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

Dear Sirs:

Thank you for the opportunity to comment on this proposal.

The Consumer Federation of America (CFA) is an association of nearly 200 non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education. CFA works to advance pro-consumer policies on a variety of issues before Congress, the White House, federal and state regulatory agencies, state legislatures, and the courts. We communicate and work with public officials to promote beneficial policies, oppose harmful ones, and ensure a balanced debate on issues important to consumers.

The American Economic Liberties Project is a nonprofit organization dedicated to addressing the problem of concentrated economic power across the economy to improve conditions for workers, honest businesses, and consumers.

As organizations dedicated to economic justice, consumer protection, fair and competitive markets, and data privacy, we write in response to the reconsideration of the Consumer Financial Protection Bureau's (CFPB) Personal Financial Data Rights (PFDR) rule. Given the strong consumer protections, the bipartisan support for the rule, the rigorous and thorough process to complete the rule that engaged a variety of stakeholders, we urge you to keep the core elements of the original rule as set forth in this comment.

While they may not recognize the term "open banking," consumers clearly want to share their financial data with third-party companies. By 2022, more than one hundred million consumers had asked their financial institution to share their personal financial data with a third-party company.[1] Those volumes have certainly grown since then. Consumer financial data is highly valuable, but without clear rules to ensure that consumers have the right to control how it is used, private interests may overwhelm consumer needs. Banks may erect barriers around financial information to benefit their competitive positions[2] and aggregators may collect and share data in ways that exceed consumers' consent. Now, JPMorgan Chase has entered into a bilateral agreement with a single aggregator, and other large banks are likely to follow suit to extract fees.[3] This contradicts Congress's clear intent to protect the rights of consumers to share their data freely. And undoubtedly, charging fees will have anti-competitive effects, as small banks and fintech companies will have less leverage.

I. The Framework of the 2024 Final Open Banking Rule Will Provide Strong Consumer Protections, Support Innovation, Ensure Competition in the Marketplace, and Advance Open Banking in the United States.

The original rule included pro-competition, anti-surveillance protections that are needed in an economy that monetizes consumers' data for purposes outside of their interests. These protections were the product of a rigorous, multi-year, bipartisan rulemaking process that began in the first Trump administration.[4] The CFPB went to great lengths to engage consumers, academics, non-profits, and industry stakeholders from banks, credit unions, financial technology companies, and trade associations, and as such, was lauded by political leaders from both parties.[5]

The text of the 2024 personal financial data rights (PFDR) final rule navigated the complex nature of the challenges presented by open banking, where the interests of data providers collide with those of the data aggregators, and consumers have little control over the use of their financial information:

> "Market participants' interests may diverge due to interrelated competitive, legal, and regulatory factors. For example, data providers may limit the data they share or refrain from sharing altogether to protect their market position, while third parties may collect more data than they

[1] United States: National Archives and Records Administration: Office of the Federal Register & United States: Consumer Financial Protection Bureau. (2024). Required Rulemaking on Personal Financial Data Rights. Part II: Rules and Regulations. Federal Register. Vol. 89, No. 222, 90547–91245. https://www.govinfo.gov/app/details/FR-2024-11-18/2024-25079

[2] Lindsey Adams. (2021). Open Banking – An Endeavor of Competing Goals. The National Law Review, XII(7). https://www.natlawreview.com/article/open-banking-endeavor-competing-goals

[3] Evan Weinberger Bloomberg & Paige Smith. (2025, July 11). JPMorgan Tells Fintechs to Pay Up for Customer Data Access. *Bloomberg Law*. https://news.bloomberglaw.com/banking-law/jpmorgan-tells-fintechs-they-have-to-pay-up-for-customer-data

[4] US Department of the Treasury. (2018). A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation. https://home.treasury.gov/sites/default/files/2018-07/Nonbank%20Financials%20EO%20-%20Fact-Sheet%20FINAL.PDF

[5] Rep. Patrick McHenry. (2024, October 22). McHenry Statement on CFPB's Final 1033 Rule. U.S. House Committee on Financial Services. https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=409400; Ranking Member Maxine Waters. (2023, October 20). Ranking Member Maxine Waters' Statement on CFPB's Proposed Personal Financial Data Rights Rule. U.S. House Committee on Financial Services Democrats. https://democrats-financialservices.house.gov/news/documentsingle.aspx?DocumentID=410872

> reasonably need to provide the products or services sought by the consumer. Such unnecessary collection, use, and retention of consumer data by third parties does not benefit consumers and needlessly encroaches on consumers' privacy interests."[6]

Without a multilateral set of open banking standards, the small set of data aggregators on whom the data sharing system depends have often requested financial data at cadences far in excess of consumer expectations, and the costs of building APIs have discouraged many banks from migrating away from risky screen scraping systems.[7] While open banking services continue to proliferate, the marketplace needs a strong set of rules. When coupled with an industry standard-setting organization, the PFDR will support competition, privacy, data security, and cost-efficiency.

Facing these challenges, the PFDR rule struck a balance between the priorities of data providers and data aggregators. By limiting how frequently aggregators could request data to only the times when consumers authorized it, the terms of the rule curbed burdens on data providers. Simultaneously, by not permitting data providers to establish fees to share data, the rule ensured that data would not be encumbered by bilateral agreements that could undermine competition. A related rule authorized an industry standards-setting organization to facilitate industry self-governance. Most importantly, the rule gave consumers the ability to control how their data was used, stored, and shared, and allowed them to revoke access at any time. The original rule expanded consumer rights well beyond the existing protections afforded under the Gramm-Leach-Bliley Act (GLBA). Together, it established a framework for holding all parties accountable to meet the privacy concerns of consumers. For these reasons, it is essential that any reconsideration of the PFDR rule preserves consumers' rights to control the use of their financial information.

II. Open Banking Provides Benefits to Consumers, Advances Innovation, and Increases Competition

There are many important open banking use cases that will benefit consumers. By using APIs, these actions will occur in safer environments where consumers have control over how their data is used. These developments underscore the ways in which the protections in the PFDR support innovation. Examples of open banking use cases that will bring benefits to consumers include:

Cash-flow underwriting: Tens of millions of Americans have a transaction account but lack other indicia needed to qualify for credit.[8] Cash flow underwriting can provide creditors with relevant information to evaluate individuals for loans and other financial services. Data aggregators often serve as an important intermediary between outside lenders and the banks holding the financial data.[9] With the additional

[6] Consumer Financial Protection Bureau. (2024, October 22). Required Rulemaking on Personal Financial Data Rights. https://www.consumerfinance.gov/rules-policy/final-rules/required-rulemaking-on-personal-financial-data-rights/
[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
[8] Kambara, M., Brevoort, K., & Grimm, P. (2015). CFPB Data Point: Credit Invisibles [Data Point]. Consumer Financial Protection Bureau. https://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf
[9] Jonathan Gurwitz. (n.d.). Cash flow underwriting: 5 ways lenders can drive growth. Credit Update. Retrieved October 14, 2025, from https://plaid.com/resources/lending/cash-flow-underwriting/

information gained from this "alternative data," lenders may feel comfortable extending credit to otherwise underserved borrowers at more favorable terms.

As opposed to screen scraping, where the use of data is not permissioned, APIs can make it safer for underserved borrowers to provide their cash flow information to creditors. Data aggregators solicit this data from banks to provide third-party lenders with the necessary information to underwrite cash flows. The PFDR rule specified that consumers could limit the use of their data to a specific purpose, such as for credit underwriting, and suspend permission after the specific purpose has been fulfilled. In practice, this means that a third party loses access to a consumer's bank account data after it has evaluated their creditworthiness. As a result, use of APIs enhances consumer privacy and provides important guardrails on the security of consumer financial information.

Banks lose an advantage to rivals when they are forced to release cash flow data to potential creditors. However, by introducing more competition, these data requests empower underserved consumers.

Personal Financial Management (PFM) tools: PFM services were the original use case for financial data sharing. When introduced, consumers gave PFM providers direct access to many of their accounts. They achieved this through the only technology available at the time: screen scraping. The PFM received the ability to log into consumer accounts to see transactions, account balances, and other available data. This gave PFMs a global insight into the financial profiles of their customers. It also created incredible demands on bank servers, as many PFMs would log on to each account many times per day, and left consumer data in insecure environments.[10] Consumers are largely unaware of the practice of PFMs to constantly review their accounts.

Switching banks and comparison shopping for services: Consumers could earn hundreds of millions of dollars in additional interest if they move funds from interest-free or low-interest over to high-yield savings accounts. Many could find alternative checking accounts that better suit their needs. In spite of those opportunities, people stay with their existing accounts. Many of the reasons go back to the high "switching costs" associated with moving an account. These include the time required to migrate bill payment directory information, the risk of receiving an overdraft from a pull payment, or the challenge in conducting research to find better alternatives. Switching can be risky. When historical account data is lost, consumers and small businesses lose important information they may need in the future for budgeting, tax preparation, and other financial activities.

The PFDR's rules required financial institutions to share transaction histories and other important account details, including bill payment records and payment directories. These data points hold significant value for account holders. With its requirement that this information be made available on request to the account holder in a machine-readable file format, the PFDR empowers consumers to more easily switch bank accounts.

[10] Brankas. Screen Scraping Unveiled: The What and How. Retrieved October 14, 2025, from https://blog.brankas.com/screen-scraping-unveiled/

Pay-by-bank: Consumers and small businesses have shown an interest in increasing the share of payments made using bank account and routing numbers. Pay-by-bank use cases are already emerging, utilizing traditional ACH, same-day ACH, or faster payments. Often, businesses choose to use pay by bank to save on their payment acceptance costs.

Pay-by-bank exposes sensitive financial information to billers. Today, many pay-by-bank transactions require consumers to manually enter their account and routing numbers into online billing platforms or over the phone. Whenever routing and account numbers are shared – including in pay-by-bank transactions and paper checks – it increases the risk of fraud and scams.

In card transactions, banks receive high interchange fees, but they assume liability for transactions where the consumer does not receive the product they purchased or if the service provided was unsatisfactory. These "chargeback" rights are an important benefit for consumers. If a debit card or an ACH is used to make the purchase, regulations do not impose the same requirements.[11] While NACHA operating rules penalize merchants with unusually high rates of returned ACH orders,[12] a dramatic shift in the share of payments made using ACH and faster payments will necessitate a re-examination of how liability is assigned for these types of payments.

Variable recurring payments and micropayments: Open banking will enable new categories of payments that can benefit consumers, provided they occur in secure environments. For example, billers can use variable recurring payments to debit an account for an amount that will not trigger an overdraft. Micropayments may enable businesses to develop revenue models for very small services – such as online newspapers or Substack authors charging readers a few cents to read a single article.

III. Responses to the Questions Posed in the Advanced Notice of Proposed Rulemaking (ANPR)

The ANPR seeks comments on four areas that will affect the experiences of consumers when they seek to exercise their financial data rights:

- Scope of Who May Make a Request on Behalf of a Consumer
- Defrayment of Costs in Exercising Rights Under Section 1033
- Information Security Concerns in the Exercise of Section 1033 Rights
- Privacy Concerns in the Exercise of Section 1033 Rights

The CFPB devised a careful PFDR rule within the boundaries of the authority granted to it by Congress. Notably, Congress did not grant the CFPB the authority to set prices for data sharing. While there are merits to both sides of the conversation surrounding fees, the greater priority is to ensure the open banking marketplace can move forward. We fear that if the CFPB does choose to set a price, it will put the rule at risk of new litigation.

[11] Ann Spiotto. (2001). Credit, Debit, or ACH: Consequences & Liabilities A Comparison of the Differences in Consumer Liabilities. Emerging Payments Occasional Paper Series, 3. https://www.chicagofed.org/~/media/others/research/papers/payments-studies-occasional-papers-series/eps-2001-3-pdf.pdf
[12] NACHA. (2015, September 18). ACH Network Risk and Enforcement Topics. https://www.nacha.org/rules/ach-network-risk-and-enforcement-topics

Section One: Scope of Who May Make a Request on Behalf of a Consumer

> Question 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?
> AND Question 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?"

Section 1002 of the Consumer Financial Protection Act (CFPA) said that data providers had to make covered financial information available to consumers upon their request and defined authorized third parties as "representatives" acting on behalf of an individual."[13] The text in the PFDR rule allowed for a reasonable interpretation of the term "representatives" to include third parties that might be critical participants in data sharing, including those entities using the data to fulfill a consumer's requests.

Absent the ability to include these entities, consumer data sharing rights would be limited. In essence, data sharing would consist solely of the transmission of financial information from a data provider directly to the consumer. For example, in such an arrangement, the consumer might receive from their data provider an XLS file with rows of data for covered transactions or a directory of bill payment providers. Such a limitation would make data useful for far fewer purposes. Additionally, many consumers lack the technical skills required to download data in the first place, let alone analyze it in a spreadsheet or transmit it to a third party.

Moreover, to exclude third parties from the definition of "agent, trustee, or representative" could have disastrous consequences for consumer control of financial data. With a narrow interpretation that excludes third parties, the sharing of data between the consumer and a non-bank third party would occur without the guardrails of Section 1033. Consumer financial data rights would be far weaker, data security would be lower, and privacy would be far from guaranteed. For these reasons, the only practical way to fulfill Congress's wishes is to define authorized third parties as "representatives."

> Question 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?
>
> And Question 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 the original rule does not hold third parties to a fiduciary standard, its robust consumer protections serve a similar purpose. Central to the obligation of a fiduciary's role is the requirement that a fiduciary

13 CFPA Section 1002(4)

will act in the interests of the beneficiary and not of their own. Under common law, an agent acting on behalf of a principal has a fiduciary relationship to the principal, and that care includes a requirement not to use a principal's confidential information for its own benefit.[14]

It would be unworkable to impose a fiduciary obligation on third parties. For example, it is not reasonable for consumers and third parties to negotiate a fiduciary relationship merely to download a personal financial management app. It is an impossible barrier in most instances and would essential prevent consumers from making use of a valuable financial tool.

The PFDR rule accomplishes the same functional outcomes. It gives the consumer the authority to dictate how their data is used. If any party fails to fulfill the consumers' requirements, they are out of compliance with the rule. While not accomplished through a fiduciary agreement, the result is the same. A critical test example is the rule's prohibition on the use of secondary data. To remain compliant with the rule, data providers and data recipients must prioritize the interests of the consumer over their own.

Section Two: Defrayment of Costs in Exercising Rights Under Section 1033

> Question 9: Does the PFDR Rule's prohibition on fees represent the best reading of the statute? Why or why not?

Congress did not set an acceptable fee or provide a conceptual framework for allocating data-sharing costs. This preference was not unusual or unique to the data-sharing text. Indeed, Congress generally chose to avoid setting fees in most cases. For example, they did not allow the CFPB to set an interest rate cap for small-dollar loans. In some cases, however, Congress has given specific instructions to the CFPB on how it can set prices. For example, Congress added an exception to permit an all-in interest rate cap on loans made to servicemembers.[15] Congress created a rebuttable presumption to exempt banks from relevant laws if banks set penalty fees on credit cards and checking accounts at rates equivalent to their cost. These outcomes underscore the need for Congress to weigh in on fee-setting.

This context explains why, absent clear instruction from Congress, the CFPB wrote the PFDR rule to prohibit data providers from imposing fees or charges on a consumer or an authorized third-party for connecting, establishing, or maintaining interfaces for controlling data usage, or for fulfilling requests from consumers to share data.[16]

In the time since the lawsuit challenging the rule was filed, banks have introduced new pricing sheets that could disrupt the data-sharing ecosystem. While the terms of the arrangement made between one large data aggregator and the largest bank have not been made public, the rates in the initial pricing sheets were widely perceived as very high. One report suggested that fees paid by the aggregator to a single bank would be equivalent to 75 percent of its annual revenue.[17] Ultimately, the bank and the aggregator reached

[14] Fiduciary relationship. (n.d.). LII / Legal Information Institute. Retrieved October 17, 2025, from https://www.law.cornell.edu/wex/fiduciary_relationship
[15] 10 USC §987(b): Terms of consumer credit extended to members and dependents: limitations, Annual Percentage Rate
16 § 1033.301(c)(1) and (2)
[17] Jeff Kauflin. (2025, July 21). Why JPMorgan Is Hitting Fintechs with Stunning New Fees For Data Access. https://www.forbes.com/sites/jeffkauflin/2025/07/21/why-jpmorgan-is-hitting-fintechs-with-stunning-new-fees-for-data-access/

an agreement on fees. While the parties did not publicize the terms of their bilateral contract, the aggregator left open the possibility that it would raise fees on its client fintechs in the future.

If the CFPB chooses to establish a fee, it will have done so outside of the instructions given to it by Congress, with enormous risks to the rule's sustainability. The CFPB's decision to set fees will expose the reconsidered 1033 rule to litigation challenges from data aggregators, third-party fintechs, their trade associations, as well as groups representing consumers and businesses.

> Question 10: Was the PFDR Rule correct to conclude that permitting fees "would obstruct the data access right that Congress contemplated"? Why or why not? AND
> Question 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? AND
> Question 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? AND
> Question 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?

While we strongly believe any fee-setting by the CFPB will necessarily put the rule at risk of litigation challenges, if it does choose to set fees, it should take several concerns into account. Fees could undermine competition. In conducting examinations, the CFPB should ensure consumers are not paying fees to share their financial information.

First, the CFPB should be cautious about undermining competition and the free flow of information if it permits fees but does not establish specific guidelines for reasonable costs. Competition will suffer when banks and fintechs sign bilateral agreements with differing fee schedules. Most likely, if banks can set bilateral pricing agreements, banks with larger retail positions can dictate the market.

Even aggregators have some understanding that fees could be possible. According to at least one report, some fintech executives speaking off the record have acknowledged that some data-sharing fees could be valid.[18] Big Tech has flourished with a business model that relies on free and virtually unlimited access to consumer information. Aggregators are not an exception. Few consumers probably realize how frequently data aggregators access consumer accounts, either via screen scraping or using an API. Without limits on secondary usage, nothing prevents them from building algorithmic models to fulfill purposes that are not of tangible benefit to consumers.

If the CPFB proceeds with a specific permitted fee or a fee cap, it should ensure that costs do not exceed the marginal cost of each API pull. Per-account data sharing costs for banks are not consistent over time; most costs to banks occur when setting up a connection, whereas subsequent API pulls are virtually free.

[18] Ibid

This cost profile aligns bank fees with long-term consumer satisfaction. Without a ceiling associated with marginal costs, banks will have a profit motive to share data more frequently, first to recover the costs of their initial connection, and then to make marginal profits. Such a policy would directly counter the purpose of the law, as oversharing is a known problem. High fees increase the risk of compromising consumer privacy. Additionally, banks have data sharing costs when data aggregators request information by screen scraping. After the initial costs to connect an account, the cost to banks of supplying data through screen scraping – a practice that the original PFDR rule called to eliminate almost entirely – is greater than the ongoing costs incurred when sharing data through APIs.[19] Moreover, one of the larger components of startup expenses is building APIs, but this can be mitigated by using the already-developed free Financial Data Exchange APIs.

The CFPB should initiate a larger participant rulemaking on data aggregators. Subsequently, the CFPB's examiners should monitor bank-aggregator arrangements to ensure data fees do not result in consumers paying fees to share their data. It is not reasonable for consumers to pay to share their data. It is their information. Fees to share information would undermine competition, as well.

While we believe the prudent approach is not to permit fees, setting a price based on the incremental costs of data pulls is the best remaining alternative, with a concurrent prohibition against data providers charging consumers for the right to share their data.

One-off bilateral agreements between banks and data aggregators will undermine competition in the marketplace. If the CFPB refuses to impose restrictions on data-sharing fees, it should be cautious of potential unintended consequences. It is entirely possible that data sharing fees could become a profit center for some financial institutions, with the greatest advantage falling to the data providers with strong incumbent market positions.

Equally vulnerable to data sharing fees could be smaller financial institutions that lack the market power to influence aggregators. Many smaller banks and credit unions rely on their core payment processors for technical solutions to complex operational problems. For example, many smaller financial institutions have contracted with their core providers to implement faster payment services. The CFPB should consider how core providers might extract some or most of the fee-sharing revenue that aggregators agree to pay to receive financial data. Such an outcome could provide large banks with an additional competitive advantage over smaller ones.

Indeed, bilateral agreements could even lead to an outcome where fintechs pay different prices to their aggregators based on which bank the consumer uses. This becomes especially problematic if consumers ultimately pay fees to request their data to be shared, as some fintechs might charge a different price based on which bank their customer used or cease to work with customers of some banks entirely. In any of these scenarios, large banks with incumbent market power will have significant influence on the relationship between data aggregators and their third-party customers. Banks could also solidify their

[19] MX. (n.d.). The Differences Between APIs, OAuth, and Screen Scraping. Retrieved October 21, 2025, from https://www.mx.com/guides/banking-apis-oauth-sceenscraping/

influence in the data-sharing sphere by offering the lowest-cost data-sharing agreement to the data aggregator owned jointly by a consortium of the largest banks.

Section Three: Information Security Concerns in the Exercise of Section 1033 Rights

> Question 18: Does the PFDR rule provide adequate protection for the security of consumers' data? Why or why not? AND
>
> Question 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?

Our economy will benefit both from the adoption of permissioned data sharing, as enabled by APIs, and the elimination of screen scraping for financial data sharing.

The original rule deftly called for this goal in several ways. First, it provided financial institutions with the option to either offer APIs directly or rely on a third-party vendor, most likely an aggregator, to utilize APIs on their behalf.

The PFDR rule addressed data security by requiring third parties to comply with the FTC Safeguards Rule, unless they are not already subject to the Gramm-Leach-Bliley Act's (GLBA) data security requirements. The FTC's Safeguards Rule requires financial institutions to ensure that third-party partners "actively maintain" safeguards to ensure the security and confidentiality of consumer information.[20] These standards echo the substance of the Interagency Guidelines Establishing Information Security Standards issued by prudential banking regulators. The interagency guidelines require businesses to have information security plans, for example. Moreover, the FTC Safeguards Rule calls for multi-factor authentication – a stronger requirement than the prudential regulators' "best practices" standard.[21] Other requirements, such as one obligating institutions to delegate compliance for information security to a specific person, add greater accountability. There is also a data deletion requirement.

The PFDR rule also called for the establishment of a standards-setting organization (SSO). The use of an SSO enables the industry to develop solutions for self-governance quickly, as long as those solutions remain compliant with the rule. The Financial Data Exchange (FDX), the SSO chosen for the initial five-year term, provides its member financial institutions with free use of their APIs, subject to the requirement that financial institution API users comply with these rules.

[20] *Safeguards Rule*. (2014, January 28). Federal Trade Commission. https://www.ftc.gov/legal-library/browse/rules/safeguards-rule

[21] *FTC Safeguards Rule: What Your Business Needs to Know*. (2022, April 27). Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

Section Four: Privacy Concerns in the Exercise of Section 1033 Rights

> Question 30: Does the PFDR Rule provide adequate protection of consumer privacy? Why or why not?

The original PFDR provided best-in-class protection for financial data sharing. The rule will protect the privacy of consumers in ways that the Gramm-Leach-Bliley Act (GLBA) privacy provisions do not. The GLBA is largely unworkable for consumers who wish to share their data but still maintain control over how it is used. While the GLBA does require financial institutions to offer account holders the ability to opt out of some data sharing with third parties, it lacks the nuance and specificity of the PFDR rule, particularly when the consumer wants to share their information with a third party. The PFDR rule prohibits secondary uses of data not authorized by the consumer, whereas GLBA does not provide a similar restriction on data use by the financial institution or its affiliates.

The CFPB must preserve the strength and scope of the data privacy protections in the PFDR rule.

Reauthorization after one year 1033.421(b): The PFDR rule prevented third parties from maintaining access to consumer data indefinitely. It is highly likely that some consumers will lose track of where their data is being shared. This risk is heightened when consumers cease to use the third party's service or product, resulting in "ghost" data surveillance. By requiring third parties to seek reauthorization of data, the PDFR established a straightforward framework to ensure that consumers do share data when they want to, but are unlikely to share data against their wishes simply because they forgot about their relationship with the third-party service.

Prohibitions against secondary uses 1033.421(a): the PDFR rule prevented third parties from gaining consent to access consumer data for one purpose but then using the data for additional commercial reasons. For example, the rule prevents third parties from using consumer data to train models to build new services. Some third parties access consumer accounts many times a day, far in excess of what the account holders contemplated.

Separately, a prohibition on secondary use addresses a concern held by banks. When third parties are limited to requesting data, they will pull data less often. Data providers have expressed concerns about the volume of requests they receive and have rightfully shown that aggregators often pull data to fulfill their own business goals, rather than those of consumers. For data providers, those pulls do create cost, such as significant burdens on the server space needed to fulfill as many as twenty requests per day from a single account. By applying a prohibition on secondary use, the CFPB can neatly address a key concern of data providers.

Clear disclosures for authorization (1033.411): Clear and conspicuous disclosures are an essential component of obtaining consumer consent. Without the protections in the PDFR rule, third parties not subject to 1033 could rely on misleading or buried agreements, most likely in fine print using "negative option" frameworks, that are not an adequate method for consumers to provide permission on how their data is used.

Revocations and Deletions of Data 1033.421: Providing consumers with a means to revoke access to data, as well as to delete previously obtained data, is also essential. Without the requirements in the PDFR rule, third parties could ignore consumer requests. Additionally, in the event that a third party goes out of business, suffers a business interruption, or is sold, consumers may be unable to exercise their right to delete their information.

Data minimization 1033.431(a): The PFDR rule's minimization requirement, stating that collection and use must be proportionate to the consumer's intentions, is an essential safeguard. It complements the prohibition against secondary use by also ensuring that third parties do not excessively pull data beyond what is reasonably necessary. Surveillance of consumers is a significant problem in the era of Big Tech, and the ability of tech firms to collect data for free is a key enabler of these harmful practices. That data minimization rule also helps to address the burden placed on data providers by otherwise unlimited data pulls.

Conclusion

Open banking has already arrived, but the original PFDR rule ensures that open banking will grow in a secure, consumer-permissioned environment. The original rule's support of APIs is essential to reforming market practices that currently leave consumers with less control over their data, permit over-sharing of data, and add unnecessary risk. By requiring banks to make data available through an API – either via their own services or with a third-party vendor – the original rule would have accelerated the shift in data sharing technology away from screen scraping.

We urge the CFPB to ensure that the strong rules outlined in the original PDFR remain part of a reconsidered rule.

If you have additional questions or seek clarification, please contact Adam Rust, Director of Financial Services for the Consumer Federation of America (arust@consumerfed.org) or Morgan Harper, mharper@economicliberties.us, with the American Economic Liberty Project.

Thank you.