www.fdata.global/north-america

October 21, 2025

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

Submitted via electronic mail to 2025-ANPR-PersonalFinancialDataRights@cfpb.gov.

Re: Personal Financial Data Rights Reconsideration, Docket No. CFPB–2025–0037

The Financial Data and Technology Association ("FDATA") appreciates the opportunity to provide comments in response to the Consumer Financial Protection Bureau's ("CFPB" or "Bureau") Advanced Notice of Proposed Rulemaking ("ANPR") on the reconsideration of its Personal Financial Data Rights ("PFDR") Rule, implementing section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("the Dodd-Frank Act").

FDATA has advocated for the CFPB to promulgate a rule affirming consumer financial data rights under section 1033 of the Dodd-Frank Act for years. Our members welcomed the announcement during President Donald Trump's first administration that the CFPB would begin the process of writing a rule, and, though the rule finalized in November 2024 was imperfect, it created a critical, long-overdue foundation for consumer financial data rights in the United States.[1] While FDATA is supportive generally of the Bureau's desire to improve the rule, the Bureau's recent reversals and re-reversals on section 1033, along with intransigence by the nation's largest financial institutions, has created significant regulatory uncertainty that is currently undermining fintech innovation and materially threatening competition in the financial services sector.[2]

Fintechs, data aggregators, and technology providers have made significant investments to innovate around the framework created by the final rule, and to comply with the final rule's requirements for third parties. In contrast, large financial institutions are creating and exploiting regulatory uncertainty to avoid the pro-innovation requirements the rule places on them and engage in anticompetitive practices that contradict both the rule and the statute, ultimately harming consumers and small businesses who rely on fair access to their own financial data, which will ultimately result in continued consolidation in the financial services sector.

---

[1] *See* https://www.govinfo.gov/content/pkg/FR-2024-11-18/pdf/2024-25079.pdf.
[2] *See* https://business.cch.com/BFLD/Forcht-Bank-v-CFPB-CFPB-Motion-For-Summary-Judgment-ECF-58-05303035.pdf.

The United States cannot afford to remain a global outlier without an open banking framework. Jurisdictions around the world—from the United Kingdom ("UK") and the European Union ("EU") to Australia, Singapore, Chile, and Canada—are embracing the principle that consumers and small and medium-sized enterprises ("SMEs") should control access to their own financial data. By contrast, the United States' continued reliance on opaque, bilateral data-access agreements represents a failure to American consumers and SMEs and places the U.S. at a growing global competitive disadvantage for fintech innovation relative to jurisdictions like Brazil and India that have well-established frameworks and large markets that attract investors.

Against this backdrop, and to ensure the United States continues leading in financial innovation, we believe the Bureau should build on the foundation laid by the current rule without needlessly slowing down the market and endangering our members' significant strategic investments in open banking powered innovation. In that spirit, we strongly urge the CFPB to hew closely to the following principles in its reconsideration of an appropriate section 1033 framework:

1. **Do not legalize data access fees**. The reconsidered PFDR framework should preserve the existing prohibition on fees for data access under both the CFPB's PFDR Rule and section 1033 of the Dodd-Frank Act, whether labeled as API fees, infrastructure recovery charges, or imposed through mandatory bilateral contracts, because section 1033 guarantees consumers and their authorized representatives the right to access financial information "upon request," not subject to payment. Allowing fees would transform a statutory right into a paid privilege, entrench incumbent banks' market dominance, and raise costs for consumers who rely on fintech tools for a myriad of use cases, including easy, secure integration of payment credentials, budgeting, savings, and credit access. No open banking regime worldwide permits financial institutions to charge for consumer-authorized data access; instead, these jurisdictions recognize that the costs of data provision are part of the normal cost of doing business, already recovered through account fees, lending spreads, interchange, and other revenue sources. The Bureau must preserve the PFDR Rule's explicit prohibition on fees to ensure that the section 1033 right remains free, accessible, and effective in promoting consumer empowerment, competition, and innovation.

2. **Affirm a broad, plain-meaning definition of "representative."** The statutory language in section 1033 of the Dodd-Frank Act makes clear that consumers have the right to designate representatives to access their data, and that this category extends beyond fiduciaries or legal guardians. Any new section 1033 framework should affirm that "representative" means any third party a consumer *affirmatively* authorizes—whether a financial institution, fintech, data aggregator, or other service provider. Limiting representatives only to fiduciaries would contradict the statutory text, undermine congressional intent, and weaken competition and consumer choice. The essential gating element should be informed consumer authorization, not fiduciary status. Importantly, we also note that applying fiduciary status would not confer stronger data protections for consumers than the current protections under Subpart D of the PFDR Rule, as many financial fiduciaries (such as broker-dealers) are only bound by data protections under the Gramm-Leach-Bliley Act ("GLBA"). Put another way, fiduciary duty would limit innovation without benefitting consumers or enhancing security.

3. **Maintain implementation timelines for the 13 largest banks**. The Bureau should maintain the current compliance date of July 1, 2026 for the largest banks, to avoid further uncertainty and market disruption. Small businesses, data aggregators, and fintech providers have already begun building and investing in innovative products and services based on the Rule's framework and compliance systems based on that timeline. Further delay would penalize responsible actors that acted in good faith. Extending implementation deadlines would also disadvantage consumers by prolonging restricted data access and allowing large incumbents to maintain anti-competitive practices for even longer. The Bureau should affirm that the largest banks, who already have compliance systems in place for consumer-permissioned data access facilitation anyway, are not off the hook due to their gamesmanship. Doing so would provide market certainty and protect the fintech sector's investments in the future.

4. **Consult small businesses and conduct a genuine cost–benefit analysis**. As the Bureau considers amendments to the PFDR framework, it is critical that it assess the impact of any potential amendments on small businesses, including startups driving innovation in financial technology, cryptocurrency, and agentic artificial intelligence ("AI"). The Bureau should prioritize a transparent process, consistent with administrative law, that fully accounts for the disproportionately negative impact that certain adjustments to the current rule, such as delaying compliance timelines or allowing fees for data access, would have on small third parties. Before making changes to the PFDR framework, the CFPB should convene a panel under the Small Business Regulatory Enforcement Fairness Act ("SBREFA") to evaluate costs, benefits, and practical implementation challenges that small third parties will surely face. To be absolutely clear, even just delaying the implementation deadlines on the current rule would have a significant economic impact on a substantial number of small entities ("SISNOSE"). Any certifications to the contrary would be a legally dubious step that would endanger fintech startups and only benefit the nation's 13 largest banks. A deliberate, data-driven SBREFA process is required by Congress for this rule and is critical to give small businesses a voice.

5. **The Bureau should affirm a broad legally binding consumer financial data right in the United States**. Countries around the world are embracing the notion that consumers and SME owners should have full control of their financial data. The U.S. risks falling behind as a global leader in fintech innovation by failing to keep up with our global competitors. Beyond fintech, the Bureau also risks setting a precedent that undermines agentic AI use cases across the economy, many of which will ultimately rely on consumer permissioned data access. With its section 1033 authority, the Bureau has the potential to improve financial access and spur growth: providing greater access to safe and affordable credit for thin or no-file borrowers; facilitating access to savings tools; and enabling secure, technology-enabled payment and budgeting tools for Americans with little or no access to traditional bank accounts. To accomplish this objective, FDATA strongly believes that any non-proprietary data element that is available to an end user through their online banking portal or is included on a paper statement, and that is not the intellectual property of the data holder, should be considered in scope as the Bureau contemplates promulgating a customer financial data right by creating protected classes of data under section 1033 of the Dodd-Frank Act. To this end, the Bureau should expand the types of accounts and data elements covered under its section 1033

rulemaking to include investment, retirement, auto loan, mortgage, student loan, public benefit accounts, and other bank-held consumer accounts.

6. **Encourage application programming interface ("API") adoption without prohibiting existing technology**. FDATA has long advocated for regulatory oversight and supervision of fintech and aggregation firms under a uniform minimum standard for those who access a customer's financial data with their consent. While FDATA is technology neutral and supports the transition to API access of customer-permissioned financial data, the narrow scope of covered accounts and data elements under the Bureau's section 1033 rulemaking has exacerbated the reality that the ecosystem is not yet ready to completely prohibit existing technological methods of accessing customer data without massive detriments to innovation. Instead, the Bureau should accelerate the ecosystem's transition to uniform API-based financial data access by expanding the scope of covered accounts and data elements under this rulemaking. With regard to legacy data connection technologies, doing so would promote faster adoption of APIs across the market, without the need for prescriptive regulatory intervention on whether or how legacy methods may continue to operate during the transition period.

7. **Ensure security parity across the ecosystem**. The new section 1033 framework must maintain interoperable and proportional risk-based security obligations, ensuring that all participants from financial institutions to fintechs, and aggregators, meet robust, risk-based standards appropriate to their activities and regulatory oversight. All participants in the open banking ecosystem should meet baseline requirements such as those aligned with the Federal Trade Commission's ("FTC") Safeguards Rule, the National Institute of Standards and Technology Cybersecurity Framework ("NIST CSF"), or ISO standards. Independent certification or standardized oversight should provide accountability and limit the burden on financial institutions to undertake third party risk management reviews for each requesting third party accessor of data. Maintaining the parity in the current rule will protect consumers while preventing incumbents from using "security" as a pretext to limit competition. This is particularly important given recent examples of financial institutions invoking "risk-based" discretion to justify "debanking" lawful customers—a practice now under federal review and the subject of a presidential executive order.[3]

8. **Provide consumers with full control over their data.** Within the PFDR Rule's framework, the permissible use of data should be determined by the consumer's affirmative direction. If a consumer explicitly authorizes a trusted third party to access and process their information for a particular purpose—such as budgeting and savings insights, credit underwriting, income and asset verification, fraud detection, and personalized financial management—that use should be deemed primary and allowed.

9. **Ensure reasonable consumer reauthorization and deletion rules**. While consumers must remain in control of their data, the PFDR framework should avoid rigid re-permissioning requirements—such as blanket 12-month expirations—that create unnecessary friction. Consumers should have flexible reauthorization options, the ability to revoke consent at any time, and the right to preserve

[3] *See* https://apnews.com/article/trump-biden-debanking-crypto-jpmorgan-bank-america-obama-fd90a869f22e3bcc801e682b7ae62b75.

beneficial historical transaction data with their authorized representatives when they choose, rather than being forced into deletion rules that disrupt ongoing consumer-permissioned services. The Bureau should also exercise caution regarding Tokenized Account Numbers ("TANs"), which, while designed for security, often introduce payment failures and operational complexity, and consumer confusion when used for recurring transactions. TAN use also creates risk of anticompetitive behavior, and the CFPB should maintain its vigilance and carefully examine financial institutions for anticompetitive uses of TANs. FDATA believes that secure, persistent API connections paired with clear consent controls can achieve the same privacy and security goals without undermining functionality or competition.

FDATA's responses to each of the CFPB's ANPR questions follow.

A. Scope of Who May Make a Request on Behalf of a Consumer

1. *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 meaning of "representative" is quite simply someone authorized to act on behalf of another. Under the Dodd-Frank Act, Congress defines "consumer" to include "an agent, trustee, or representative acting on behalf of an individual."[4] The Dodd-Frank statute expressly included "representative[s]" as covered, authorized parties. Statutory text and context preclude the artificially narrow reading of "consumer" limited to individual consumers or their fiduciaries pressed by data providers. Nothing in the statutory text of Dodd Frank suggests that Congress intended to limit "representative" to fiduciaries or legal guardians; when Congress means to impose that limitation, it uses terms like "legal representative" or "fiduciary," which it did not do here. Indeed, the Dodd-Frank Act itself uses those terms in other sections of the statute when such limitations were intended by Congress.

Instead, the section 1033 Rule requires data providers to "make available to a consumer [or their agent, trustee, or representative], upon request".[5] The Dodd Frank statute defines "consumer" to include not only individuals themselves but also those acting on their behalf, making clear that Congress contemplated authorized third parties within its scope. The only tenable reading of that provision is that authorized third parties, as representatives, fall within its scope. Attempting to read "representative" more narrowly would render the term superfluous, contradict the statutory structure created by Congress, and reduce the section 1033 Rule to merely duplicating rights that individual consumers already enjoyed.

This interpretation aligns directly with the U.S. Department of the Treasury's 2018 report which was produced during the first Trump Administration. That interpretation affirmed that the term "consumer" under Title X of Dodd-Frank "is best interpreted to cover circumstances in which consumers affirmatively authorize, with adequate disclosure, third parties such as data aggregators and consumer fintech application providers to access their financial account and transaction data."[6] Treasury specifically recommended that the CFPB affirm that "third parties properly authorized by consumers, including data aggregators and

[4] *See* https://www.congress.gov/111/plaws/publ203/PLAW-111publ203.pdf, pg. 582.
[5] *Id*, pg. 634.
[6] *See* https://home.treasury.gov/system/files/136/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf, pg. 31.

consumer fintech application providers, fall within the definition of 'consumer' under Section 1002(4) of Dodd-Frank for the purpose of obtaining access to financial account and transaction data."[7]

In other words, a narrow interpretation of Section 1033 as applying only to direct consumer access would, as Treasury observed, "do little to advance consumer interests by eliminating many of the benefits they derive from data aggregation and the innovations that flow through from fintech applications."[8]

The existing section 1033 Rule's interpretation—that consumers may direct authorized third parties to access their information—is therefore not only faithful to the ordinary meaning of the term "consumer" but also the only construction that comports with the statute's text, context, and purposes of promoting consumer choice, competition, and innovation. Any other reading of this statutory language would raise a major question as to why Congress would have intended to create such a limited, duplicative consumer right that fails to advance the statute's broader goals related to competitiveness and transparency, even though it was well aware of the increasing importance of representatives in the consumer financial data ecosystem.

2. *Are there other provisions in Federal statutes or financial services market practice in which third parties authorized to act on behalf of an individual encompass, on an equivalent basis, both those having fiduciary duties and those who do not?*

Federal statutes and financial market practices frequently distinguish between fiduciary roles and other authorized third parties, and they do so by using specific language. When Congress intends to invoke a fiduciary relationship, it uses terms like "legal representative" or "fiduciary," as used in: the Federal Deposit Insurance Act, which prohibits certain mortgage loans to persons "acting in a fiduciary capacity"; the National Bank Act, authorizing recovery of interest by a person "or his legal representatives"; and the Federal Credit Union Act (same).[9,10,11] Other federal provisions reflect this same deliberate drafting distinction. For example, the Employee Retirement Income Security Act defines "fiduciary" in a precise, technical manner, showing that fiduciary duties attach only when explicitly stated.[12] The Bankruptcy Code defines "person" broadly but then separately enumerates "trustee" and "legal representative of the estate," treating legal representatives as distinct fiduciary roles.[13]

The Dodd-Frank Act itself draws this line clearly, using "legal representative" four separate times to mean fiduciary-type relationships—for example, in provisions governing whistleblower representation, and in defining "retail customer" to include a "natural person, or the legal representative of such natural person." [14,15] By contrast, the section 1033 Rule uses the term "consumer" that includes only the broader term "representative" within its prescribed definition. Under ordinary meaning, this choice makes clear Congress's intent to extend data access rights to both fiduciary and non-fiduciary third parties alike. Given

---

[7] *Id.*
[8] *Id*.
[9] *See* https://uscode.house.gov/view.xhtml?edition=prelim&num=0&req=granuleid%3AUSC-prelim-title12-section1831b.
[10] *See* https://www.govinfo.gov/content/pkg/USCODE-2024-title12/pdf/USCODE-2024-title12-chap2-subchapIV-sec86.pdf.
[11] *See* https://www.govinfo.gov/content/pkg/COMPS-264/pdf/COMPS-264.pdf?utm.
[12] *See* https://www.govinfo.gov/content/pkg/COMPS-896/pdf/COMPS-896.pdf.
[13] *See* https://www.govinfo.gov/content/pkg/USCODE-2011-title11/pdf/USCODE-2011-title11.pdf.
[14] *See* https://www.congress.gov/111/plaws/publ203/PLAW-111publ203.pdf, pg. 367.
[15] *Id*, pg. 450.

the varied nature of the word "representative" within different parts of Dodd Frank, the choice in section 1033 can only be reviewed as a clear intent by Congress to allow consumers to designate both categories of representatives on an equivalent basis.

3. *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?*

The statutory phrase "agent, trustee, or representative" does not confine "representative" to fiduciaries. Indeed, the Internal Revenue Service even recognizes that "agent" does not inherently denote a fiduciary relationship.[16] Congress frequently uses the term "agent" in a non-fiduciary context—for example, a "withholding agent" in the tax system or a "service agent" in employment settings—to describe entities that perform administrative or operational functions on behalf of others, illustrating that the term does not inherently imply a fiduciary relationship.[17,18]

When Congress intends to require fiduciary duties, it says so <u>expressly</u>, using terms like "fiduciary" or "legal representative." For example, the Sports Agent Responsibility and Trust Act refer to an "agent" in the context of an agency contract, while the Higher Education Opportunity Act uses the term "trustee" in defining an employment relationship. [19,20] The use of different terms underscores that "agent" and "trustee" do not share a common fiduciary quality. Accordingly, applying noscitur a sociis doctrine to narrow "representative" is misplaced. As courts have previously cautioned, a short list containing one fiduciary term ("trustee") and one non-fiduciary term ("agent") cannot dictate that the third term ("representative") must also mean fiduciary as ruled in *Graham County Soil & Water Conservation Dist. v. United States*.[21] The statutory context confirms that all three terms share the broader common quality of "acting on behalf of another" under Dodd Frank. Thus, interpreting "representative" to require fiduciary duties would not only lack textual support but also collapse the distinctions among the listed terms, contrary to Congress's intention.

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

The Bureau should rely on established interpretive principles that give effect to Congress's words and purpose. First, the canon against surplusage requires that "representative" be given an independent and

---

[16] *See* https://www.govinfo.gov/content/pkg/CFR-2011-title26-vol18/pdf/CFR-2011-title26-vol18-sec301-7701-5.pdf.
[17] *See* https://www.govinfo.gov/content/pkg/USCODE-2011-title26/html/USCODE-2011-title26-subtitleA-chap4.htm.
[18] *See* https://www.govinfo.gov/content/pkg/USCODE-2023-title49/pdf/USCODE-2023-title49-subtitleVI-partB-chap313-sec31306a.pdf.
[19] *See* https://sports-entertainment.brooklaw.edu/wp-content/uploads/2021/01/15-USC-%C2%A7-7801-7807-Sports-Agent-Responsibility-and-Trust.pdf.
[20] *See* https://www.govinfo.gov/content/pkg/USCODE-2024-title20/pdf/USCODE-2024-title20-chap28-subchapI-partE-sec1019.pdf.
[21] *See* https://www.justice.gov/sites/default/files/osg/briefs/2008/01/01/2008-0304.pet.ami.inv.pdf.

meaningful role, rather than being collapsed into the existing concepts of "agent" or "trustee." If "representative" were read narrowly to mean only fiduciary relationships, the term would add nothing new to the statute, making it redundant. Courts consistently reject readings that render statutory terms superfluous. Second, Congress's drafting history and word choice are highly significant. In numerous other statutes—such as the Federal Deposit Insurance Act, the National Bank Act, and the Federal Credit Union Act—Congress has expressly used terms like "fiduciary" or "legal representative" when it intended to impose fiduciary obligations. The absence of those qualifiers here demonstrates an intentional choice to use "representative" in its broader, ordinary sense, encompassing both fiduciary and non-fiduciary designees.

Third, statutory context and purpose confirm the breadth of the term. The section 1033 rule is designed to expand consumer control, enhance competition, and promote transparency by enabling consumers to authorize trusted third parties to access their financial data. A narrow reading would undermine these goals by limiting consumer choice to only fiduciary actors, cutting out a wide range of legitimate service providers that Congress clearly intended to include. Fourth, practical considerations highlight the flaw in the financial institutions' restrictive interpretation. Financial institutions themselves are not uniformly fiduciaries with respect to consumer financial data. Reading "representative" to mean only fiduciary would lead to the paradoxical result that financial institutions would assume fiduciary obligations only when consumers grant outside access to their data, while escaping such duties for much of the data generated directly in the financial institution-consumer relationship. This result is inconsistent, illogical, and contrary to the overall statutory scheme.

Finally, precedent and interpretive canons caution against constructions that nullify statutory innovations. Limiting "representative" to fiduciaries would reduce section 1033 to a near nullity; duplicating access rights already provided to consumers long before Dodd-Frank was enacted into law. To give effect to Congress's innovation in section 1033, "representative" must be understood in its plain and ordinary sense—as encompassing all third parties that consumers affirmatively authorize, whether or not they occupy a fiduciary role. Taken together, text, context, purpose, and interpretive canons all point to a broad construction of "representative." Congress deliberately chose a capacious term to ensure that consumers, not incumbent financial institutions, would control who may access their data on their behalf.

5. *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?*

Interpreting "representative" to mean only fiduciaries would drastically narrow the scope of the consumer right that Congress established in section 1033. The vast majority of third parties that consumers rely on to access and use their financial data—fintech applications, budgeting tools, payment platforms, and even banks themselves—do not operate as fiduciaries with respect to consumer data. By conditioning participation on fiduciary status, consumers' ability to permission third parties to act on their behalf would be effectively extinguished in practice.

Such a reading would also be fundamentally unworkable. Imposing fiduciary duties across the entire spectrum of open banking use cases—from routine account aggregation to specialized lending services—would force every bank, credit union, aggregator, payment wallet, lender, or crypto platform into the role of a legal fiduciary. That requirement would be inconsistent with existing law, which has never recognized financial institutions as fiduciaries in ordinary consumer relationships, and it would create an impossible compliance burden for new entrants. Beyond practical impossibility, this approach would undermine competition and innovation. Globally, open banking frameworks have been successful precisely because they allow consumers to permission both fiduciary and non-fiduciary actors to access and use their data. By contrast, a fiduciary-only regime would lock out many non-fiduciary service providers, dramatically reducing consumer choice, entrenching incumbent institutions, and frustrating Congress's purpose of expanding consumer control, competition, and transparency in financial services.

Finally, the absurdity of the result underscores the interpretive flaw. Financial institutions themselves do not treat consumer financial data in a fiduciary manner in the ordinary course; requiring third-party providers to assume fiduciary obligations as a precondition to data access would give incumbents a competitive exemption from the very duties imposed on challengers. This asymmetry would distort the market, discourage innovation, and render section 1033 hollow, as consumers would be left with fewer real choices for exercising their statutory right to share and use their own data.

For all these reasons, narrowing "representative" to fiduciaries would both gut the consumer right and eliminate the very competition Congress intended to foster. The statute's text in Dodd Frank, purpose, and global practice all confirm that "representative" must be understood more broadly, encompassing any third party that a consumer affirmatively authorizes.

6. *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?*

The section 1033 Rule's requirement that the Bureau prescribe standardized formats underscores that Congress intended the data access right to extend beyond natural persons acting individually and to include third parties authorized to act on their behalf. If Congress had envisioned that only individual consumers would exercise the right, there would have been no need to mandate interoperability through standardized formats, because individuals would typically receive information in human-readable form rather than through machine interfaces. The statutory text in Dodd Frank makes this point explicit, where in section 1033(d) it requires that standardized formats account for "the use of machine-readable files."[22] This language plainly signals that Congress anticipated a data-sharing ecosystem in which consumers designate third parties—often technology-based service providers—to receive, interpret, and utilize information on their behalf. By directing the Bureau to ensure formats are compatible with machine-to-machine transfer, Congress recognized that consumer representatives would not merely be fiduciaries, but also non-fiduciary entities such as fintechs, aggregators, and other software-driven platforms.

Moreover, this language choice is consistent with the purpose of the section 1033 Rule: to give consumers meaningful control over their financial data in a modern, digital economy. Interpreting "representative" narrowly to include only fiduciaries would be at odds with Congress's vision of automated, scalable, and consumer-driven data portability, curbing the development of standardized formats and undermining the competitive ecosystem Congress sought to promote. Accordingly, the Bureau should interpret "representative" in light of section 1033(d) as including both fiduciary and non-fiduciary designees, particularly technology-enabled intermediaries that rely on machine-readable access to deliver services to consumers.

[22] *See* https://www.congress.gov/111/plaws/publ203/PLAW-111publ203.pdf, pg. 634.

7. *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?*

Because “representative” cannot be limited to fiduciaries in a way that is consistent with the statutory text of Dodd Frank, the essential element is consumer authorization. A representative must demonstrate that the end user has knowingly and affirmatively consented to the representative accessing their data. At a minimum, this requires:

- **Informed consumer consent**: The consumer must clearly and affirmatively grant permission for the representative to access their financial information, rather than through implied or coerced arrangements.
- **Transparency and disclosure**: The representative must provide clear notice to the consumer regarding the scope of data access, the purposes for which the data will be used, and any limitations or conditions.
- **Obligations regarding protection**: Representatives must certify compliance with standards governing secure data handling, consistent with the Bureau’s rulemaking authority.
- **Revocation**: Representatives must disclose how consumers may revoke their data access and provide an easy means to do so.

These elements ensure that the concept of “representative” is neither unbounded nor dependent on fiduciary status. Instead, it is tethered to the consumer’s right to control their own financial data and to designate trusted third parties to act on their behalf. By structuring the definition around consumer authorization and enforceable safeguards, the Bureau can preserve flexibility and competition while ensuring strong protections for consumers.

8. *Are there any legal precedents or other considerations relevant to the above questions based on the applicability of the same definition of ‘‘consumer’’ to other Dodd-Frank Act provisions?*

The Dodd-Frank Act’s definition of “consumer” applies throughout the statute and expressly includes not only the individual consumer but also their authorized representative. In multiple other provisions in Dodd Frank, however, Congress chose narrower terminology—such as “legal representative” or “fiduciary”—when it intended to confine access to those with fiduciary obligations. The deliberate use of the broader “representative” in the section 1033 Rule must therefore be given effect under the canon of consistent usage, which requires terms to be interpreted consistently across a statute unless context clearly dictates otherwise.

If “representative” were collapsed into “fiduciary,” that interpretation would create a mismatch with Congress’s drafting pattern elsewhere within Dodd Frank. Courts have long cautioned that when Congress varies its wording across statutory provisions, the difference is presumed intentional. For example, in *Russello v. United States*, “[W]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.”[23] Under this principle, the broader choice of

[23] *See* https://myattorneyusa.com/wp-content/uploads/2024/06/russello-v-us.pdf.

“representative” in section 1033 must be read to include both fiduciary and non-fiduciary third parties authorized by the consumer.

Reading “representative” more narrowly would not only contradict the plain text but also frustrate Congress’s overall objectives in Dodd-Frank—expanding consumer control, promoting competition, and ensuring transparency in financial markets. Moreover, adopting a fiduciary-only construction would invite major questions of statutory interpretation: why would Congress use “legal representative” when it meant fiduciary, but then turn around and use only “representative” in a provision designed to empower consumers? Such a narrowing would be unlikely to withstand judicial review, particularly in light of the clear drafting contrast. Taken together, statutory canons, case law on word variation, and Dodd-Frank’s purpose all reinforce that “representative” in section 1033 should be construed broadly to encompass any third party the consumer affirmatively authorizes, not just fiduciaries.

B. Defrayment of Costs in Exercising Rights Under Section 1033

9. *Does the PFDR Rule’s prohibition on fees represent the best reading of the statute? Why or why not?*

The PFDR Rule’s prohibition on fees is the best—and only tenable—reading of the section 1033 Rule. The statutory text directs that data providers must “make available” information to consumers, and by definition, their authorized representatives, “upon request.” Nothing in the text of the section 1033 Rule authorizes data providers to impose a charge for the exercise of this statutory data access right. If Congress had intended to permit fees, it would have said so expressly, as it has in other statutes where user rights are conditioned on payment. The absence of such language confirms that the section 1033 Rule advances cost-free access. Historical practice supports this reading. For years, financial institutions have provided no-fee data access to consumers and their designated intermediaries, consistent with the statutory mandate and the principle that a legal right cannot be transformed into a transactional commodity. Permitting fees would recast section 1033’s guaranteed right into a conditional, paid privilege, undermining the consumer choice and market competition that Congress intended to foster.

Global practice reinforces the point. In every jurisdiction that has implemented open banking frameworks—including Brazil, India, the UK, the EU, Australia, and Canada—financial institutions are required to provide consumer-authorized access without imposing fees on the requesting party. To allow fees in the United States would place the domestic regime out of step with international norms in a way that weakens American competitiveness in financial innovation by driving consolidation.

Moreover, the policy rationale against fees is compelling. Financial institutions already recover the costs of their data infrastructure through account fees, interest spreads, and service charges. They also enjoy significant public benefits: access to low-cost funding through the Federal Reserve’s discount window, participation in Fed-operated payment rails, and liquidity facilities that stabilize their balance sheets. Against that backdrop, an additional toll for consumer-permissioned data access functions not as cost recovery but as an anticompetitive barrier—an effort to extract monopoly rents that harm innovation and entrench incumbents’ control over consumer data. For all of these reasons—statutory text, legislative purpose, historical practice, international comparison, and policy rationale—the PFDR Rule’s categorical prohibition on fees represents not only the best reading of section 1033, but the only reading consistent with Congress’s objectives and the broader open banking ecosystem.

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

The PFDR Rule was correct that permitting fees would obstruct the data access right Congress created in section 1033. The plain statutory command is that data providers must "make available" information to "consumers," as defined, to their authorized representatives. A right that is contingent on paying a toll is no longer a right, it is a commodity, accessible only to those able or willing to pay. Congress did not use conditional language, nor did it authorize financial institutions to monetize compliance with section 1033.

The broader statutory purpose reinforces this reading. Title X of the Dodd-Frank Act was enacted to make markets for consumer financial products and services more fair, transparent, and competitive. Allowing incumbents to charge fees for consumer-authorized data access would move in the opposite direction, creating new barriers to entry, raising consumer costs, and entrenching incumbents' market power. Practical experience demonstrates the risk. JPMorgan Chase has already attempted to impose unilateral fees on data aggregators and fintechs across the entire sector, using its market power to threaten to block or limit consumer-permissioned access. If fees are permitted under the rule or if the rule is silent on fees, other large institutions will inevitably follow suit, converting the statutory right into a "pay-to-play" regime. The result would be to gut the portability Congress intended to guarantee, leaving consumers with fewer choices and reinforcing the dominance of established financial institutions.

11. *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?*

The fixed costs of implementing the standards required by section 1033(d) will vary substantially across covered persons, reflecting differences in size, existing infrastructure, and technological maturity. Some larger financial institutions and data aggregators have already incurred many of these costs through business decisions made in recent years to develop and deploy open banking–style APIs or data-sharing frameworks in anticipation of greater regulatory standardization. For those entities, incremental compliance costs may be limited to aligning existing technical specifications and governance policies with the final standards adopted under subsection (d). The magnitude of the fixed costs will depend on several interrelated factors, including:

- The institution's infrastructure and its compatibility with modern API-based systems;
- The extent of data normalization required due to disparate storage systems, formats, or vendor dependencies;
- The robustness of existing cybersecurity and authentication frameworks; and
- The degree of reliance on third-party service providers to supply or maintain technology infrastructure.

Smaller financial institutions face a unique set of challenges in modernizing their data infrastructure, including limited in-house technical expertise, constrained development resources, and longer implementation timelines. Fortunately, many have viable options to partner with third-party vendors to build and maintain the architecture needed not only to comply with section 1033, but—more importantly—

to deliver the digital experiences and innovative services their consumers increasingly expect. In some instances, these smaller institutions obtain these services for free.[24] Without offering these capabilities, smaller institutions risk losing customers to larger financial institutions that already provide seamless digital services, accelerating market consolidation and reducing consumer choice. In today's environment, smaller financial institutions simply cannot afford not to offer these innovative services. The Bureau's PFDR rulemaking instead should be contemplated as bringing much-needed standardization to the marketplace, enabling smaller institutions to compete more easily with larger incumbents.

By contrast, large institutions often already maintain robust internal data-sharing infrastructure and possess both the financial and human capital necessary to absorb implementation costs more efficiently. Consequently, the relative impact of compliance will be far less severe for them. The disparity in fixed-cost burdens could therefore deepen competitive imbalances in the marketplace—undermining the very goals of section 1033 if not carefully accounted for in the Bureau's analysis.

Because any changes to the rule are expected to have a disproportionate impact on smaller entities—including community banks, credit unions, and non-depository fintechs that meet the definition of a covered person—the Bureau should convene a SBREFA panel prior to undertaking any proposals to amend the existing rule. Such a panel would allow for more accurate input from small entities on implementation challenges, operational costs, and alternative approaches to compliance that could mitigate undue burden while preserving the consumer rights intended by Congress.

12. *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?*

This question is best answered by covered financial institutions themselves.

13. *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?*

The cost range identified above is not affected by the need to confirm that a representative has been properly authorized. The standards developed through the CFPB's approved Standard Setting Organization ("SSO") will provide consistent, secure methods to validate authorization, allowing this process to operate efficiently and at scale. That said, the Bureau should ensure that authorization verification does not become a tool for large financial institutions to restrict or delay data access. Granting large financial institutions control over authorization or mandating a single authentication pathway could create de facto veto power over consumer-permissioned data sharing. Instead, the final rule should promote a technology-agnostic approach—one that allows multiple secure methods for confirming representative authority while maintaining strong auditability and fraud protections. Such flexibility will help contain costs for covered persons, prevent competitive distortions, and ensure both digitally native and non-digitally native consumers can safely benefit from open banking.

[24] *See* https://plaid.com/blog/plaid-exchange-jack-henry/.

14. *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?*

Legal precedent makes clear that agencies cannot impose cost-sharing obligations in the absence of explicit statutory authorization—and that silence is dispositive here. When Congress intends for an agency to set, recover, or allocate costs, it does so unambiguously. Examples include the Securities and Exchange Commission's ("SEC") authority to establish fee schedules, user-fee frameworks that fund the Federal Deposit Insurance Corporation ("FDIC"), and cost-recovery mechanisms available to agencies such as the National Credit Union Administration ("NCUA") and the Federal Reserve for their payment services. The section 1033 Rule contains no comparable provision authorizing the CFPB to establish or approve cost-sharing arrangements.

Consumers already pay for the infrastructure supporting their financial data rights through account fees, interest charges, and other service-related costs assessed by their financial institutions. Imposing additional charges on the exercise of those rights would effectively transform a statutory entitlement into a paid privilege—contrary to both the plain meaning of the law and Congress's intent to empower consumers through free access to their own financial information. A "right," by definition, must be free to exercise. Allowing covered persons to charge for data access would undermine that principle, distort market competition, and restrict consumer choice. The Bureau was therefore correct in the PFDR Rule to prohibit such fees and should reject any argument suggesting it can "balance" consumers' statutory rights through unauthorized cost-sharing in the absence of clear congressional direction.

15. *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?*

Covered persons should not be permitted to recover a "reasonable rate" or any other form of compensation for enabling consumers to exercise their rights under section 1033. Congress created a statutory right of access to financial data, and by definition, a right must be free to exercise. The Dodd-Frank Act makes clear that these rights are intended to promote transparency, competition, and consumer choice—not to establish new revenue streams for data holders. Consumers already pay their financial institutions through existing account fees, loan interest, service charges, and interchange fees, all of which support the infrastructure that generates, maintains, and stores financial data. Permitting additional cost recovery would therefore amount to double charging consumers and their authorized representatives for the same functionality. It would also undermine the very purpose of section 1033 by turning a statutory entitlement into a paid privilege.

Moreover, allowing covered persons to charge "reasonable" access fees would introduce a structural bottleneck that entrenches incumbent advantage. Large financial institutions could exploit such provisions to extract monopoly rents, delay or restrict data access, and steer consumers toward higher-cost payment products or closed ecosystems. Doing so would directly contradict the rule's intent—to empower consumers to easily move their data and switch between financial institutions or fintech providers—thereby entrenching incumbent market power instead of reducing it. JPMorgan Chase's recent attempt to impose unilateral API fees offers a concrete example of how financial institutions can wield their market power to threaten competition and harm consumers, while setting a market precedent for other financial institutions to follow. For these reasons, the Bureau was correct in the PFDR Rule to prohibit cost recovery through fees. Maintaining that prohibition is essential to ensuring that consumer financial data rights remain meaningful, affordable, and consistent with the statute's intent to foster innovation, competition, and consumer empowerment.

16. *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?*

If the Bureau were to allow covered persons to recover a "reasonable rate" for enabling consumers to exercise their section 1033 rights, then a cap would be essential to prevent abuse, but FDATA maintains that no such recovery should be permitted in the first place. Congress created a statutory right to access "upon request," and by definition a right must be free to exercise. Consumers already pay their financial institutions through account fees, interest, and service charges, meaning that additional charges for data access would amount to double payment and would obstruct the right Congress established. The better course—and the one consistent with the statute, with the PFDR Rule, and with internal priorities established in the April 16, 2025, memorandum from CFPB Chief Legal Officer Mark R. Paoletta (which declares that the Bureau "shall not engage in attempts to create price controls")—is to preserve the current prohibition on fees.[25] Any departure from that standard would turn a guaranteed consumer right into a paid privilege, undermining competition and consumer choice.

17. *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?*

Consumers already bear the costs associated with implementing the section 1033 Rule. Financial institutions and other covered persons already fund the infrastructure supporting consumer data access through existing revenue streams such as account maintenance fees, service charges, loan interest, and interchange fees—all of which are paid by consumers today, regardless of whether they actively exercise their rights under section 1033. Imposing additional costs—either directly on consumers who request data access or indirectly by spreading those costs across the customer base—would effectively charge them twice for the same service. This outcome would contradict the purpose and plain meaning of section 1033, which established a statutory right of access meant to be free at the point of use. Congress designed this right to empower consumers, not to create new cost centers for institutions.

Requiring consumers to further subsidize data providers' costs would undermine the statute's intent to enhance transparency, competition, and innovation in the financial ecosystem. Moreover, given the strong profitability of major financial institutions, it is entirely plausible for such institutions to absorb these costs without instituting additional consumer fees. For example, JPMorgan Chase reported $58.5 billion in net

[25] *See* https://www.consumerfinanceandfintechblog.com/wp-content/uploads/sites/58/2025/04/CFPB-Memo.pdf.

income in 2024.[26] This financial strength underscores that large, covered persons are in a position to internalize compliance costs rather than shift them onto consumers. The Bureau should therefore maintain its position that exercising one's data access right must remain free and universal for all consumers.

C. Information Security Concerns in the Exercise of Section 1033 Rights

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

The PFDR Rule provides robust and appropriate protections for the security of consumers' financial data. It requires third parties accessing consumer-permissioned data to comply with the same core data security obligations that apply to financial institutions through the FTC's Safeguards Rule. This alignment ensures that all entities operating within the open banking ecosystem—whether traditional financial institutions or authorized third parties—adhere to equivalent standards for encryption, access controls, breach notification, and oversight of service providers.

By incorporating these established data security requirements, the PFDR Rule ensures that consumers can safely exercise their rights under section 1033 without exposing their personal or financial information to undue risk. Importantly, the rule recognizes that the effectiveness of a security program depends on the rigor of its controls—not on the size of the company or how much it spends on data. Simply paying more for data or maintaining larger infrastructures does not equate to stronger protections. In sum, the PFDR framework balances consumer empowerment with strong, enforceable safeguards, giving consumers control over their financial data while maintaining the same level of protection expected within the banking system.

19. *What are the fixed costs of establishing an information security architecture that is capable of ensuring, in the absence of compromise of operational protocols, that customer financial information can be securely acquired, stored, and transmitted, by the consumer, from a ''covered person'' to the consumer?*

The fixed costs of establishing an information security architecture capable of meeting section 1033's requirements are substantial, though they vary significantly by institution based on size, technological maturity, and existing infrastructure. Core elements of a compliant architecture include the deployment of secure and standardized APIs, encryption of data both at rest and in transit, continuous monitoring and incident detection systems, and adherence to recognized frameworks such as the FTC's Safeguards Rule, ISO 27001, or NIST SP 800-53. These components require considerable upfront capital investment and ongoing operational expenditures to maintain security integrity, manage third-party vendor risks, and ensure regulatory compliance.

Because these costs are highly fact-specific, broad generalizations risk overstating or understating the actual burden. For larger financial institutions and aggregators that already maintain advanced cybersecurity and data-sharing infrastructure, incremental costs may be relatively modest. For smaller or mid-sized institutions, however, establishing comparable systems may require meaningful new investment or outsourcing to qualified third-party providers.

---

[26] *See* https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/annualreport-2024.pdf.

FDATA recommends that the Bureau rely on empirical evidence to inform its analysis rather than theoretical assumptions. Specifically, the Bureau should draw on information collected through its prior Section 1022(c)(4) market monitoring process and invite additional input from covered persons, fintechs, and technology providers that currently operate secure, consumer-permissioned data access systems. Doing so will ensure that any cost assessments reflect real-world experience and avoid imposing disproportionate compliance burdens on smaller or less technologically advanced institutions.

20. *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?*

The market is beginning to respond to this challenge by offering reasonably priced, scalable solutions that reduce the compliance gap. A growing number of technology vendors and open finance platforms now provide turnkey or modular compliance offerings—such as secure APIs, consent dashboards, authentication systems, and continuous monitoring tools—that align with the PFDR Rule's data access and security requirements. These shared infrastructure solutions enable smaller participants to achieve compliance without the prohibitive cost of building full-stack systems internally.

In this way, economies of scale are being realized collectively across the market rather than institution by institution. This evolution helps ensure that compliance with the PFDR Rule is achievable even for covered persons and third-party representatives serving a limited customer base—advancing the Bureau's broader goals of inclusion, competition, and innovation within the open banking ecosystem.

21. *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 or non-existence of a fiduciary relationship is not a meaningful factor in determining the incentives of third parties to invest in strong information security. Consumer-permissioned third parties rely fundamentally on consumer trust to sustain their business models, and that reliance creates powerful market incentives to build and maintain robust security practices regardless of fiduciary status.

Indeed, fiduciaries themselves have been subject to significant data breaches in recent years. For example, Fidelity Investments and TIAA-CREF have both disclosed breaches exposing sensitive customer information, and JPMorgan Chase—acting as a fiduciary for certain trust and investment accounts—suffered one of the largest cybersecurity incidents in financial services history in 2014.[27] These examples make clear that fiduciary status alone does not guarantee effective data protection.

Moreover, the PFDR Rule already establishes security requirements by incorporating the FTC's Safeguards Rule and other enforceable standards, ensuring that all authorized third parties—whether fiduciaries or not—must meet consistent, high-level protections. These statutory and regulatory guardrails make fiduciary designation unnecessary as a determinant of security outcomes. In practice, fintechs and other authorized third parties invest heavily in advanced security technologies not because they are fiduciaries, but because their ability to operate depends on maintaining consumer confidence in data safety.

---

[27] *See* https://archive.nytimes.com/dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/.

With respect to cost-benefit analyses, FDATA agrees with the Bureau that they are essential to understanding implementation impacts and ensuring proportionality. We look forward to the CFPB conducting its Regulatory Flexibility Act ("RFA") and SBREFA-mandated cost-benefit analyses before making any future adjustments to the rule or compliance timelines. Such reviews are critical to maintaining both strong consumer protections and a competitive, innovation-friendly open banking ecosystem.

22. *Are there any peer-reviewed studies discussing whether levels of information security materially vary between those businesses that have fiduciary duties to their clients and those that do not?*

FDATA is not currently aware of any peer-reviewed studies demonstrating that levels of information security materially vary between businesses that have fiduciary duties to their clients and those that do not. In practice, the key determinants of security performance are market expectations, regulatory requirements, and reputational risk—not fiduciary status.

Financial technology providers and other third parties operating under consumer authorization face identical incentives—and, under the PFDR Rule, identical obligations—to maintain strong data safeguards as fiduciaries do. Their business models depend on earning and retaining consumer trust, and their compliance obligations under the FTC's Safeguards Rule and related frameworks impose robust, enforceable standards for data protection.

Indeed, these obligations are in some respects more comprehensive than those applicable to all fiduciaries, as not every fiduciary entity is subject to the GLBA data security requirements. This further underscores that fiduciary designation is not a reliable predictor of cybersecurity maturity or investment levels. The absence of peer-reviewed evidence confirming such a distinction supports the conclusion that fiduciary status does not materially affect security outcomes across the industry.

23. *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?*

This question is best answered by financial institutions themselves, as they have historically experienced significantly larger and more frequent data breaches than consumer-permissioned fintech providers.

24. *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?*

Financial technology firms have deep experience with the secure storage and transmission of consumer financial data, in many cases spanning more than two decades. FDATA's members, in particular, have long been at the forefront of developing and maintaining secure, consumer-permissioned data-sharing systems that enable individuals to safely access and share their financial information across platforms and providers.

These firms collectively invest substantial resources in cybersecurity architecture, encryption protocols, continuous monitoring, and consent management systems to safeguard consumer information.

Their operational record reflects the effectiveness of these investments: to FDATA's knowledge, there have been no significant data breaches associated with open finance platforms operating under consumer-permissioned access. This exemplary track record demonstrates that open banking participants—guided by consumer consent, competitive pressures, and rigorous compliance frameworks—are already maintaining robust controls that meet or exceed the expectations outlined in the PFDR Rule.

This experience underscores both the adequacy of the Rule's baseline data security requirements and the industry's capacity to comply with them effectively. It also highlights that innovation and security are not mutually exclusive—consumer-permissioned data access can be both safe and transformative when paired with strong standards and responsible governance.

25. *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?*

When making information available to consumers under section 1033, covered persons must continue to comply with their existing obligations under the Bank Secrecy Act ("BSA"), Anti-Money Laundering ("AML") regulations, and general safety-and-soundness standards. However, there is no genuine conflict between these obligations, and the statutory right Congress granted consumers to access and share their own financial data. Section 1033 of the Dodd-Frank Act is explicit: data pertaining to a consumer must be made available in a machine-readable format upon request. Claims that fulfilling this mandate would undermine BSA, AML, or prudential responsibilities are unfounded.

In fact, secure, standardized interfaces—such as those prescribed under the PFDR Rule—enhance oversight and risk management by reducing reliance on methods like screen-scraping and enabling more transparent audit trails for regulators. Authorized third parties can also strengthen institutions' compliance frameworks by providing enriched transaction insights, anomaly detection, and other risk-based data that improve AML monitoring and fraud prevention.

The PFDR Rule's interface access provision already supports these obligations by mandating standardized, secure, and monitorable data-sharing channels. To further improve alignment, the Bureau could underscore that API-based data sharing gives covered persons greater visibility into data flows, consumer consent activity, and system access—tools that directly complement existing BSA and AML compliance frameworks rather than conflict with them.

Finally, to the extent any tension arises between the PFDR Rule and non-binding prudential risk-management guidance; the Bureau should affirm that the PFDR Rule prevails as a matter of statutory authority and regulatory obligation under the Dodd-Frank Act. Doing so will provide clarity and ensure that consumer data rights and prudential compliance operate in concert to strengthen, not weaken, the overall integrity of the financial system.

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

The PFDR Rule's reliance on existing information security standards under the GLBA delivers clear benefits with minimal incremental costs. GLBA has long provided the foundational federal framework governing financial data privacy and security, and FDATA's members—many of whom have operated under GLBA oversight for years—already comply with its requirements. Building the PFDR Rule on this established framework promotes regulatory consistency across the financial ecosystem and avoids unnecessary duplication or conflict between agencies.

This harmonization ensures that both incumbents and new entrants operate under a shared, well-understood set of obligations. It reduces compliance confusion, prevents regulatory fragmentation, and allows smaller participants to scale more efficiently by leveraging existing compliance systems already structured around GLBA standards. The outcome is a level playing field where financial institutions, fintechs, and other third parties meet the same baseline security expectations—strengthening consumer protection while fostering competition and innovation.

The costs associated with this approach are minimal, as they largely reflect the ordinary obligations of GLBA compliance, which financial institutions have long internalized as part of doing business. In short, reliance on GLBA standards provides continuity, scalability, and legal certainty while ensuring that the PFDR framework builds upon a proven, enforceable, and well-integrated regulatory foundation.

27. *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?*

Entities that access consumer financial data should adhere to widely recognized, risk-based information security frameworks such as the NIST CSF, ISO/IEC 27001, and other sector-specific standards like PCI DSS for payments. These frameworks are technology-neutral, updated regularly to reflect emerging threats, and already well understood by both financial institutions and technology providers. Adopting a common baseline of these standards ensures consistent protection of consumer data across banks and non-banks while preserving flexibility for innovation and scalability.

With respect to oversight, independent, accredited auditors are best positioned to evaluate compliance with these standards, operating under supervisory guidance from the CFPB. This model avoids duplicative or inconsistent reviews across multiple regulators and ensures that assessments are neutral, expert-driven, and scalable. Critically, data providers should not have unilateral authority to "approve" or "reject" counterparties based on opaque, proprietary criteria.

Instead, a standardized certification framework—validated by independent assessors against recognized benchmarks—would enable entities of all sizes to demonstrate compliance and give both consumers and regulators confidence in the security of data flows. This approach delivers strong, enforceable protections for consumers while promoting a competitive playing field, reducing barriers to entry, and preventing the misuse of "security" as a pretext to limit interoperability and competition.

28. *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?*

The PFDR Rule's provisions aimed at reducing reliance on screen scraping deliver significant benefits, though they also entail costs that should be managed carefully to avoid unintended consequences. On the benefits side, API-based data access represents a major improvement in security, efficiency, and reliability compared to screen scraping. APIs provide standardized data formats, auditable transaction records, and more stable connections, all of which support the Bureau's objectives of enhancing consumer protection, fostering competition, and promoting innovation.

FDATA urges the Bureau to take a technology-neutral approach in implementing the PFDR Rule. While reducing reliance on credential-based screen scraping is a shared goal across the ecosystem, the Bureau should avoid imposing mandates or prohibitions on specific technologies, including legacy methods that may still serve as the only viable means of enabling consumer-permissioned data sharing for certain account types or data elements. A premature mandate from the CFPB restricting legacy access could inadvertently limit consumer choice and disrupt existing connections, particularly where APIs are not yet deployed or fully functional. The Bureau can instead accelerate the transition to secure, API-based access by expanding the scope of covered accounts and data elements under the PFDR Rule—ensuring that more account types and data elements are accessed via APIs without imposing any technology mandates on third parties or financial institutions pertaining to legacy methods of data access. Such an approach preserves consumer access and data portability while respecting the operational and cybersecurity realities faced by smaller financial institutions.

29. *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?*

The PFDR Rule provides strong, comprehensive protections to ensure that requests for consumer financial data are knowingly authorized by the individual consumer and that the data is shared only with the consumer or their authorized representative—not with malicious actors. Under the Rule, authorized third parties must present consumers with clear, conspicuous, and standardized authorization disclosures specifying the categories of data to be accessed, the purpose of that access, the duration of authorization, and the consumer's right to revoke consent at any time. Consumers must affirmatively provide consent and receive a copy of the authorization, ensuring transparency and traceability throughout the process.

The Rule also incorporates robust authentication workflows developed by the CFPB's recognized SSO, which ensures that access requests are validated and that identity verification is secure, consistent, and auditable. This framework shifts the market away from credential-sharing toward tokenized, API-based access—greatly reducing the risks of impersonation, phishing, or unauthorized collection of consumer information. In addition, covered persons and authorized third parties remain subject to the GLBA and the FTC's Safeguards Rule, providing overlapping layers of regulatory protection. These obligations, combined with prompt revocation rights and enforceable compliance oversight, ensure that consumer authorization is genuine, informed, and verifiable. Collectively, these measures fulfill both the letter and spirit of section 1033 by safeguarding consumers' data security while preserving their right to control, access, and share their financial information freely and safely.

D. Privacy Concerns in the Exercise of Section 1033 Rights

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

The PFDR Rule makes meaningful progress in advancing consumer privacy by codifying informed consent and authorization and requiring that all authorized third parties adhere to consistent security standards. These provisions strengthen consumer control, transparency, and accountability across the ecosystem, establishing a uniform baseline that applies equally to financial institutions, fintechs, and other third parties.

However, certain provisions—particularly those related to data use, authorization revocation, and authorization confirmation—would benefit from additional clarity and implementation guidance to ensure privacy protections are balanced with consumer choice and functionality. For example, the current revocation framework could unintentionally force deletion of historical transaction data that consumers wish to retain for legitimate purposes. Consider a tax preparation use case: a consumer who connects a financial data platform to automatically aggregate income, investment, and expense information would be subject to a requirement that the provider revoke account connections after 12 months, without exception. As a result, a tax preparation tool would be unable to maintain connectivity on behalf of a consumer who files in February one year and in March the next, even if the consumer has provided informed consent for those connections to remain active. Similarly, the authorization confirmation process could be manipulated by incumbents to introduce friction or steer consumers toward proprietary tools, impeding their ability to freely access or share data with trusted third parties.

In sum, while the PFDR Rule represents a substantial step forward in protecting consumer privacy, targeted clarifications on data use, revocation, provider confirmation, and parity would ensure protections enhance—rather than restrict—consumer autonomy, innovation, and competition. These refinements would strengthen both privacy and practicality, ensuring the rule delivers section 1033's promise of empowering consumers with secure, meaningful control over their financial data.

31. *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?*

FDATA and its member companies adhere to the fundamental belief that consumers are the best stewards of their own data and should retain full control over their financial data. With informed consent, a consumer should be permitted to enable the use of their data for any purpose they choose, and to revoke that consent and data access at any time.

With informed consumer consent, both financial institutions and non-bank financial technology providers may use consumer data for product development or analytics, though these activities vary widely in scope. The Bureau should focus on any amendments to its PFDR Rule on ensuring that consumers retain meaningful control and transparency over their financial data, rather than attempting to reconcile or equalize data licensure practices governed by a host of other statutes and requirements administered and overseen by other agencies, including the GLBA. Informed, affirmative consumer consent should remain the governing principle across all entities.

32. *How prevalent is the licensure or sale of consumer financial data by bank and non-bank financial institutions where consent to license or sale is part of a standard user agreement or privacy notice?*

Standard user agreements and privacy notices often include broad consent provisions that permit financial institutions to use or share consumer data for a range of purposes permitted under existing law.

These practices are well established and regulated through frameworks such as the GLBA and its implementing regulations. While the Bureau's Section 1033 authority does not extend to altering those frameworks, it can strengthen consumer protection by ensuring that when data is shared at a consumer's direction, such sharing is transparent, limited to the authorized purpose, and consistent across market participants. Both financial institutions and non-bank providers may leverage consumer data for service improvement, analytics, or product design. Accordingly, the Bureau's focus should remain on promoting clarity and comparability in consent mechanisms—not on redefining the underlying licensure or sale regimes established under other federal statutes.

33. *What is the prevalence of licensure or sale of consumer data by companies with a fiduciary duty to their clients?*

The licensure or sale of consumer data by companies with a fiduciary obligations underscores FDATA's view that informed consumer consent is the most appropriate means through which to exert control over whether and how consumer financial data may be shared.

34. *What estimates exist on the percentage of financial service platform users who actually read and/or understand user agreements and privacy notices in their entirety?*

Research consistently shows that only a very small percentage of financial services users read or fully understand user agreements and privacy notices in their entirety. Studies across industries have found that most consumers either skim such documents or do not review them at all, given their length, complexity, and legalistic language. This reality applies equally to financial institution-issued privacy notices and to the user agreements of fintech platforms—consumers rarely engage meaningfully with either.

For financial institutions, these notices are typically bundled into lengthy account-opening documents or annual disclosures that consumers often receive in the mail and disregard as junk. For fintechs, digital consent screens may be more accessible, but the underlying challenge remains that consumers do not generally parse or comprehend every term. This reality underscores why the PFDR Rule's requirement for clear, concise, and standardized authorization disclosures is so critical. Unlike the status quo, where consumer "consent" is often more theoretical than informed, the Rule provides a framework to ensure that permission for data access is genuine, understandable, and enforceable.

In short, most consumers do not read traditional agreements or notices in full, which is precisely why the Bureau must continue to emphasize standardized, consumer-friendly disclosures to give effect to section 1033's purpose.

E. Compliance Dates

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

Authorized third parties have encountered unexpected difficulties and costs in implementing the PFDR Rule. The 12-month reauthorization requirement has introduced additional strain, forcing entities to build costly re-permissioning systems that risk frustrating consumers and increasing abandonment rates.

Unresolved issues around TANs, including a lack of interoperability and practical implementation concerns, have added to compliance burdens without clear consumer benefit.

Collectively, these challenges highlight the need for targeted refinements to reduce friction and costs while preserving the PFDR Rule's core consumer-protection objectives. Revisions to these minor but important elements of the existing Rule could easily be implemented without any correlating delay in the Rule's compliance deadlines.

36. *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?*

If the Bureau were to make substantial revisions to the PFDR Rule, the implementation timeline would necessarily vary by the size and resources of the covered entity. Large financial institutions with significant compliance infrastructures and in-house technical capacity could reasonably be expected to comply within 12 to 18 months, as could most mid-sized firms that have already invested in modern API frameworks. Smaller and community institutions, however, would likely require 24 to 36 months to comply, given their heavier reliance on third-party providers and the longer development cycles needed to update legacy systems.

That said, it is important to emphasize that the industry has already invested significant time, capital, and technical resources preparing for the existing final rule. Allowing that rule to take effect as scheduled would therefore not impose substantial new compliance costs. On the contrary, reopening settled issues or layering on significant revisions would force stakeholders to retool ongoing implementation efforts, delaying consumer benefits, and multiplying expenses. Minor adjustments—such as modest disclosure changes or incremental modifications to consent flows—could be implemented relatively quickly across the board.

For these reasons, the most equitable and practical course is to permit the final rule to come into force as written, with staggered compliance deadlines by institution size (as the Bureau has already provided) to accommodate smaller institutions and ensure reliable, secure implementation across the ecosystem.

Conclusion

By building on, rather than abandoning the PFDR framework, the CFPB can ensure that the United States not only catches up to—but ultimately leads—the global movement toward open banking and open finance. A durable, well-implemented section 1033 rule will empower consumers and small businesses with true data mobility, drive innovation across financial services, and establish a more transparent, competitive, and secure marketplace.

To achieve these outcomes, the Bureau must preserve fee-free, consumer-permissioned access; ensure security parity across financial institutions, aggregators, and fintechs; uphold technological neutrality while remaining vigilant around the use of tools such as TANs; and recognize both fiduciaries and non-fiduciaries as proper representatives under the PFDR Rule's authorization procedure.

Equally important is adopting a pragmatic implementation strategy—one that meaningfully consults small entities through a formal SBREFA process, assesses the real-world costs and benefits of any revisions on small businesses, and provides the regulatory clarity and consistency necessary to guide investment and compliance. Any retreat from these principles' risks entrenching dominant incumbents, discouraging innovation, and delaying the tangible consumer benefits Congress envisioned under section 1033.

The Bureau's leadership at this juncture will determine whether the United States remains a fragmented outlier or embraces a modern, innovative financial ecosystem that rivals its global peers. FDATA and its members stand ready to support the Bureau in advancing a rule that restores consumer trust, promotes competition, spurs innovation, and unleashes economic prosperity and opportunity through open, permissioned, and secure data sharing. We urge the Bureau to move swiftly toward finalization of a durable, enforceable section 1033 rule that delivers on the promise of consumer financial data rights and cements America's position as a global leader in competitive, innovative, and prosperous open finance.

<u>About FDATA</u>

FDATA and our members have long advocated for the provision of a legal right for consumers, small businesses, investors, public benefits recipients, and others to safely and securely access and share their financial data electronically. Global experience in jurisdictions such as Brazil, India, the UK, the EU, Australia, and many others demonstrates that open banking frameworks grounded in legal rights to data access drive more inclusive, competitive, and fraud-resistant financial ecosystems. Our members' tools and platforms underscore this reality. Founded in 2018, FDATA represents financial technology firms that empower consumers and SMEs with innovative services ranging from personal finance management and lending tools to real-time payment solutions. Together, our members serve more than 100 million U.S. consumers and SMEs. All of these services are built on one core capability: the ability for customers to permission access to their financial data held by other providers.

Sincerely,

Steven Boms
Executive Director
FDATA