October 21, 2025

The Honorable Russell Vought
Acting Director
Consumer Financial Protection Bureau
1700 G Street, N.W.
Washington, D.C. 20552

Re: Personal Financial Data Rights Reconsideration (Docket No. CFPB-2025-0037)

Dear Acting Director Vought:

The American Financial Services Association (AFSA)[1] appreciates the opportunity to provide comments on the Consumer Financial Protection Bureau's (CFPB) advance notice of proposed rulemaking (ANPR) relating to Section 1033 of the Dodd-Frank Act and the Personal Financial Data Rights (PFDR) rule adopted in 2024.[2] As providers of various consumer financial products and services, AFSA members are eager to share their perspectives on the development of the PFDR.

******

AFSA Responses to Questions Posed in the ANPR (Responses in blue)

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 someone explicitly authorized to act on another's behalf, often with some level of trust or responsibility. This may include non-fiduciary third parties based on informed consent where the third party has a special relationship with the consumer and obligation to act in the consumer's best interests. Enabling wider data sharing would dilute any protective intent behind the term. A narrower interpretation, aligning with established legal concepts of agency or fiduciary duty (e.g., guardian, power of attorney, etc.), would better ensure consumer protection and accountability.

[1] Founded in 1916, the American Financial Services Association (AFSA) is the national trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including traditional installment loans, mortgages, direct and indirect vehicle financing, payment cards, and retail sales finance.
[2] 89 FR 90838 (November 18, 2024).

1750 H Street NW, Suite 650, Washington, DC, 20006 ▲ 202.296.5544 ▲ www.afsaonline.org ▲ @AFSA_DC

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?

   Third parties act on behalf of individuals without necessarily owing a full fiduciary duty, such as certain authorized users on accounts or individuals granted limited power of attorney for specific transactions. These relationships often involve clear limitations on authority and explicit consent for specific actions.

   Under Federal law, the process for a third-party authorization is often formal. The Fair Debt Collection Practices Act specifically provides for a consumer's representation by an attorney and the statute provides a mechanism for validating the attorney's representation. Under the Health Insurance Portability and Accountability Act Privacy Rule, a person authorized to act on behalf of a patient is deemed a "personal representative,"[3] This personal representative must have legal authority to make health care decisions on behalf of the patient. This typically involves the health care power of attorney or a legal guardian. The Social Security Act allows for "representative payees" if the Commissioner of Social Security determines that the interest of any individual would be served thereby regardless of the individual's legal competency.[4]

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 grouping of "agent, trustee, or representative" strongly suggests that "representative" should be interpreted similarly to "agent" and "trustee," implying a relationship rooted in fiduciary or quasi-fiduciary duties. If "representative" is limited to those with fiduciary duties, the distinction between "agent" and "representative" for Section 1033 purposes might be nuanced. An "agent" typically acts under specific instructions and control of the principal, while a "representative" could denote a broader, perhaps more discretionary, authority, but both generally entail a duty of loyalty and care. The critical commonality is the heightened duty to act in the consumer's best interest, which is often absent in purely contractual or consent-based third-party arrangements.

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?''

   - **Consumer protection focus:** An interpretation that prioritizes robust consumer protection, including clear accountability and liability for third parties handling sensitive

[3] *See* 45 CFR 502(g).
[4] *See* § 205 (j)(1)(A) of the Social Security Act.

financial data on behalf of the consumer. There should also exist a clear carve-out if there is evidence of abuse.

- **Consistency with existing law:** Aligning the definition with established legal frameworks for agency and fiduciary relationships in other financial regulations.
- **Specificity in a definition:** A specific definition with objective criteria regarding creation of the representative relationship will help participants ensure compliance.

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?

   While this might narrow the immediate pathways for data transfer, it would also elevate the standard of care and accountability for those handling consumer data, which is paramount for consumer trust and security. This could emphasize secure and responsible data handling over broad, unchecked access. It would compel third parties to adopt more rigorous security frameworks.

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?

   Standardized formats facilitate data exchange, however they do not inherently clarify the legal nature of the relationship between a consumer and their "representative."

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?

   - **Explicit, granular, and revocable consent:** Clear, affirmative consent for specific data elements and purposes, with easy revocation mechanisms.
   - **Clear scope of authority:** Well-defined limits on what data can be accessed and how it can be used.
   - **Identity verification:** Robust processes to verify both the consumer's identity and the third party's identity.
   - **Transparency:** Clear disclosures to the consumer about the third party's business model, data handling practices, and potential risks.
   - **Accountability framework:** Mechanisms for consumers to seek recourse if the third party misuses data or breaches security.

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?

1750 H Street NW, Suite 650, Washington, DC, 20006 ▲ 202.296.5544 ▲ www.afsaonline.org ▲ @AFSA_DC

AFSA is not aware of any such precedent.

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 Dodd-Frank Act did not specifically grant the CFPB authority to regulate fees in connection with Section 1033. Section 1033 is silent on cost allocation, and interpreting silence as a prohibition on cost recovery places an unfunded mandate on covered persons. Covered persons incur significant fixed and marginal costs to build and maintain secure data access infrastructure, respond to requests, and ensure compliance. The ability to recover reasonable costs is essential to support a thriving data sharing 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?

    Excessive or unreasonable fees could obstruct data access, a well-structured cost recovery mechanism would not. Prohibiting fees may obstruct the development of robust and secure data-sharing mechanisms by disincentivizing financial institutions from investing adequately in them. A reasonable fee structure could incentivize the development of high-quality, standardized APIs and robust security, ultimately benefiting consumers by providing reliable and secure access.

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?

    We do not have a cost estimate. However, stakeholders in this ecosystem are making the following investments including:

    - **API development and maintenance:** Designing, building, and continually updating secure APIs.
    - **Enhanced data security infrastructure:** Upgrading systems to handle increased data egress and third-party access securely, including encryption, access controls, and threat monitoring.
    - **Authorization and consent management systems:** Developing robust platforms for managing consumer consent, third-party authorization, and revocation.
    - **Compliance and legal overhead:** Establishing internal policies, training staff, and ensuring ongoing regulatory adherence.
    - **Audit and logging capabilities:** Implementing systems to track data access and usage for compliance and incident response.
    - **Third Party risk management.**

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?

We do not have an estimate. Costs would include:

- **Processing individual data requests:** Computing resources, staff time for verification, monitoring, and transfer.
- **Customer support:** Handling inquiries, troubleshooting access issues, and managing consent changes.
- **Ongoing security monitoring:** Real-time monitoring of API access and data transfers for anomalies or breaches.

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?

- **Fixed costs:** identity verification and consent management systems. This includes developing standards for proof of agency or fiduciary relationship.
- **Marginal costs:** Each request necessitates a verification step, which adds processing time and staff resources. This could involve reviewing documentation, multi-factor authentication, and ongoing monitoring of authorization status.

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?

AFSA is not aware of any such precedent.

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?

Yes, covered persons should absolutely be able to recover a reasonable rate for offsetting these costs.

- **Fairness:** It is fundamentally unfair to impose significant compliance and operational costs on covered persons without a mechanism for recovery, especially when these costs are incurred to facilitate a new consumer right.
- **Sustainability and Security:** Cost recovery ensures that financial institutions can invest adequately in the secure and robust infrastructure necessary for data sharing.

1750 H Street NW, Suite 650, Washington, DC, 20006 ▲ 202.296.5544 ▲ www.afsaonline.org ▲ @AFSA_DC

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?

    It is not clear that the Dodd-Frank Act authorizes the CFPB to impose caps on fees in connection with Section 1033.

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?

    Costs should not be borne by consumers directly.

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's reliance on existing GLBA standards and restrictions on screen scraping were a good start, but may not be fully adequate given the evolving threat landscape and the unique challenges of third-party data access.

    - **Third-party risk:** The primary gap is often the security posture of the third parties accessing the data, especially those without robust regulatory oversight. A covered person can only secure its own systems; the data once transferred to a third party is subject to that party's controls.
    - **Lack of direct oversight:** Financial institutions often lack direct oversight or audit rights over the information security practices of all third parties that might receive data.

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 can include:
    - **Secure API gateways:** Implementing and maintaining secure gateways for data exchange.
    - **Data encryption:** Robust encryption for data at rest and in transit.
    - **Access controls:** Granular access controls and identity and access management (IAM) systems.

- **Security monitoring tools:** Intrusion detection/prevention systems (IDPS), security information and event management (SIEM) systems, and data loss prevention (DLP) tools.
- **Vulnerability management:** Regular penetration testing, vulnerability scanning, and patching.

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?

    Fixed costs typically have a high initial outlay regardless of client numbers because the core infrastructure (APIs, security systems, compliance frameworks) must be built to a certain standard. While some solutions might scale with client numbers, the baseline investment is significant. For covered persons with few customers, these fixed costs represent a much higher per-customer burden, potentially making compliance disproportionately expensive.

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?

    Fiduciary relationships often come with stricter regulatory oversight regarding data protection, further incentivizing higher security standards.

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?

    AFSA is not aware of any such studies.

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?

    The cost could include:
    - **Investigation and remediation:** Forensic analysis, system patching.
    - **Notification costs:** Legal and administrative costs of notifying affected individuals.
    - **Credit monitoring and identity theft protection:** Providing services to affected clients for an extended period.
    - **Legal fees and settlements:** Costs associated with lawsuits, regulatory fines, and class-action settlements.
    - **Reputational damage:** Loss of customer trust and potential business impact.

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 institutions comply with GLBA Safeguards Rule standards and other guidance such as FFIEC, that include:

- **Multi-layered security:** Firewalls, intrusion detection, endpoint protection.
- **Encryption:** Data at rest and in transit.
- **Regular audits and assessments:** Internal and external security audits, penetration testing.
- **Employee training:** Mandatory security awareness training for all staff.
- **Incident response capabilities:** Dedicated teams and processes for managing security incidents. These controls are generally effective for data within our direct control.

The challenge with Section 1033 arises when data is transmitted to and subsequently handled by third parties whose security postures may not be as robust or transparent.

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?

The PFDR Rule's interface access provision could better allow covered persons to satisfy these obligations by:

- **Requiring robust third-party identity verification:** Ensuring that third parties are legitimate and not front companies for illicit activity.
- **Mandating audit trails:** Requiring third parties to maintain and provide audit trails of their data access and usage to covered persons.
- **Enabling real-time monitoring:** Allowing covered persons to monitor data access for suspicious patterns that might indicate BSA/AML or fraud risks.
- **Clear liability frameworks:** Establishing clear liability for third parties that compromise BSA/AML or fraud controls.

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

Benefits:

- **Familiarity:** GLBA standards are well-established and familiar to financial institutions, leveraging existing compliance programs.
- **Foundation:** GLBA provides a baseline for security practices, ensuring a minimum level of protection.

1750 H Street NW, Suite 650, Washington, DC, 20006 ▲ 202.296.5544 ▲ www.afsaonline.org ▲ @AFSA_DC

- **Reduced burden for initial implementation:** Avoids the need to create entirely new, potentially conflicting, security frameworks.

Limitations:

- **Scope limitations:** GLBA primarily covers the financial institution's own data handling. It does not directly regulate the security practices of unregulated third parties once data is transferred.
- **Lack of specificity for APIs:** GLBA was not designed with API-based data sharing in mind, so specific guidance for this context may be lacking.

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 accessing consumer financial data should adhere to robust information security standards, ideally equivalent to, or exceeding, those applicable to the covered financial institutions themselves, such as the GLBA Safeguards Rule and potentially more specific API security standards (e.g., NIST Cybersecurity Framework, ISO 27001, or industry-specific API security best practices). Access by authorized users should have a limited duration, requiring reauthorization to access again.

FTC could play a role for non-bank entities. However, given the complexity and financial nature of the data, a collaborative approach might be best. The CFPB, in conjunction with the FTC and prudential regulators, could establish clear guidelines and enforcement mechanisms. The key is that there must be *some* regulatory body with clear authority and expertise to evaluate and enforce these standards on all entities in the data chain, especially data aggregators, who currently operate with less direct oversight.

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?

Costs of reducing screen scraping:

- **Initial investment in APIs:** Covered persons incur significant costs to develop and maintain robust APIs as an alternative to screen scraping.

Benefits of reducing screen scraping:

- **Enhanced security:** Eliminates the need for consumers to share their credentials with third parties, significantly reducing credential compromise risks. This is a major benefit.
- **Improved control:** APIs allow covered persons to exert more control over the data being shared and to monitor access.
- **Better user experience:** APIs can provide more reliable and faster data access than screen scraping.

Changes to better protect consumer credentials:

1750 H Street NW, Suite 650, Washington, DC, 20006 ▲ 202.296.5544 ▲ www.afsaonline.org ▲ @AFSA_DC

- **Mandatory API-only access:** Prohibit screen scraping entirely for covered data as soon as viable API alternatives are in place.
- **Strong authentication for APIs:** Require secure authorization frameworks where consumers directly authorize data sharing without divulging credentials to third parties.
- **Revocation mechanisms:** Easy-to-use and immediate mechanisms for consumers to revoke third-party access.

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 aimed to provide protections through informed consent requirements. Requiring granular consent for specific data types and uses, presented in plain language, would improve this. Periodic re-authorization could be a valuable mechanism to ensure ongoing, active consent and prompt consumers to review their sharing permissions. Even with consent, robust identity verification of both the consumer and the third party is crucial to prevent malicious actors from impersonating either. The Rule needs to clarify the process and liability for verifying the legitimacy of the third party and the consumer's request.

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, as structured, likely does *not* provide adequate protection of consumer privacy, primarily due to the lack of clear regulatory authority and oversight over data aggregators and other third parties once they possess the data.

- **Data Aggregator Oversight:** Financial institutions cannot reasonably be expected to monitor and manage the privacy controls of every data aggregator or third party that accesses consumer data. These entities are not service providers to the covered institution in the traditional sense.
- **Secondary Use of Data:** The Rule needs stronger provisions limiting the secondary use, sale, or licensing of consumer data by third parties, especially for purposes unrelated to the consumer's initial authorization. The ANPR itself highlights concerns about "unwitting licensing or sale of sensitive personal financial information."
- **CFPB Role:** The CFPB should indeed take responsibility for regulating data aggregator practices. Promulgating a "large participant rule" for data aggregators or similar regulatory framework would be a crucial step to ensure consistent privacy standards and accountability across the entire data ecosystem. This would also address the competitive imbalance where regulated financial institutions operate under strict privacy rules, while some data aggregators do not.

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?

Regulated financial institutions operate under strict privacy regulations (e.g., GLBA) that generally restrict the sale or licensing of customer financial data without explicit consent or within defined exceptions. The regulations provide clear opt-out mechanisms for certain types of data sharing with affiliates or non-affiliated third parties for marketing purposes.

However, for unregulated data aggregators, the prevalence of data licensure or sale might be higher, and the mechanisms for consumer choice (opt-in/opt-out) can vary significantly and may not always be transparent or easily understood by consumers. While specific data on the balance between opt-in and opt-out regimes is difficult to quantify without comprehensive studies, it is often observed that opt-out is the default for many non-essential data sharing activities where permitted, placing the burden on the consumer. Consumers are usually unaware of the licensure or sale of their data, as this undermines informed consent. It is important to note that the current PFDR Rule does not impose any restrictions on data provider financial institutions' use, licensing, selling, or sharing of consumer data, meaning it doesn't directly address this concern.

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?

It is highly prevalent for consent to data sharing, including potential licensing or sale where permitted, to be embedded within standard user agreements or lengthy privacy notices, particularly across digital finance and data brokerage generally. Many firms rely on "clickwrap" agreements or policy notices rather than granular, purpose-specific opt-ins.

The CFPB and numerous researchers have highlighted the opacity and length of these policies and the fact that consumers rarely read them, significantly weakening the quality of such "consent." Consumer Financial Protection Bureau

This practice often leads to consumers unknowingly agreeing to terms that grant broad data usage rights.

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

Hard prevalence numbers for the licensure or sale of consumer data by companies with a fiduciary duty are not widely published. However, entities such as broker-dealers and

investment advisers are subject to regulations like Regulation S-P and fiduciary duties under Regulation Best Interest (Reg BI).

These obligations generally discourage the disclosure or sale of nonpublic personal information, except where explicitly permitted with proper notice and opt-out options, and only with robust safeguards in place. Consequently, many such firms actively avoid selling identified client data, focusing instead, if at all, on aggregated or anonymous analytics. Therefore, the prevalence of such activities by fiduciaries is likely very low compared to non-fiduciary entities.

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?

Estimates consistently show that a very low percentage of users actually read and fully understand user agreements and privacy notices in their entirety, a trend observed across various industries, not just financial services. This reality significantly undermines the concept of informed consent. For instance:

- A 2008 study by McDonald & Cranor estimated that reading all online privacy policies would take an individual approximately 201–244 hours per year, highlighting the impracticality for consumers. lorrie.cranor.org
- Research by Obar & Oeldorf-Hirsch, often referred to as "The Biggest Lie on the Internet," found that roughly 75–98% of participants did not meaningfully read policies, with average reading times around 70–80 seconds. A significant majority missed "gotcha" clauses embedded within the terms. biggestlieonline.com
- More recently, a 2023 Pew Research Center study indicated that 67% of U.S. adults feel they understand little to nothing about how companies handle their personal data. Pew Research Center

These findings underscore the challenge of relying on lengthy legal documents for obtaining true consumer consent regarding data practices.

Compliance Dates

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

Yes. Key challenges include:

- API Development and Maintenance: Building and maintaining standardized APIs that meet requirements for "commercially reasonable performance," telemetry, denial documentation, and monthly metrics represent a substantial engineering and ongoing operational cost.

- Consent Management: Designing and implementing robust consent flows, clear authorization disclosures, efficient revocation handling mechanisms, and precise scope management for data sharing is complex.
- Security Program Alignment and Due Diligence: Ensuring alignment with existing security standards (like GLBA/FTC Safeguards) and conducting thorough due diligence on third parties accessing data requires significant resources.
- Uncertainty and Re-planning: The phased compliance schedule, tied to asset and receipt size, combined with the uncertainty arising from litigation and the CFPB's reconsideration, has led to significant re-planning costs for many entities.

Also, the litigation challenging the PFDR Rule and changes in CFPB priorities have affected industry's understanding of the validity and stability of the rule. In light of these challenges, the CFPB should promptly suspend compliance dates on the current Section 1033 Rule in order to prevent waste of resources.

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, a significant implementation period would be necessary to allow covered entities to adapt their systems and processes. The original PFDR Rule established a phased schedule for compliance, roughly from April 1, 2026, to April 1, 2030, based on entity size, and the CFPB is currently considering extensions during reconsideration; a 90-day stay has already been noted in commentary.

Should revisions be substantial—for example, introducing new scope or definitions, altering consent standards, changing interface performance requirements, or adjusting liability frameworks—reasonable implementation windows, based on prior timelines and typical bank change cycles, would likely be on the order of:

- Largest providers: Would likely require 24 -30 months from the date of finalization to achieve production readiness. While these firms may have already invested in API programs, substantial revisions would necessitate significant re-work and testing.
- Mid-size entities: Would likely need 30 –36 months. These entities often have greater dependency on vendors and standard-setting bodies (SSBs), leading to longer contract and integration cycles.
- Small entities: Would likely require 36 months. They typically face greater resource constraints and rely more heavily on vendor APIs and the evolution of recognized standards, which have only recently been framed by the rule.

This spread in implementation time is primarily due to the differing capabilities and resources across institutions. Larger firms often possess dedicated open-banking teams that

can parallelize engineering and compliance efforts. Smaller providers, conversely, depend on vendor availability and the finalization of recognized standards, which can take more time to mature and integrate.

******

We appreciate the opportunity to provide feedback on issues relating to the PFDR and Section 1033 generally. Please let me know at 202-466-8605 or pbohi@afsamail.org if you have any questions.

Philip Bohi
General Counsel
American Financial Services Association