").

[28] *See, e.g.*, 15 U.S.C. § 1691(e)(4) (requiring creditors to provide a copy at no additional cost to the applicant of each written appraisal or valuation developed in connection with the applicant's application for a loan that is secured or would have been secured by a first lien on a dwelling); 15 U.S.C. § 1639h(b)(2)(B) (prohibiting charging applicants the cost of a second appraisal that a creditor must obtain from a different certified or licensed appraiser in connection with certain higher-risk mortgages). *See also* 42 U.S.C. § 1320f (directing the Secretary of Health and Human Services to establish a Drug Price Negotiation Program to, among other things, renegotiate maximum fair prices for selected drugs).

faster, more reliable access to customer data is inherently more valuable to the marketplace than slower, less reliable access. Additionally, certain data elements offered by data providers are more valuable to downstream third parties than others, as evidenced by the different prices charged by data aggregators to their downstream customers for certain data elements. Typically, data used to power financial tools—such as transactions and balances—is priced lower by data aggregators than data that can be used to effectuate payments, even though the costs to access these different types of data are the same.

In the beginning of the data access ecosystem, data aggregators did not pay to access data provider infrastructure, instead relying on screen scraping,[29] which is an inherently unsafe practice. Screen scraping can result in consumer harm because it eliminates any tailoring of the consumer's authorization, potentially allowing third parties to access more information than the consumer intended. Moreover, screen scraping requires consumers to share their access credentials with third parties, creating the risk that these credentials could be misused or compromised. Banks paved a way for safer data use by developing APIs that enabled data aggregators to access the *appropriate* amount of data as requested by the consumer. Some banks even use tokenized account numbers (TANs) to further protect the data; if a TAN were to be obtained by malicious party, the bank could discontinue the TAN then issue a new one, rather than having to close the deposit account. APIs provide a safer alternative to screen scraping and CBA has advocated for the CFPB to pursue action that would efficiently and meaningfully prohibit the practice.[30]

Below are some of the upfront and ongoing costs, along with fixed and variable costs, reflecting the investments banks have made to create a thriving data access ecosystem:

- *Technology costs*, which include software development, product management, production management, infrastructure costs, analytics, screen scraping blocking algorithms, and other personnel to support the developer interface;

- *Cyber and security costs* to protect customer data and secure interfaces;

- *Third-Party Risk Management (TPRM) costs* as data providers adapt to an increased number of third parties connecting directly and to a potential increase in the scope of activities for third party oversight;

- *Fraud costs* as data providers face increased fraud events due to the sharing of data, including, but not limited to, sharing of payment initiation information if ultimately required by the CFPB, under the PFDR Rule;

- *Operational, customer support, and third-party support costs*, which include

[29] "Screen scraping" refers to the use of consumer credentials by a third party to log into banks' websites millions of times daily to pull consumer data.
[30] CBA, *supra* note 6.

enabling direct integrations, legal and compliance activities, addressing and resolving issues raised by customers and third parties, managing any data breaches, and complying with numerous operational requirements in the PFDR Rule; and

- *Costs stemming from downstream uses of shared data*, as certain use cases will have their own additional costs associated with each particular use case (e.g., the costs related to resolving claims from ACH debits enabled by data sharing).

Q12. What is a reasonable range of estimates regarding the marginal cost to covered financial institutions of responding to requests made under the auspices of section 1033? How do these estimates vary by the size of the covered financial institution?

As detailed in the response to Q11, costs are not the correct lens through which fees for data access should be assessed. It is vital to remember that businesses in a free-market economy do not price their services at cost. The costs for data access will necessarily be related to the value of such data in the market, as well as the manner in which the data is provided and protected. To the extent the CFPB considers costs in connection with fees for data access, it should look to: (i) technology costs; (ii) cyber and security costs; (iii) TPRM costs; (iv) fraud costs; (v) operational, customer support, and third-party support costs; and (vi) costs stemming from downstream uses of shared data.

Q13. How is the range above affected by the need of the "covered person" to confirm that an agent, trustee, or representative acting on behalf of an individual has actually been authorized by the consumer to act on their behalf?

In light of the ever-growing, ever-evolving scope of fraud and hacking, data providers must be able to protect their customers' sensitive financial data by confirming directly with the consumer who they are (i.e., capture authentication) and what they want to share (i.e., confirm authorization) before sharing data with any third party. It is important for data providers to have the *right* to capture authentication and confirm authentication directly, rather than rely on information or attestations from the third party only.

This approach would be consistent with current marketplace practices. In the current ecosystem, data providers confirm authorization because they are in the best position to know what accounts the customer has and share the applicable data categories. Moreover, data providers function as the customer's system of record; whereas entities accessing customer data can subsequently simplify or modify consumer information, such as by creating a combined view for consumers of their data across multiple sources, the originating data provider for that data retains the original information and is ultimately the consumer's source for confirmation of the base data. As such, data

providers must retain the ability to capture the customer's authentication and confirm the authorization directly from the consumer.

Q14. Is there any legal precedent from other Federal statutes, not involving Federal criminal law or provision of services by the U.S. Government, where there is a similar omission of explicit authorization to the agency to set a cost sharing balance in effectuation of a new statutory right and, if so, what principles has the court allowed the agency to use in establishing a proper balance?

As discussed in the response to Q9, Congress has historically explicitly delineated when it seeks to prohibit fees, including when the Fair and Accurate Credit Transactions Act[31] amended the FCRA to provide consumers with a right to receive one free credit report every year[32] and when the Credit Card Accountability Responsibility and Disclosure Act[33] amended the Truth in Lending Act[34] to, among other things, outline requirements related to late fees[35] and prohibit certain types of fees, such as double-cycle billing and penalties for on-time payments.[36] Moreover, as noted in the response to Q11, Congress has traditionally been explicit when it wants a government agency to engage in price controls.[37]

Q15. Absent any legal precedent from other laws, should covered persons be able to recover a reasonable rate for offsetting the cost of enabling consumers to exercise their rights under section 1033? Why or why not?

As summarized in the responses to Q9 and Q10, the CFPB does not have the authority to prohibit fees, and doing so would harm both consumers and the competitive market. Covered persons should be able to charge third parties and data aggregators that profit from consumers' data. This is because material costs will be incurred by data providers in building and maintaining the necessary API platform, including appropriate oversight and governance of third parties and data aggregators, as detailed in the response to Q11. Furthermore, as outlined in the response to Q10, nothing in the text of Section 1033 of the Dodd-Frank Act prohibits data providers from imposing fees on third parties and data aggregators—let alone fees intended to offset costs. As described in the response to Q9, prohibiting data providers from charging fees would result in a windfall for data aggregators at the expense of data providers, consumers, and the broader market. Permitting data providers to impose fees on third parties and data aggregators could also incentivize data minimization by deterring excessive or abusive API consumption

[31] *See* Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. § 1681-1681x.
[32] *See* 15 U.S.C. § 1681j(a).
[33] *See* Public Law 111-24, 123 Stat. 1734 (2009).
[34] *See* Public Law 90-321, 82 Stat. 146 (1968).
[35] *See* 15 U.S.C. § 1637(b)(12).
[36] *See* 15 U.S.C. § 1637(j).
[37] *See supra* note 28.

patterns and encourage third parties and data aggregators to only seek data truly needed to provide the given product or service.

Q16. If covered persons should be able to recover a reasonable rate for offsetting the costs of enabling consumers to exercise their rights under section 1033, should the Bureau place a cap on the upper bounds of such rates that can be charged? If so, what should the cap be on such rates, and why? If not, why not?

No, the CFPB should not place a cap on the upper bounds of any data access fees by data providers. Each data provider operates under different circumstances and will have unique considerations in setting costs for API access. They should have the freedom to set rates that reflect the volume and type of API access they experience. Such prices will be set at a reasonable rate as data providers seek to compete in the marketplace, which has over 4,000 banks[38] competing with an ever-expanding selection of nonbanks. This principle should apply equally to all participants in the market: just as the CFPB should not impose limits on what data aggregators and third parties may charge for products and services that support consumer-permissioned data sharing, it should likewise refrain from capping the fees data providers may charge aggregators and third parties.

From an economic perspective, a government agency setting pricing rates in a nascent market can have damaging, unintended consequences. Data sharing through APIs is still an emerging market, and key factors—such as the extent of consumer adoption, the volume of API calls data providers will handle, and the dominant use cases for consumer data—remain uncertain. As emerging technologies, such as agentic artificial intelligence (AI), continue to reshape this ecosystem, imposing fixed costs on data providers at this early stage could distort the market and disincentivize investment.

Q17. If consumers ought to bear some of the cost in implementing requirements under section 1033, should that be shared by every consumer of a covered person, including those who may not wish to exercise their rights under section 1033?

As a matter of business practice, individual consumers may not be required to bear the costs associated with implementing the requirements of, or exercising their rights under, section 1033 of the Dodd-Frank Act. Data providers should be permitted to impose fees on data aggregators and authorized third parties that access consumers' data through an API. Nonetheless, data aggregators may make the business decision to charge fees to third parties, which could ultimately be passed on to consumers, as discussed in the response to Q9.

[38] *See* FED. DEPOSIT INS. CORP., *Insured Institutions Report Return on Assets of 1.16 Percent and Net Income of $70.6 Billion in the First Quarter* (May 28, 2025), *available* here (indicating the data in the Q1 2025 Quarterly Banking Profile is from 4,462 insured commercial banks and savings institutions).

Generally speaking, consumers using a particular service should bear the associated costs. These costs should not be distributed across all individual consumers, including those who are not exercising their rights under Section 1033. If a consumer is to be charged, it should be by the entity from which they are procuring a good or service (i.e., the third party), which is also profiting from secondary uses of that consumer's data, not by the entity holding their data (i.e., the data provider). Furthermore, consumers have no control over system-level costs and cannot influence or limit the volume of aggregated API calls.

Information Security (Questions 18-29)

Q18. Does the PFDR Rule provide adequate protections for the security of consumer's data? Why or why not?

No, the PFDR Rule fails to provide adequate protections for the security of consumer's data in two key respects: (i) it fails to prohibit screen scraping; and (ii) the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule is principles-based so the actual implementation of the safeguard is what matters and data providers have a limited ability to evaluate the security of third parties and data aggregators. For each of the foregoing, it is vital that at least the largest data aggregators and third parties are actually examined by the CFPB for their compliance with these obligations.

Screen Scraping: As discussed more in Q11, screen scraping is a fundamentally unsafe method of access that can result in consumer harm because it exposes consumers' credentials to greater risk of being misused or compromised, and because it eliminates any tailoring of the consumer's authorization, potentially allowing third parties to access more information than the consumer intended. The PFDR Rule does not actually prohibit or meaningfully limit the use of screen scraping by third parties. As CBA explained in its response to the 1033 NPRM, "[a]bsent an express prohibition, it would be unduly costly for data providers to effectively block screen scraping and push usage of safer APIs."[39] A reconsidered version of the PFDR Rule must take more meaningful steps toward ending the unsafe practice of screen scraping. For example, the CFPB could explicitly state that, since entities engaged in screen scraping of data they could access through secure APIs demonstrate inadequate concern for consumers' data privacy and the principles of data minimization, (i) it constitutes a "reasonable denial" for data providers to block a data aggregator's or third party's access to the API if that aggregator or third party attempts to use screen scraping to access information already made available through the API, and (ii) it is reasonable risk management for the data provider to proactively block screen scraping attempts by such aggregators or third parties.

[39] CBA, *supra* note 6.

GLBA Safeguards Rule: As discussed further in the responses to Q26 and Q27, the information security standards in the GLBA Safeguards Rule are principles based. Imposing them on data recipients without corresponding supervision to ensure adequate practices are actually implemented does not sufficiently safeguard individual consumers' data. Currently, data providers rely on data access contract terms to ensure third parties handle consumers' data securely. In practice though it is difficult for data providers to substantiate the ongoing adherence of each relevant third party to these contractual requirements. It is vital that data providers be able to retain their ability to require, via these bilateral contracts, that third parties meet the necessary information security obligations as a precedent condition for accessing the data provider's API.

Fundamentally, the data security shortcomings in the PFDR Rule, as well as the privacy issues discussed below, would be best addressed with revisions to the current rule and by the CFPB exercising its authority to directly supervise at least the large fintechs and other third-party providers, especially data aggregators. Otherwise, the proliferation of consumer financial data across a network of effectively unsupervised entities could lead to significant consumer harm, even from a single data breach.

Q20. How do the fixed costs above relate to the number of clients serviced by the covered person or a person acting on behalf of an individual consumer? Is the market providing reasonably priced solutions to meet the provisions of the PFDR Rule for covered persons with few customers?

Given the volume of data that will be shared by data providers, increased security investments will be necessary due to the heightened risk exposure, as consumer data will be increasingly shared with various parties outside the well-regulated and protective environment of the data provider. These security investments—intended to safeguard consumer data—are distinct from the resilience measures implemented by data providers to ensure the stability and scalability of their data-sharing infrastructure.

Q21. In what way does the existence or non-existence of a fiduciary relationship affect the incentives in doing cost-benefit analysis regarding the level of information security established?

The existence of a fiduciary relationship shifts the incentives away from a primarily business-centered approach to one that focuses on the customer by placing a duty to act in the best interest of the client on the fiduciary. Third party data recipients in the open banking context are not currently *explicitly* subject to this duty under the PFDR Rule. Given that all fiduciaries are obligated to act in their clients' best interests, fiduciaries in open banking should be expected to engage in practices such as: (i) prioritizing customer understanding of who their data is being shared with and how it is being used; (ii) ensuring informed consent for data sharing; (iii) implementing robust security measures (e.g., encryption, tokenization, validation) to protect customer data and minimize the risks associated with data sharing; and (iv) promoting data minimization.

Q23. In the case of large-scale data breaches, what is the general cost per client in protecting such clients from the risks created by the breach, and how well-cushioned must working capital reserves be to respond to such breaches?

It is difficult to provide a per-customer cost to remediate harm and protect consumers in the event of a data breach, as the facts and circumstances of each breach are unique. In fact, the time delay between a credential breach and a subsequent attack could be days, months, or years. It could be years before fraudsters use credentials from an attack to defraud individual banks, and nearly impossible to trace back. The risk of loss in the data sharing context is significant, given the vast amounts of data involved, the ways in which this data can be misused (e.g., account takeover, fraud, money movement), and the extensive corrective actions that may be required by the data provider to address any misuse (e.g., new card issuance, new demand deposit account issuance, call center/customer support involvement). The working capital reserves for responding to data breaches held by every data provider also vary, and depend on factors including the nature of the data provider's business, whether the data provider holds insurance for data breaches, the type and volume of data being shared by the data provider, and any contractual indemnification provisions the data provider may have in its third party agreements. While the exact costs of individual large-scale data breaches will vary, a recent IBM report summarizes that the average cost of a data breach in the United States was $10.22 million, an all-time high for any region in the world.[40]

As CBA has previously articulated,[41] including in response to Q7, any reconsidered PFDR Rule must allocate liability when data is shared between permissioned parties such that the party responsible for loss is responsible for redress. Liability of data providers for any incident leading to loss or harm should end when the data leaves the data provider's portal, since the data provider in that instance is no longer in the best position to prevent the harm from occurring. Third parties and data aggregators must assume liability for instances in which they are best positioned to prevent harm to consumers (including in instances when those entities suffer a data breach) and be adequately capitalized to make good on their liability obligations to consumers. Clarifying liability obligations in such a manner would also encourage all market participants to ensure they have appropriate security controls and safeguards in place to protect consumer data.

---

[40] IBM, *Cost of a Data Breach Report 2025 – The AI Oversight Gap* 6 (Jul. 2025), *available* here.
[41] *See, e.g.*, CBA, *supra* note 6 (Part VIII discusses liability allocation in-depth, and argues that the PFDR Rule should: (i) explicitly state liability rests with the response third party or data aggregator if a consumer's credentials are misused to initiate a fraudulent transaction by such party or are impermissibly acquired by another actor through a data breach the party experienced; (ii) mandate third parties and data aggregators be adequately capitalized and carry sufficient indemnity insurance to satisfy liability obligations; and (iii) obligate third parties to certify as part of the certification statement that they are adequately capitalized, have accepted their liability obligations, and are carrying sufficient indemnity insurance).

Q24. What has been the experience of covered persons with secure storage and transmission of consumer financial data and how effective have such institutions been in establishing controls and information security protocols?

In general, industry is continuing to make advances, but has still not fully adopted security best practices, such as broad tokenization, encryption of data both at rest and in transit, and key data management practices. While entities like the Financial Data Exchange (FDX) have implemented in-transit security standards, not all entities implement these standards, and non-standard implementations of OAuth continues to hinder the security of the data access ecosystem as a whole. Controls and information security protocols also must contend with emerging threats, such as AI and machine learning. Not all data providers will be invested in cybersecurity to the same degree, nor will all entities be able to remediate breaches with the same speed. Greater adherence across the marketplace to security standards will improve the security of the data access ecosystem in the United States.

Q25. Covered persons are subject to several legal obligations regarding risk management, such as safety and soundness standards, Bank Secrecy Act (BSA) requirements, and Anti Money Laundering (AML) regulations. What should covered persons consider under these legal obligations when making information available to consumers? How could the PFDR Rule's interface access provision better allow covered persons to satisfy these legal obligations?

Data provider banks are subject to several legal obligations regarding risk management, including safety and soundness standards, BSA requirements, and AML regulations. The applicability of these obligations, though, depends on the interpretation of the term "consumer."

If the consumer refers to an individual consumer, then no additional considerations are necessary, as individuals already undergo "Know Your Customer" (KYC) assessments and are subject to existing controls. These frameworks are well established and sufficient to satisfy risk management and compliance requirements.

As summarized in response to Q1, the term "consumer" should not encompass third parties and data aggregators. However, if the CFPB determines the term "consumer" does encompass these entities, there are significant third- and fourth-party risk management questions that will need to be addressed, including: (i) who these companies are controlled by, (ii) where these companies store data they access, (iii) whether a controlling influence of the company could compromise data security, (iv) what industry these companies primarily conduct business in; and (v) what the data is being used by the company for.

Data providers need clearer guidelines than what the current PFDR Rule provides on TPRM practices. Indeed, the PFDR Rule implicates both a data provider's ability to deny access pursuant to risk management concerns, as well as a data provider's role in confirming a third party's compliance. It also raises interagency TPRM concerns, such as the expectations for banks to conduct TPRM under interagency guidance and the extent to which bank TPRM obligations extend to downstream parties. While certain actions, like liability rules or tokenization may help decrease some risks, TPRM can further assist in meaningfully mitigating some of these risks, including:

- Identity theft leading to scams;
- Takeover of a third-party account, leading to disputes;
- Unauthorized transactions resulting from either data theft or a fraudulent app;
- Security breach and account closure;
- Overcollection of data/privacy violation/loss of trust;
- Authorized transactions that are disputed; and
- Mass data breaches that create reputational risks.

CBA recommends that TPRM guidance pertaining to third parties receiving data under the PFDR Rule should be clear and consistent across all regulators to support predictability and reduce friction. Specifically, CBA suggests TPRM guidance should:

- Support bank discretion to implement risk management programs and allow denials of access based on reasonable risk concerns defined holistically;
- Harmonize requirements under the PFDR Rule[42] with existing interagency guidance on TPRM, which permits institutions to manage risks broadly, including potential and emerging risks, across all operational areas;
- Permit data providers to evaluate third parties' risk management practices before sharing data with such third parties, and affirm that denying access for valid risk concerns – beyond data security and consistent with interagency TPRM guidance – is *per se* reasonable;

[42] To facilitate a data provider's evaluation of data aggregators and third parties from a risk management perspective, a revised PFDR Rule should explicitly require entities accessing consumer data through the API to disclose to the data provider *before* accessing any data: (i) the specific use cases for which the customer has provided authorization, (ii) the entity's role in the transaction (whether the entity is a data aggregator or an authorized third party), and (iii) whether any additional downstream fourth parties will access or use the consumer data.

- Reaffirm that third parties and data aggregators are not agents of data providers and may warrant a different approach to TPRM, particularly because data providers cannot easily in the onboarding process refuse to have a relationship with a third party under the PFDR Rule without increasing the risk of violating the rule; Indicate data providers are not responsible for conducting ongoing oversight of every data recipient or data aggregator that access the data provider's API; and

- Indicate that if a data security incident occurs at a third or fourth party, that entity has the obligation to inform the data provider.

Q26. What are the costs and benefits of the PFDR Rule's reliance on existing information security standards in the GLBA?

The information security standards in the GLBA Safeguards Rule are principles based. Imposing such principles-based standards on data recipients without corresponding supervision to ensure adequate practices by the third parties does not sufficiently safeguard individual consumers' data. Currently, data providers rely on data access contract terms to ensure third parties securely handle consumers' data; nevertheless, it is practicably difficult for data providers to substantiate the ongoing adherence of each relevant third party to these contractual requirements. It is vital that data providers be able to retain their ability to require, via these bilateral contracts, that third parties meet the necessary information security obligations as a precedent condition for accessing the data provider's API.

Q27. To what information security standards ought entities adhere when accessing consumer financial data held by a covered person, and who is best positioned to evaluate whether these entities are adhering to such standards?

The GLBA, Interagency Guidelines Establishing Information Security Standards[43] (Appendix D-2 to Part 208) and the FFIEC IT Examination Information Security Booklet[44] provide critical baseline guidance for third parties and data aggregators accessing consumer data held by a data provider. Specific information security control objectives are further outlined in the Cyber Risk Institute Profile.[45] To achieve these objectives, entities should follow standards like the FDX security model and related FDX standards, which draw on:

- National Institute of Standards and Technology (NIST) information security

[43] 12 C.F.R. Appendix D-2 to Part 208 (2025), *available* here.
[44] FED. FIN. INST. EXAMINATION COUNCIL, *FFIEC Information Technology Examination Handbook – Information Security* (Sept. 2016), *available* here.
[45] *See* CYBER RISK INST., *Our Cyber Profile for the financial sector is a global standard for cyber risk assessment*, *available* here.

special publications such as NIST SP 800-53[46] and NIST SP 800-63;[47]

- Internet Engineering Task Force (IETF) standards such as IETF RFC 5246,[48] IETF RFC 8446,[49] and IETF RFC 9470;[50] and

- Strengthened and adapted IETF and OpenID Foundation (OIDF) standards such as IETF RFC 6749,[51] IETF RFC 9700,[52] and OIDF FAPI 2.0.[53]

The responsibility for evaluating and ensuring adherence to security standards should be divided among Federal regulators–which should continue their existing supervision of "covered persons"–and independent, licensed and accredited third-party auditors–who can assess third parties and data aggregators for compliance with security standards, in addition to any relevant examination that may occur of data aggregators and third parties by the CFPB.[54] Additionally, data providers should be able to establish bilateral contracts with data aggregators that clearly address individual obligations and responsibilities of both downstream parties and the data aggregator itself. These contracts can afford the parties to address concerns like data security and liability for the data provider, the data aggregator, and downstream third parties.

Q28. What are the costs and benefits of the PFDR Rule's provisions designed to reduce the use of screen scraping? What changes would better protect the security of consumer credentials?

As discussed in the responses to Q11 and Q18, screen scraping is a fundamentally unsafe method of access that can result in consumer harm because it exposes consumers' credentials to greater risk of being misused or compromised, and because it eliminates any tailoring of the consumer's authorization, potentially allowing third parties to access more information than the consumer intended. AI, and the advent of third-party AI agents as autonomous interactors who can log into consumer accounts and take action on behalf of the consumer vis-à-vis that account, exponentially increases the risks associated with screen scraping. While banks have made significant investments in data scanning, analysis, and remediation technologies to manage the proliferation of screen

---

[46] NAT'L INST. OF STANDARDS AND TECH., NIST SP 800-53 REV. 5, SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS (2020), *available* here.
[47] NAT'L INST. OF STANDARDS AND TECH, NIST SP 800-63, DIGITAL IDENTITY GUIDELINES (2025), *available* here.
[48] *See RFC 5246*, INTERNET ENGINEERING TASK FORCE (Aug. 2008), *available* here (obsoleted by RFC 8446).
[49] *See RFC 8446,* INTERNET ENGINEERING TASK FORCE (Aug. 2018), *available* here.
[50] *See RFC 9470,* INTERNET ENGINEERING TASK FORCE (Sept. 2023), *available* here.
[51] *See RFC 6749,* INTERNET ENGINEERING TASK FORCE (Oct. 2012), *available* here.
[52] *See RFC 9700,* INTERNET ENGINEERING TASK FORCE (Jan. 2025), *available* here.
[53] *FAPI 2.0 Security Profile,* OPENID FOUNDATION (Feb. 22, 2025), *available* here.
[54] Such reports from independent, licensed, and accredited third-party auditors on third parties and data aggregators could also be used by financial institution data providers in their own safety and soundness assessments.

scraping so as to protect consumers and their data, screen scrapers continue to find alternative methods to counteract these efforts. For example, entities may instead engage in data scraping via Interactive Voice Response systems. As CBA informed the CFPB in response to the 1033 NPRM:

> "Even for the largest data providers, it is complicated and expensive to differentiate and block automated web scraping while not inadvertently blocking real consumer traffic. Given the important focus on customer service, data providers generally err on permitting traffic rather than blocking real customer access. Distinguishing between the two has only become more difficult as third parties now regularly modify their automated scripts to appear more human and bypass efforts to restrict screen scraping. Efforts to counter screen scraping are akin to addressing each attempt individually as they occur."[55]

To that end, CBA recommends that the CFPB in a reconsideration of the PFDR Rule:

- Prohibit credential-based access and screen scraping by third parties and data aggregators once a data provider has enabled API access;

- Explicitly acknowledge a data provider's right to block credential-based access and screen scraping once the data provider has an API that third parties and data aggregators can use; and

- Prohibit screen scraping by third parties for access to information not defined as "covered data" under the PFDR Rule.

Q29. Does the PFDR Rule provide adequate protections for consumers and covered persons to ensure that the request for a consumer's information is in fact knowingly authorized by the individual consumer and that the information is in fact being made available to the consumer as opposed to a malicious actor?

Generally CBA is supportive of the authorization disclosure requirements of the PFDR Rule. Nevertheless, the CFPB should remain aware that there are onboarding complications that could result in malicious actors requesting consumer data.

In the case of a third party integrating directly with a data provider, there is an onboarding process in which the data provider integrates the data provider into their API sharing process, which necessarily means such entities are not able to access consumer data immediately.

However, data aggregators could potentially onboard malicious actors as third-party data recipients, thereby putting consumer data at risk downstream. Currently, data providers must rely on data aggregators to assess the risk levels of any third-party data

[55] CBA, *supra* note 6.

recipient. While data providers may conduct a content review to flag anything suspicious about a third-party data recipient, the rigorous oversight criteria imposed on data aggregators are often assumed to extend to these third parties, regardless of their actual legitimacy. In such cases, the data aggregator is in contractual privity with the third-party data recipient, but the data provider is not. Given this unique arrangement, the CFPB should ensure that data aggregators have adequate regulatory incentives to vet third-party data recipients thoroughly to confirm they are not malicious actors and to ensure they adhere to industry best practices.

Data Privacy (Questions 30-34)

Q30. Does the PFDR Rule provide adequate protection of consumer privacy? Why or why not?

CBA supports the consumer protections under the PFDR Rule pertaining to access, use, sharing, sale, and deletion of data. These secondary uses often stem from consumer misunderstandings. For example, disclosures may be buried in the terms of service that are read by very few consumers, and fully understood by even less. As a result, consumers may think they are granting access for one purpose, but unknowingly are consenting to the use of that data for some other purpose beyond their initial intent. Additionally, CBA supports the PFDR Rule's inclusion of fraud and product improvement uses as reasonably anticipated uses of a consumer's data by authorized third parties only.[56] There remain two key areas where the CFPB could provide clarity to further enhance consumer protection and privacy: (i) consumer consent and revocation, and (ii) data aggregator access to and practices with consumer data.

Consumer Consent and Revocation: Data sharing is not a one-time event – it is a lifecycle, starting with the initial request to share data, the use of that data, and then the eventual decision to stop sharing that data. Any revised PFDR Rule must consider the customer's ability to control their data throughout the data sharing lifecycle. This means consumers need to be informed about the nature of the data sharing at the outset of the initial request. There must also be a clean break when the customer no longer wishes to use the service offered by an authorized third party. Customers should be able to give, and data providers should be able to capture, explicit consent for third parties to use specific data from specified accounts. Customers should also be able to easily revoke access for each account and each third party at any time without friction or delay. Such circumstances can easily occur, as CBA has previously noted: "There could be reasons for any particular consumer that they may initially consent to sharing deposit account and credit card covered data, then at a future time may wish to no longer share data from one of those accounts (i.e., a consumer may initially consent to sharing deposit account and credit card covered data, then later change their mind with respect to only the credit card covered data)."[57]

---

[56] *See* Required Rulemaking on Personal Financial Data Rights, *supra* note 3, at 90996.
[57] CBA, *supra* note 6.

Data Aggregator Access and Practices: The CFPB must revisit the PFDR Rule's approach to data aggregator access to and practices with consumer data. Data aggregators should be prohibited from (i) keeping copies of consumer data, and (ii) monetizing consumer data without their explicit consent.

- *Data Aggregators Should be Prohibited from Keeping Copies of Consumer Data*: Data aggregators function as intermediaries to collect consumer data on behalf of authorized third parties engaged by consumers. Consumers do not proactively choose to engage in data sharing with authorized third parties with the intention of having their data be used by an unrelated entity in perpetuity. Some data aggregators collect consent from consumers to use consumer data for the data aggregator's own separate purpose, unrelated to the product or service the consumer is seeking from the authorized third party. These data aggregators may utilize consumer data to derive their own insights about consumers, which then may be sold by the data aggregator. Consumers often will not be aware of this, though, because the consent form is presented during the account linking flow when the consumer is connecting another, downstream app to their data provider. Even if the consumer *does* realize that a data aggregator will be accessing their data, the consumer may often forget who the data aggregator is or how to revoke that data aggregator's distinct access or use of the consumer's data. If the CFPB wishes to preserve data privacy, consumer data collected by data aggregators for the primary purpose of passing data from a data provider to an authorized third party should be promptly deleted by the data aggregator.

- *Data Aggregators Should be Prohibited from Monetizing Consumer Data without their Explicit Consent*: Consumers are generally unaware of how their data is being used by data aggregators, including whether their consumer data is being sold by data aggregators.[58] While the value-added services provided by data aggregators may be appealing to some consumers, consumers must be aware of what they are actually consenting to and how their data is being monetized, particularly by entities the consumer has no direct relationship with. When individual consumers share data with fintechs and other third-party providers, they do so for the express product or service offered by those entities. Individuals do not contemplate the ongoing use and sale of their data by the intermediary.

Q31. How prevalent is the licensure or sale of consumer financial data by bank and non-bank financial institutions, where customers either have the right to opt into or opt out of having their data licensed or sold? What is the approximate balance between such regimes where the customer is given a choice?

[58] *See, e.g., 2021 Consumer Survey: Data Privacy and Financial App Usage,* THE CLEARING HOUSE (Dec. 2021), *available* here ("Only 24% know that these data aggregators can sell personal data to other parties for marketing, research, and other purposes").

As further discussed in Q30, CBA is supportive of the consumer protections under the PFDR Rule pertaining to access, use, sharing, sale, and deletion of data.

However, *if* a reconsidered version of the PFDR Rule were to permit the licensure or sale of data, it is imperative that such regime requires consumers to *opt in* to having their data licensed or sold, rather than permitting consumers to opt out. Moreover, any such regime should ensure that consumers are fully aware of how their data is being used and sold, and should contain key guardrails including that: (i) use of the service cannot be conditioned by the authorized third party on the consumer opting in to having their data licensed or sold, which must be clearly indicated to the consumer; (ii) the authorized third party must provide be an easy method for consumers to subsequently opt out of having their data licensed or sold, and such method must not result in a termination of the underlying service offered by that third party; (iii) consumers must have notice of who their data is being licensed or sold to; and (iv) entities that an authorized third party licenses or sells consumer data to cannot resell or further disseminate that consumer's data.

Compliance Dates (Questions 35-36)

Q35. Have entities encountered unexpected difficulties or costs in implementing the PFDR Rule to date?

Yes, as CBA has informed[59] the prior CFPB leadership, the PFDR Rule significantly underestimates the ease with which a third-party access portal in the form of an API can be developed and implemented by data providers. Data providers in the data access ecosystem are in a true conundrum: while they know that the PFDR Rule is likely to be revised, as things stand today, they are still obligated to comply with the soon-to-be-outdated PFDR Rule starting June 30, 2026 for the first tranche of entities.[60] As a result, these data providers will need to make significant investments and decisions *now* to comply next year with the PFDR Rule *of today* while knowing that, at some point in the future, the PFDR Rule will be substantially revised, thereby negating or requiring even further costly changes to systems implemented to comply with current PFDR Rule. In light of the foregoing, the CFPB has good cause[61] to immediately issue an interim final rule extending the compliance dates for the current PFDR Rule a minimum of one year pending the finalization of the CFPB's re-proposal of the rule, inclusive of a final

[59] CBA, *Letter re: Feedback on Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights - Outline of Proposals and Alternatives under Considerations* (Jan. 25, 2023), *available* here; CBA, *supra* note 6.
[60] The first compliance dates under the PFDR Rule were initially set for April 1, 2025, though the compliance dates were stayed 90 days pursuant to a court order, and thus the first compliance date is now June 30, 2026. Personal Financial Data Rights Reconsideration, 90 Fed. Reg. 40986, 40989, fn. 11 (Aug. 22, 2025), *available* here.
[61] *See* 5 U.S.C. § 553(b)(B).

resolution of the litigation[62] regarding the rulemaking, or suspending the compliance dates altogether.[63]

Many data providers, small and large alike, do not currently have an API, and for even many of those data providers that do have APIs, their APIs do not have capabilities to provide the large swath of consumer information with authorized third parties and data aggregators as required under the PFDR Rule. The cost of developing or modifying these APIs will be immense, and maintenance costs for these systems will skyrocket following the expected exponential increase in data requests once the compliance dates for the current PFDR Rule pass. These changes are not simple; data providers require significant time and resources to build their systems to comply with the PFDR Rule.

These activities include:

- Establishing *internal connections* within the institution to facilitate implementation of open banking;
- *Identifying* the data that would need to be shared;
- *Identifying any compliance gaps* that an institution may have for such data between their current functionalities and the requirements of the rule;
- *Mitigating any identified compliance gaps* to come into compliance with the requirements of the rule;
- *Compiling the relevant data fields into API-structured formatting*, since many data fields may only be available in older, structurally different technologies;
- *Optimizing systems for internal API pulls* to gather the relevant data when faced with an external pull request, since each API pull will likely result in multiple internal API pulls; and
- *Optimizing systems for external API pulls* to ensure that data is delivered consistent with relevant uptime and response times.

As illustrated by the list above, not only will developing or modifying APIs take more time than contemplated in the PFDR Rule, but the changes necessitated by the PFDR Rule will involve diverse internal parties at every institution, including, but not limited to a range of stakeholders from organizations representing the Legal, Compliance, Risk,

[62] *See generally* Joint Status Report, Forcht Bank, N.A. v. Consumer Fin. Prot. Bureau, No. 5:24-cv-304-DCR (E.D. Ky. May 30, 2025), *available* here (explaining status of the parties in relation to the stay granted on July 29, 2025, in light of the Dodd-Frank Act 1033 ANPR).
[63] *See supra* note 5.

and Technology departments.[64] This will significantly expand the necessary time required to implement changes. These changes will also likely trigger the need for many institutions to engage in new or updated TPRM assessments, which will also significantly expand the minimum implementation time.

These significant compliance hurdles have been exacerbated by delays in industry alignment and standardization around key data elements and documentation required by the PFDR Rule. Although the rule was published in November 2024, the CFPB did not identify a "recognized standard setter" until January 2025.[65] While there has certainly been collaboration among industry, a common understanding of what completely constitutes adequate compliance for all parts of the PFDR Rule has yet to be reached. In particular, the methods of sharing terms and conditions, bill pay information, and authorization disclosures are not yet standardized, and indeed fall outside existing industry-developed patterns. Significant lead time would be required for building a consensus, developing standards, and implementing compliant solutions for these elements.

The above, taken together with the uncertainties caused by the as-of-yet unresolved litigation, has generated significant uncertainty in the marketplace, making it necessary for the CFPB to extend the compliance dates. Moreover, because data aggregators or authorized third parties may alter standardized data shared by data providers into proprietary formats, leading to market distortion and increasing customer switching costs, CBA recommends that the final rule explicitly obligates data providers, authorized third parties, and data aggregators to be compliant with whatever obligations a revised PFDR Rule contains at the same time. As the CFPB itself summarized, "[t]he PFDR Rule did not set explicit compliance dates for third parties that receive data on the grounds that their compliance was functionally tied to compliance by data providers."[66] The CFPB here has a chance to correct that error and ensure all market participants adhere to the same standards, which will promote a fair and competitive data sharing ecosystem.

Q36. If the Bureau were to make substantial revisions to the PFDR Rule, how long would entities need to comply with a revised rule? How would the necessary implementation time vary based on the size of the entity covered by the rule?

As a threshold matter, CBA notes that the required lead time for complying with a substantially revised PFDR Rule will necessarily depend on the nature of the revisions.

---

[64] *See, e.g.*, Consumer Bankers Association et al., *Ex Parte submission – BPI-TCH-ABA-CBA* (Oct. 15, 2024), *available* here (summarizing a meeting on August 7, 2024 between the Consumer Bankers Association, Bank Policy Institute, The Clearing House, and the American Bankers Association and representatives from their member institutions with CFPB staff).

[65] In the Matter of: Financial Data Exchange, Inc., CFPB No. 2024-CFPB-PFDR-0001, (Jan. 8, 2025), *available here*.

[66] Personal Financial Data Rights Reconsideration, *supra* note 2, at fn. 10.

Many of the procedural complexities outlined in Q35 for complying with the current PFDR Rule will also exist for complying with a revised PFDR Rule. For example, data providers will still need to identify the data to be shared, identify and mitigate compliance gaps, optimize their systems for internal and external pulls, etc. Moreover, the completion of a new PFDR Rule will require the relevant "recognized standard setter" to revise its guidance, which will prompt data providers to redo or undo various technical implementations that have already been completed in anticipation of a June 30, 2026 compliance date with the current PFDR Rule.

While the timelines may vary depending on the scale of the changes and each respective data provider's progress toward implementing the PFDR Rule, CBA estimates that approximately 24 months will be needed to comply once the "recognized standard setter" finalizes a standard. For large data providers, compliance with the rule will require extensive work, including, but not limited to:

- Modifying API platforms and related programs to align with new requirements;
- Enhancing public-facing websites to meet disclosure standards;
- Generating and publishing performance metrics that meet the CFPB's definitions;
- Supporting new required data elements (*e.g.*, bill payment data, specific terms and conditions)
- Developing and implementing required policies, procedures, and processes;
- Upgrading technology infrastructure to meet defined API performance standards;
- Building functionality for "machine-readable" consumer-accessible files, if required;
- Managing consumer impacts related to the new maximum access duration limits;
- Operationalizing notice processes for developer interface denials;
- Implementing third-party notifications for consumer access revocations;
- Adjusting customer service operations to reflect new functionalities and scope;
- Conducting robust testing to ensure safe, resilient implementation;
- Updating data access agreements and third-party oversight processes; and
- Addressing the other requirements as outlined in the rule.

Sufficient implementation time is critical not just for data providers to meet their obligations accurately, securely, and with proper controls, but also for data aggregators and third parties accessing these systems to ensure they can do so without experiencing interruptions or other technical issues. For the good of consumers and the health of the data access ecosystem as a whole, it is imperative that market participants have sufficient time to comply with the PFDR Rule's requirements.

* * *

CBA appreciates the opportunity to comment on this Dodd-Frank Act 1033 ANPR, and hopes that its feedback will be incorporated into the CFPB's final determination over how the PFDR Rule should be reconsidered to align with the statutory intent and to ensure a credible, durable final rule.

Sincerely,

/s/
Brian Fritzsche
Vice President, Associate General Counsel
Consumer Bankers Association