October 21, 2025

Submitted via Regulations.gov
Comment Intake
c/o Legal Division Docket Manager
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Personal Financial Data Rights Reconsideration Docket No. CFPB–2025–0037/ RIN 3170–AB39

The undersigned fifty-two (52) consumer, economic justice, privacy, and advocacy groups submit these comments in response to the Consumer Financial Protection Bureau's (CFPB) Advance Notices of Proposed Rulemaking (ANPR)[1] reconsidering its final Personal Financial Data Rights rule implementing section 1033 of the Dodd-Frank Act, codified at 12 C.F.R. Part 1033. We strongly support the current 1033 Rule as issued in October 2024[2] and urge the CFPB to retain its provisions without modification. We especially urge the CFPB to keep the excellent and thoughtful consumer protections of the Personal Financial Data Rights Rule (the 1033 Rule or Rule) at 12 C.F.R. §§ 1033.411 and 1033.421, which are among the best-in-class for data privacy safeguards in the United States.

The ANPR seeks comment on four issues specifically:

1. Who can serve as a ''representative'' making a request on behalf of the consumer.

We believe that any third party that a consumer knowingly and explicitly authorizes to access their own data, including but not limited to data aggregators, should be considered an agent or representative, given that the strong consumer protections of the rule ensure the third party is acting in the consumer's interest. ***If Section 1033 does not govern consumer-authorized data accessed by third parties, and data is only accessed via bilateral agreements or screen scraping, both consumers and data providers may be left unprotected without the strong privacy protections in the 1033 Rule.***

2. Whether to allow the assessment of fees for data access pursuant to a Section 1033 request.

We strongly support the 1033 Rule's ban on fees and urge the CFPB to retain it. Consumers should not be charged for exercising a statutory right. Even if the Rule prohibits data providers from charging fees directly to consumers, but allows them to

[1] CFPB, Personal Financial Data Rights Reconsideration, 90 Fed. Reg. 40,986 (Aug. 22, 2025).

[2] CFPB, Required Rulemaking on Personal Financial Data Rights, 89 Fed. Reg. 90838 (Nov. 18, 2024).

charge fees to third-party users or aggregators, such costs will ultimately end up being paid for by the consumer.

3. Data security for information accessed pursuant to the 1033 Rule.

The 1033 Rule subjects third parties accessing consumer-authorized data to the data security requirements of the Federal Trade Commission (FTC) Safeguards Rule, which is as strong as or even stronger than the Interagency Guidelines Establishing Information Security Standards that depository institutions are subject to. While data security could be improved, that is not a reason to narrow the scope of the 1033 Rule.

4. Data privacy for information accessed pursuant to the 1033 Rule

The consumer protections in the 1033 Rule are best-in-class, including prohibitions on secondary use, requirements for data minimization, a one-year limit for authorizations, clear segregated disclosures for authorization, and a requirement to delete data once there is no longer authorization. These protections not only safeguard consumers, they benefit data providers by limiting the amount, usage, and retention of the data. If the Rule does not cover third parties when they access consumer-authorized data, including when screen scraping, both consumers and data providers will be left vulnerable.

**A. Consumers Benefit Greatly from the Uses Enabled by the 1033 Rule**

Consumers derive enormous benefit from being able to share bank account and credit card transaction information, including via data aggregators. The uses enabled by the ability to use consumer-authorized data include:

- Cashflow underwriting: American consumers desperately need to have an alternative to the Big Three credit bureaus. That competition could come from the use of consumer-authorized data accessed via data aggregators of bank account transaction information, *i.e.*, "cashflow underwriting." There are already promising cashflow underwriting projects, such as the ones piloted by Fannie Mae and Freddie Mac.[3] Cashflow underwriting will also help the tens of millions of credit invisible and thin file consumers without exposing them to the downsides posed by alternative data added to traditional credit reports.
- Personal financial management: Consumer-authorized data allows consumers and their financial advisors to more easily manage their finances across multiple accounts at

[3] Press Release, Fannie Mae Introduces New Underwriting Innovation to Help More Renters Become Homeowners August 11, 2021, https://www.fanniemae.com/newsroom/fannie-mae-news/fannie-mae-introduces-new-underwriting-innovation-help-more-renters-become-homeowners; Press Release, Company will factor on-time rent payments into loan purchase decisions, June 29, 2022, https://freddiemac.gcs-web.com/news-releases/news-release-details/freddie-mac-takes-further-action-help-renters-achieve.

financial institutions and other data providers, providing valuable insights and enabling better administration of their finances.

- Tax Preparation – The use of consumer-authorized data helps taxpayers easily access IRS Form-1099 data from financial institutions and investment firms, which can then be integrated into commercial tax software, saving countless hours and much frustration during tax filing season.
- Switching Depository Institutions – One of the most promising uses of consumer-authorized data is to allow consumers to switch financial institutions for their deposit accounts. The ability to switch banks more easily could result in consumers earning billions more in interest.[4]
- Pay by bank – Another promising use of consumer-authorized data is to enable consumers to pay with their bank account credentials, which will save merchants billions in interchange fees.[5] Those savings may also benefit consumers, as interchange fees are ultimately reflected in the prices of goods and services.

The CFPB developed the provisions of the 1033 Rule to enable consumers to reap these benefits. But it appears that the current administration intends to revise the 1033 Rule in a way that will stymie or even eliminate those benefits, either by allowing data providers to charge fees that will make these uses more costly or uneconomical, or even by preventing third parties from being able to carry out the wishes of consumers to access their own data for these beneficial purposes.

To support innovation and safety, the CFPB must force the market to move away from screen scraping, which can only be done if data providers are required to make access available via the 1033 Rule. Screen scraping is a dangerous and outmoded technology that makes accounts vulnerable to compromise, limits consumer control over how their data is used, and places added burdens on data providers. It increases the likelihood of phishing attacks, exposes sensitive login credentials, and is prone to malfunctions.[6] To the extent that some banks will offer APIs while others will not, the slow transition to open banking will favor large banks and incumbent relationships over smaller financial institutions and competitors seeking new customers in the United States.[7]

---

[4] Dion Rabouin, Ditching Big Banks Could Have Saved Americans $42 Billion More in Interest, Wall St. J., Jan. 6, 2023, https://www.wsj.com/story/ditching-big-banks-could-have-saved-americans-42-billion-more-in-interest-24cf979b.

[5] Press Release, National Retail Federation, Retailers Say CFPB Open Banking Rules Could Reduce Need for 'Swipe' Fees and Save Consumers Billions, October 22, 2024, https://nrf.com/media-center/press-releases/retailers-say-cfpb-open-banking-rules-could-reduce-need-swipe-fees-and.

[6] Aibangbee, Y. (2024, November 26). Screen Scraping: What Is It and How Does It Work? *Bank Policy Institute*. https://bpi.com/screen-scraping-what-is-it-and-how-does-it-work/

[7] Lin, X., Zhang, S. S., & Zachariadis, M. (2025). Open data and API adoption of U.S. banks. *Journal of Financial Intermediation*, *63*, 101162. https://doi.org/10.1016/j.jfi.2025.101162

**B. Our Responses to the Issues Posed by the ANPR**

*1. Prohibiting consumers from sharing their own data with their authorized agents and representatives is contrary to the letter and spirit of Section 1033.*

The Dodd-Frank Act clearly permits the CFPB to allow consumers to authorize third-party agents or representatives to access their data. Section 1033 provides "a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person,…". 12 U.S.C. § 5533. In turn, Section 1002(4) of the Dodd-Frank Act defines "consumer" to include "an agent, trustee, or representative acting on behalf of an individual." 12 U.S.C. § 5841(4).

Treating authorized third parties, such as users or data aggregators, as agents or representatives of the consumer is directly supported by the definition of "consumer" in the Dodd-Frank Act. And allowing access to legally restricted data pursuant to the consumer's authorization is a common practice. For example, one of the permissible purposes of the Fair Credit Reporting Act allows a consumer reporting agency to share a consumer report "in accordance with the written instructions of the consumer to whom it relates" 15 U.S.C. § 1681b(a)(2). Frankly, it seems bizarre to give the consumer the right to access their own data but prohibit them from sharing that same data with a third party selected by the consumer to help facilitate a usage that the consumer desires to engage in.

Furthermore, the strong consumer protections in the current 1033 Rule work hand in hand in defining the role of a third party to ensure they are actually acting as the agent or representative of the consumer. For example, the current rule prohibits most secondary use of the data and requires the third party or user to only obtain what data is necessary (data minimalization). This ensures that third parties are acting in the best interests of the consumer, which comports the notion that they are the consumer's agent or representative. At common law, an agent who acts on behalf of a principal has a fiduciary relationship to that principal,[8] and is prohibited from using the principal's confidential information for its own benefit.[9] Thus, the consumer protections in the current rule serve to define a relationship to parallel the role of agent at common law.

The text of Section 1033 shows that Congress contemplated that third parties would access a consumer's information at the consumer's request. Section 1033 requires the CFPB to "promote the development and use of standardized formats for information, including through the use of machine-readable files,…" 12 U.S.C. § 5533(d). Information provided in a machine-readable file necessarily involves an intermediary since such a format is not directly readable by

[8] Restatement (Third) Of Agency § 8.01 (2006) ("An agent has a fiduciary duty to act loyally for the principal's benefit in all matters connected with the agency relationship").

[9] *Id.* at § 8.05 ("An agent has a duty … (2) not to use or communicate confidential information of the principal for the agent's own purposes or those of a third party.)

consumers, which shows Congress contemplated that third parties would be involved in accessing consumer data shared pursuant to Section 1033.

Finally, some data providers have claimed that eliminating the ability of third-party aggregators or other representatives will not hinder the development of open banking because aggregators will still be able to access the data via bilateral agreements. But that is the worst outcome for consumers, and less than optimal for data providers. First, that outcome would result in aggregators continuing to access data via screening scraping if they do not have a bilateral agreement with a data provider. Second, a system of bilateral agreements will undermine competition because large financial institutions will use their market power to negotiate favorable terms not available to smaller institutions. Finally and most importantly, ***if Section 1033 does not govern account data accessed by aggregators, then the strong consumer protections of the 1033 Rule do not apply.*** Consumers will be left unprotected without the privacy safeguards of the 1033 Rule and subject to abuses such as secondary use of data for target marketing or aggregators taking more data than necessary for a particular usage. As discussed in Section 4 below, these protections also benefit data providers, while their elimination actually benefits aggregators.

*2. The CFPB Should Retain the Prohibition Against Data Providers Charging Fees for Consumer-Authorized Data Access*

The current 1033 Rule contains a firm prohibition against data providers charging fees for access to consumer-authorized data. 12 C.F.R. 1033.301(c). We strongly support this ban on fees and urge the CFPB to retain it. Consumers should not be charged for exercising a statutory right. Allowing data providers to charge a fee significantly impedes and undermines the consumer's ability to do so. Even a small fee could deter consumers from accessing their own information,[10] and constitute a de facto nullification of Section 1033 information, contrary to Congress's intent in passing Section 1033.

Even if the 1033 Rule prohibits data providers from charging fees directly to consumers, but allows them to charge fees to aggregators, those costs will ultimately end up being paid for by consumers. It will also encourage aggregators to use screen scraping instead of application programming interfaces (APIs). Allowing data providers to charge fees to aggregators will also stymie the positive uses of data, such as cashflow underwriting and account switching.

Finally, allowing data providers to charge fees for data sharing may result in them ramping up efforts to share as much data as possible instead of minimizing data disclosure to what is reasonably necessary for beneficial uses, because now data selling will become a profit stream.

---

[10] For example, a small-scale survey of NCLC employees found that 65 percent who were currently receiving paper statements were unwilling to pay anything to continue receive them. Only 13 percent were willing to pay $2-3. Chi Chi Wu and Lauren Saunders, NCLC, Paper Statements: An Important Consumer Protection, March 2016, https://www.nclc.org/resources/paper-statements-an-important-consumer-protection/.

A massive increase in and promotion of data selling by financial institutions will ultimately harm consumers.

*3. The 1033 Rule Provides for Data Security at a Level Similar to or Even Stronger Than the Data Security Requirements Imposed on Banks*

The 1033 Rule addresses data security by requiring third parties (including aggregators) and users to comply with the FTC Safeguards Rule, unless they are already subject to the data security requirements of the Gramm-Leach-Bliley Act (GLBA). 12 C.F.R. § 1033.421(e). The standards in the FTC Safeguards Rule are similar to the standards imposed by the banking regulators set forth in the Interagency Guidelines Establishing Information Security Standards.[11] Both sets of standards are promulgated pursuant to GLBA and require businesses to have information security plans. However, in some cases, the standards in the FTC Safeguards Rule are even stronger than those in the Interagency Security Standards. For example:

1. The FTC Safeguards Rule requires multi-factor authentication or an equivalent protection for anyone accessing customer information on the institution's system.[12] The Interagency Information Security Standards only require that the institution have some sort of controls to authenticate and limit access to authorized individuals.[13]

2. The FTC Safeguards Rule requires an institution to designate a single qualified individual to be responsible for overseeing and implementing the information security program.[14] The Interagency Information Security Standards only require the involvement of the institution's Board of Directors in approving and overseeing the program.[15]

c. The FTC Safeguards Rule requires the secure disposal of customer information no later than two years after the most recent use of it to serve the customer. [16] The Interagency Information Security Standards merely require institutions to have an information security program with "appropriate measures to properly dispose of customer information and consumer information." [17]

While we believe data security can be improved for both third parties and banks, the idea that the 1033 Rule should be rolled back because it places data security at risk is preposterous. If

---

[11] See 12 C.F.R. pt. 30, app. B ("Interagency Guidelines Establishing Information Security Standards"). These comments will cite the OCC version for ease of readability. There are parallel cites to the same Interagency Guidelines for the Federal Reserve Board and FDIC.

[12] 16 C.F.R. § 314.4(c)(5).

[13] 12 CFR Part 30, Appx. B, ¶ III.C.i.a.

[14] 16 C.F.R. § 314.4(a).

[15] 12 CFR Part 30, Appx. B, ¶ III.A.

[16] 16 C.F.R. § 314.4(c)(6)(i).

[17] 12 CFR Part 30, Appx. B, ¶ III.C.4

data security for third parties is not sufficient under the Safeguards Rule, it is not sufficient for banks and depositories either, given that the Interagency Security Standards are not any stronger.

Finally, we understand that data providers have criticized the 1033 Rule for not imposing liability on aggregators in the event of a data security breach or fraud. While we do not have a position on whether data providers versus aggregators should be liable, the most important principle is that the consumer should not bear any liability and should be made whole in the event of monetary losses from a data security breach, unauthorized charges, or fraud.

*4. The Privacy Guardrails in the 1033 Rule are Best-in-Class and Should Be Retained for the Benefit of Consumers **and** Data Providers*

The consumer protections at §§ 1033.421 of the Rule are best in class, perhaps the strongest for any privacy regime. These protections are light years ahead of the meager provisions of what data providers are subject to already, *i.e*., the privacy provisions of the Gramm-Leach-Bliley Act, which only require financial institutions to offer the ability to opt out of sharing with unaffiliated third parties and do not prohibit secondary use by the institution or its affiliates.

We urge the CFPB to retain all of the privacy protections in the 1033 Rule. We also urge the CFPB to retain the scope of the 1033 Rule in covering all access to consumer-authorized data, including by third parties such as aggregators. Without such coverage, as discussed above, third parties will not be subject to these protections, including when they obtain data via screening scraping. They will not be subject to the protections such as:

- Prohibition against secondary use (§ 1033.421(a)) – third parties not subject to the 1033 Rule will be free to use consumer-permissioned data to target market consumers.
- One-year limit on authorizations (§ 1033.421(b)(2)) – third parties not subject to the 1033 Rule will be able to access consumer-permissioned data indefinitely, including for many years after the consumer granted consent (and probably forgotten that they did so).
- Clear, conspicuous, segregated authorization disclosures (§ 1033.411)– third parties not subject to the 1033 Rule could bury tiny fine print authorizations with insufficient information in clickwrap consents.
- Requirement to honor revocations and delete data (§ 1033.421(h)) – third parties not subject to the 1033 Rule could ignore consumers' requests to end data access; third parties will be able to indefinitely retain data after there is no longer authorization
- Data minimization (§ 1033.421(a)) – third parties not subject to the 1033 Rule can access whatever data they desire pursuant to consumer authorization, whether or not the data is reasonably necessary for the usage requested by the consumer. In fact, the current 1033 Rule actively discourages screen scraping for consumer interfaces (and explicitly prohibits it for developer interfaces) because it is difficult to achieve data minimization with that method.

The strong consumer protections in the 1033 Rule do not just benefit consumers, they benefit data providers by reducing the volume of data accessed via consumer authorization, putting time limits on such access, requiring deletion after the authorization expires, and prohibiting the misuse of such data for secondary use. We urge the CFPB to retain these best-in-class safeguards.

We welcome the opportunity to discuss these matters in more detail. You can contact Chi Chi Wu of the National Consumer Law Center (cwu@nclc.org) or Adam Rust of the Consumer Federation of America (arust@consumerfed.org).

Sincerely,

**National Organizations**
National Consumer Law Center, on behalf of its low-income clients
Consumer Federation of America
Americans for Financial Reform Education Fund
Accountable.US/Accountable.NOW
Center for Digital Democracy
Center for Economic Justice
Center for LGBTQ Economic Advancement & Research (CLEAR)
Center for Survivor Agency & Justice
Consumer Action
Consumer Reports
Demand Progress Education Fund
Electronic Privacy Information Center
Hip Hop Caucus
Media Access Project
National Association of Consumer Advocates
National Association of Consumer Bankruptcy Attorneys
National Disability Institute
National Urban League
Public Citizen
Public Good Law Center
TechTonic Justice
U.S. PIRG

**State and Local Organizations**
AKPIRG (AK)
William E. Morris Institute for Justice (AZ)
Center for Economic Integrity (AZ)
Arkansas Community Organizations
Community Legal Services in East Palo Alto (CA)
The Academy of Financial Education (CA)
Center for California Homeowner Association Law

Consumers for Auto Reliability and Safety (CA)
Media Alliance (CA)
Oakland Privacy (CA)
Public Law Center (CA)
ProgressNow Colorado
Tzedek DC
Jacksonville Area Legal Aid, Inc. (FL)
Georgia Watch
Indiana Legal Services, Inc.
Economic Action Maryland Fund
Maine People's Alliance
Economic Empowerment Center DBA Lending Link (NE)
New Jersey Appleseed Public Interest Law Center
New Jersey Citizen Action
New Yorkers for Responsible Lending
TakeRoot Justice (NY)
Advocates for Basic Legal Equality Inc. (OH)
Oregon Consumer Justice
Oregon Consumer League
South Carolina Appleseed Legal Justice Center
Texas Appleseed
Virginia Citizens Consumer Council
Virginia Poverty Law Center