4810-AM-P

CONSUMER FINANCIAL PROTECTION BUREAU

12 CFR Part 1033

[Docket No. CFPB-2025-0037]

RIN 3170-AB39

Personal Financial Data Rights Reconsideration

AGENCY: Consumer Financial Protection Bureau.

ACTION: Advance notice of proposed rulemaking.

SUMMARY: The Consumer Financial Protection Bureau (CFPB or Bureau) is seeking comments and data to inform its consideration of four issues related to implementation of section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). These issues are: the proper understanding of who can serve as a "representative" making a request on behalf of the consumer; the optimal approach to the assessment of fees to defray the costs incurred by a "covered person" in responding to a customer driven request; the threat and cost-benefit pictures for data security associated with section 1033 compliance; and the threat picture for data privacy associated with section 1033 compliance.

DATES: Comments must be received on or before [**INSERT DATE 60 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER***].

ADDRESSES: You may submit responsive information and other comments, identified by Docket No. CFPB-2025-0037 by any of the following methods:

- *Federal eRulemaking Portal: https://www.regulations.gov.* Follow the instructions for submitting comments.
- *Email:* 2025-ANPR-PersonalFinancialDataRights@cfpb.gov. Include Docket No. CFPB-2025-0037 in the subject line of the message.

- *Mail/Hand Delivery/Courier:* Comment Intake — Personal Financial Data Rights Reconsideration, c/o Legal Division Docket Manager, Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

Instructions: The CFPB encourages the early submission of comments. All submissions should include the agency name and docket number. Additionally, where the Bureau has asked for specific comment on a topic, commentors should seek to highlight the topic to which its comment is applicable. Because paper mail is subject to delay, commenters are encouraged to submit comments electronically. In general, all comments received will be posted without change to *https://www.regulations.gov.*

All submissions, including attachments and other supporting materials, will become part of the public record and subject to public disclosure. Proprietary information or sensitive personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included. Submissions will not be edited to remove any identifying or contact information.

FOR FURTHER INFORMATION CONTACT: Dave Gettler, Paralegal Specialist, Office of Regulations, at 202–435–7700 or at: https://reginquiries.consumerfinance.gov/. If you require this document in an alternative electronic format, please contact *CFPB_Accessibility@cfpb.gov*.

SUPPLEMENTARY INFORMATION:

I. Background

Technology has made it possible to store, analyze, and share personal financial data electronically, and interest has grown within the financial services industry and among policymakers in the potential benefits of bolstering consumers' rights to access personal financial data. Consistent with this desire to increase consumers' access to their financial information, section 1033(a) of the Dodd-Frank Act provides that, subject to rules issued by the CFPB, consumers shall have access to requested information in the control or possession of financial entities relating to the products or services obtained from those financial entities.

Section 1033 of the Dodd-Frank Act, codified as 12 U.S.C. 5533, outlines the requirement for "covered persons" to make financial transaction data available to consumers and authorized third parties upon request, under rules prescribed by the Bureau. The statutory text of section 1033 is quite sparse and does not specifically address several important questions that arise from the rights it creates, in particular: a) precisely who may act on behalf of the consumer; b) how the costs of effectuating such rights may be defrayed by the "covered person" providing the data; c) the potential negative consequences to the consumer of exercising this right in an environment where there are tens of thousands of malign actors regularly seeking to compromise data sources and transmissions; d) the potential negative consequences to the consumer in exercising this right where the data contains information that the consumer may not want disclosed, but does not fully understand or realize may be disclosed by the third party through which it has made a request; and e) the potential benefits to consumers or competition of facilitating the consumer-authorized transfer of data to financial technology companies, application developers, and other third parties.

The structure of section 1033 consists of the following:

- A general articulation of the scope of the information that may be obtained by the consumer. (Sub-section A)
- An explicit list of exceptions laying out information a covered person is not required to provide. (Sub-section B)
- An explicit statement that section 1033 does not impose any duty on a covered person to maintain or keep any information about a consumer. (Sub-section C)
- Authorization for the CFPB to prescribe standards for how information will be transmitted to consumers. (Sub-section D)
- The inter-agency consultation requirements when prescribing rules implementing section 1033. (Sub-section E)

On November 18, 2024, the Bureau published the Personal Financial Data Rights final rule (PFDR Rule) under section 1033.[1] In general, the PFDR Rule applies to financial institutions, which it describes as "data providers," that issue credit cards, hold transaction accounts, issue devices to access an account, or provide other types of payment facilitation products or services. The rule generally requires these financial institutions to provide information about transactions, costs, charges, and usage to consumers upon request. And the rule contains additional provisions regulating how covered data are to be made available and the mechanics of data access, and provisions establishing authorization procedures and obligations for third parties seeking to access covered data from data providers. A bank, a national trade association representing banks, and a State trade association representing banks filed a lawsuit challenging the PFDR Rule in the United States District Court for the Eastern District of Kentucky.[2] On July 29, 2025, the court granted a motion to stay proceedings in the case, following the Bureau's announcement that it "seeks to comprehensively reexamine this matter alongside stakeholders and the broader public to come up with a well-reasoned approach . . . that aligns with the policy preferences of new leadership and addresses the defects in the [PFDR Rule]."[3]

II. Executive Order 12866

The Office of Information and Regulatory Affairs within the Office of Management and Budget (OMB) has determined that this action is a "significant regulatory action" under Executive Order 12866, as amended. Accordingly, the OMB has reviewed this action.

III. Questions

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

---

[1] 89 FR 90838 (Nov. 18, 2024). In June 2024, the Bureau finalized a portion of the proposal, regarding attributes a standard-setting body must possess to receive CFPB recognition and establishing the application process for CFPB recognition. 89 FR 49084 (June 11, 2024). The June 2024 rule was then incorporated into the November 2024 final rule.

[2] *Forcht Bank, N.A. v. CFPB*, No. 5:24-cv-00304 (E.D. Ky. 2024).

[3] Order Granting Motion to Stay, No. 5:24-cv-00304 (July 29, 2025) (ECF No. 83).

As the term is used in section 1033 of the Dodd-Frank Act, a "consumer" is defined as an individual or an agent, trustee, or representative acting on behalf of an individual. 12 U.S.C. 5481(4). At common law, an agent has fiduciary duties such as those of care, loyalty, good faith, and confidentiality. Also at common law, a "trustee" has these fiduciary duties as well as any specific duties that are required by the terms of the trust. The PFDR Rule interpreted the phrase "representative acting on behalf of an individual" to include third parties that access consumers' data pursuant to certain authorization procedures and substantive obligations.[4] The Bureau estimated that "more than 100 million consumers have used consumer-authorized data access" in the U.S. via third parties as of 2024.[5] The Bureau is seeking comments generally on the proper scope of how the term "representative" should be interpreted. Specifically, the Bureau requests comments on the following questions:

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?
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?
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?
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?"

[4] *See* 12 CFR part 1033, subpart D.
[5] *See* 89 FR 90838 at 90958.

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?
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?
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?
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?

Defrayment of Costs in Exercising Rights Under Section 1033

Under current § 1033.301(c)(1) and (2), provisions finalized as part of the PFDR Rule,[6] a data provider must not impose any fees or charges on a consumer or an authorized third party in connection with establishing or maintaining the required consumer and developer interfaces or receiving requests or making available covered data in response to requests as required by part 1033. Section 1033 of the Dodd-Frank Act, however, is silent on the question of how the burden of consumers' exercise of the rights it creates should be shared between the consumer and the "covered person." The Bureau is seeking comments and data generally on how to deal with this

[6] 89 FR 90838 at 90884-87.

omission, and whether costs, benefits, or market forces might justify modifying the PFDR Rule's provisions. Specifically, the Bureau requests comments and data on the following questions:

9. Does the PFDR Rule's prohibition on fees represent the best reading of the statute? Why or why not?
10. Was the PFDR Rule correct to conclude that permitting fees "would obstruct the data access right that Congress contemplated"? Why or why not?
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?
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?
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?
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?
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?

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?
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?

Information Security Concerns in the Exercise of Section 1033 Rights

One unfortunate byproduct of the transition to a largely digital information architecture is the increased number of threat vectors to the secure storage and transmission of data. In the context of the PFDR Rule, in which several types of covered persons are engaged in the use, retention, and transmittal of consumer financial data, adequate information security standards and controls must be in place to guard against malicious actors, including fraudsters, scammers, and "Business Email Compromise" or "BEC" perpetrators.[7]

The existence of data breaches is a constant threat and has affected some of the most sophisticated and well-financed institutions including: Yahoo (2013 and 2014); the Office of Personnel Management (2015); Equifax (2017); Marriott (2018); LinkedIn (2019); Facebook (2019); and OCC (2025). All it takes is a single mistake in compromising internal data security protocols for an enormous amount of personal information, including personally identifiable information (PII), to become available to malign actors and available for sale on the dark web. The risks regarding improper transmission of personal financial data underscore the need to ensure that entities authorized to access that information have appropriate safeguards in place.

The PFDR Rule attempted to address information security in several ways. It prohibited data providers from relying on a third party's use of screen scraping to access the developer

[7] The Federal Bureau of Investigation has estimated that BEC has caused $55 billion in losses between 2013 and 2023. *See* Fed. Bureau of Investigation, *Business Email Compromise: The $55 Billion Scam*, https://www.ic3.gov/PSA/2024/PSA240911 (last visited Aug. 1, 2025).

interface required by the rule and discouraging the use of screen scraping by third parties when more secure methods of data access were available; required data providers and third parties to adhere to the applicable information security standards under the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. 6801; and provided that data providers may deny access to consumers or third parties if granting access is inconsistent with policies and procedures reasonably designed to comply with the GLBA's information security standards.

The Bureau is seeking comments and data generally on the threat and cost-benefit of securing consumer financial data both in storage and in transit by consumers, including any information security developments that might justify modifying the PFDR Rule's provisions. Specifically, the Bureau is seeking comments and data on the following questions:

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

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

Privacy Concerns in the Exercise of Section 1033 Rights

A consumer's financial transactions reveal an enormous amount of information about their habits and lifestyle. Even for those who are comfortable with the existence of an extensive digital record that can often accurately be used to predict their behavior, there is certain information that few individuals may not want revealed to everyone and anyone, sometimes even those closest to them. Such information includes transaction data that reveals the existence of: a) medical conditions; b) financial vulnerability; c) financial abundance that could make them the target of criminal activity; and d) substance abuse problems or other high-risk behaviors. So long as the information is limited to the consumer, the "covered persons" they use, and the authorized third parties who are given access to that information, the consumer is able to better calibrate the level of privacy they maintain.

Financial institutions collect, use, and disclose data in many ways that impact consumer privacy. One major privacy threat is when customers are unaware of ongoing licensure or sale of their data. The percentage of service platform users who actually read user agreements is very low.[8] While such individuals are responsible for the consequences of such inattentiveness, it does not reduce the potential annoyance or harm from use of that data to target an individual for financial profiling and aggressive marketing.

Subpart D of the PFDR Rule required third parties to obtain a consumer's express informed consent to access covered data on behalf of the consumer, prescribed what a third party must disclose to a consumer, and limited a third party's collection, use, and disclosure of covered data.[9] The Bureau is seeking comments and data generally on the threats to data privacy as a result of unwitting licensing or sale of sensitive personal financial information, and on any

---

[8] *See, e.g.*, Pew Rsch. Ctr., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, at 38 (Nov. 2019) (poll of American adults finding that nine percent reported that they "always" read privacy policies).

[9] *See* 12 CFR 1033.401(c) (requiring consumer's express informed consent to access covered data on behalf of the consumer by obtaining an authorization disclosure that is signed by the consumer electronically or in writing); 12 CFR 1033.411(b) (specifying content requirements for the authorization disclosure); 12 CFR 1033.421 (explaining a third party's obligations with respect to the collection, use, and retention of covered data). The PFDR Rule also requires third parties to provide the consumer with a copy of the authorization disclosure that the consumer has signed electronically or in writing and that reflects the date of the consumer's electronic or written signature. 12 CFR 1033.421(g)(1).

modifications to the PFDR Rule's provisions. Specifically, the Bureau is seeking comments and data on the following questions:

30. Does the PFDR Rule provide adequate protection of consumer privacy? Why or why 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?
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?
33. What is the prevalence of licensure or sale of consumer data by companies with a fiduciary duty to their clients?
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?

Compliance Dates

The PFDR Rule included a series of compliance dates by which data providers would need to comply with the requirements in subparts B and C of the PFDR Rule.[10] These compliance dates were determined by the size of the entity, and ran from April 1, 2026, through April 1, 2030.[11] As part of its reconsideration of the PFDR Rule, the Bureau plans to issue a Notice of Proposed Rulemaking to extend the compliance dates. The Bureau is seeking comments and data generally on the appropriateness of the compliance dates in the PFDR Rule,

[10] The PFDR Rule did not set explicit compliance dates for third parties that receive data on the grounds that their compliance was functionally tied to compliance by data providers.
[11] Pursuant to a court order, the compliance dates have been stayed by 90 days. Thus, the first compliance date is now June 30, 2026.

and what extension may be appropriate. Specifically, the Bureau is seeking comments and data on the following questions:

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

Russell Vought,

Acting Director, Consumer Financial Protection Bureau.

[FR Doc. 2025-16139 Filed: 8/21/2025 8:45 am; Publication Date: 8/22/2025]