October 21, 2025

By electronic submission to:
Comment Intake—Nonbank Registration of Certain Agency and Court Orders
c/o Legal Division Docket Manager
Bureau of Consumer Financial Protection
1700 G Street, NW
Washington, DC 20552

Re: Advance Notice of Proposed Rulemaking on Personal Financial Data Rights Reconsideration (Docket No. CFPB-2025-0037; RIN 3170-AB39)

Dear Sirs and Madams:

The Online Lenders Alliance (OLA) welcomes the opportunity to respond to the Bureau's advance notice pf proposed rulemaking (ANPR) on *Personal Financial Data Rights Reconsideration* (Docket No. CFPB-2025-0037)**.**

About OLA

OLA represents the growing industry of innovative companies that develop and deploy pioneering financial technology, including proprietary underwriting methods, sophisticated data analytics, and non-traditional delivery channels, to offer online consumer loans and related products and services. OLA's members include online lenders, vendors, and service providers to lenders, consumer reporting agencies, payment processors, and online marketing firms.

Fintech companies are at the vanguard of deploying innovative online tools that reach new customers, prevent and mitigate fraud, manage credit risk, and service loans. As technology evolves and the public's comfort with online financial transactions grows, protecting consumers will be more important than ever. OLA is leading the way to improve consumer protections, with a set of standards that ensure borrowers are fully informed, fairly treated, and able to use lending products responsibly. To accomplish this, OLA members voluntarily agree to hold themselves to a set of Best Practices, a set of rigorous standards above and beyond current legal and regulatory requirements. OLA members, the industry, and any partners with whom OLA members work use these standards to stay current on the changing legal and regulatory landscape.

OLA Best Practices cover all facets of the industry, including advertising and marketing, privacy, payments, and mobile devices. Most importantly, OLA Best Practices are designed to help consumers make educated financial decisions by ensuring that the industry fully discloses all loan terms in a transparent, easy-to-understand manner.[1]

Much of the innovation undertaken by OLA members has given consumers greater control over their financial future. This is especially the case when it comes to access to capital. Whether borrowing for major purchase, paying for critical auto repairs or other emergencies, or just bridging the gap between paychecks, the ability to find and secure credit is often a determining factor in a consumer's financial wellbeing. Online lenders provide benefits to consumers, particularly those in underserved communities, with fast, safe, and convenient choices that simply are not available through traditional lending markets.

Introduction

Once locked away in file cabinets, consumers' personal financial data is increasingly online, in the cloud, and effortlessly transmitted around the globe in seconds. This sea change has helped make innovative financial products like mobile banking and online lending possible. But those innovations depend upon consumers' ability to protect and access their data, not to mention the public's confidence that their personal data is safe and within reach to them.

How app developers or third parties access this data is markedly different from the processes that mainstream financial institutions use. While mainstream institutions have a direct pipeline to this information, third parties or app developers must connect to this data using a designated conduit or additional software tools. This can be unreliable and restrictive due to out-of-date processes and rules not designed for these new ways of storing and sharing data.

Inadequate security protections and potential liability exposure are often cited as rationales for limiting third-party access to data. OLA and its members take data security very seriously, as evidenced in our Best Practices. In addition, providers must comply with the provisions of the Gramm-Leach-Bliley Act (GLBA) to the extent that they obtain and redisclose personally identifiable financial information from banks. Working within these guardrails, fintech firms have been able to harness the very same technology that has allowed fintech firms to create new products to assist in the development of strong security protocols.

But the complex and inconsistent patchwork of rules and regulations that oversee data protection has impeded consumers' ability to access the capital they need. Consumers may, for example, find themselves forced to make financial decisions based on incomplete information or locked out of innovative online credit or payment products altogether. While consumer demand for new and expanded services has spurred successful partnerships between traditional lending institutions and fintech firms, the regulatory structure has held back further innovation. The only way to change this dynamic is to foster an innovative and collaborative environment among all stakeholders.

[1] Online Lenders Alliance Best Practices, https://onlinelendersalliance.org/best-practices/

The CFPB's Role in Advancing Open Banking

The CFPB has made substantial efforts to promote open banking, including its market monitoring orders looking to secure information from data aggregators related to contracts, payments, data security, error resolution, liability, fraud, data accuracy, customer controls, privacy, and uses of data including metrics and traffic. For providers, the CFPB has requested information related to consumer direct access, screen scraping, third-party portals, and third-party service providers. Additionally, as a part of this process, the CFPB published outlines and followed the requirements defined under the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), publishing their panel report in April 2023.

One key obligation under the Regulatory Flexibility Act (Reg Flex) is that the Bureau must consult with the other banking regulators, including the Federal Reserve, the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the Federal Trade Commission (FTC), to ensure that any proposal does not impose substantially similar requirements on covered entities. The CFPB also must take into consideration certain account conditions under which covered entities do business in the U.S. and internationally and cannot require or promote the use of any particular technology for the development of compliance procedures.

OLA believes that any open banking proposal needs to ensure that data aggregation services are fair, transparent, and competitive. The current patchwork of rules setting different standards at the state and federal levels for a broad range of market participants creates confusion and inhibits growth. This current regulatory structure could result in putting consumers and their financial information at risk. Stakeholders have hoped to see the CFPB engage and define these rules in order to level the playing field for all participants, especially given the broad range of entities that will be collecting, storing, and analyzing consumer information. It will be critical that all participants are subject to the same financial standards and supervision.

OLA would like to take this opportunity to provide some additional insights to the Bureau to consider as it looks to reconsider the Personal Financial Data Right rule (PFDR), including some of the intricacies of implementation of Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) and its possible impacts on consumer privacy, data security, and financial services.

Overall Impact of the Rule

The current PFDR rule, which is set to take effect in June 2026, bestows new rights and imposes new obligations related to consumer financial data. This includes the right of access for consumers and third parties, including a data portability component. The rule requires that data access be accomplished through interfaces and imposes significant limits on how third parties may use data. The long-term impacts are still unclear, and OLA would encourage the Bureau in its ongoing effort to provide further clarity on these issues as it proceeds with its rulemaking efforts.

The rule as currently constituted would also expand the scope of data security regulations, especially the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, which the FTC updated earlier this year. The rule's broad scope may bring significant impacts to the fintech sector on several fronts.

The rule would affect two very specific categories of covered persons, data providers, and third parties. For purposes of the rule, data providers are institutions defined under Regulation E, card issuers defined under Regulation Z, or any other entity that controls or possesses information concerning a covered consumer financial service or product. This scope would encompass such entities as banks; credit unions; and other providers of checking, savings or credit card accounts, as well as various other payments and account products. The latter category would encompass a wide range of non-financial institutions, such as digital wallets, which the Bureau specifically mentions in the rule's preamble.

The other impacted entities are third parties, which are defined as any person or entity that is not the consumer to whom the covered data pertains or the data provider that controls or possesses the consumer-covered data. Given this definition, a third party could be another financial institution that is a data provider in its own right but also could be fintech companies or data aggregators. The rule has specific requirements for data aggregators, which would be defined as an entity that is retained by or provides services to the authorized third party to enable access to covered data.

It should be no surprise that the effects of the PFDR rule will be significant. From a data provider perspective, one benefit would be a move away from the use of consumer account information by third parties to access accounts. This use can create liability issues, especially when entities access more information than necessary to provide the product or service sought by the consumer. The rule also will establish more transparent standards, giving consumers some additional control over their ability to share their data with other entities, which may make it easier to move from one financial institution to another.

However, OLA notes that whenever a federal rule is implemented, some states follow suit with more stringent provisions. Yet the proposed rule does nothing to take future actions by the states into account. OLA encourages the Bureau to consider the implications of state action as it looks to update the PFDR rule.

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

Section 1033 of Dodd-Frank mandates that covered financial institutions provide consumers with access to their financial data upon request, and it authorizes the CFPB to issue rules governing how this access is implemented. The CFPB’s October 2024 final PFDR rule correctly recognizes the role of authorized third parties, including that of technology firms, in facilitating consumer access to their financial data.

As of 2024, over 100 million consumers had authorized third parties to access their financial data.[2] This widespread adoption reflects market realities and demonstrates a clear consumer demand for fintech services.

OLA urges the CFPB to continue allowing fintech's to serve as authorized third parties under Section 1033. Permitting fintech's to serve as authorized third parties will enhance consumer choice and financial inclusion. Fintech's provide consumers with tools they need to better manage their finances, access credit and make informed financial decisions. Nearly 90 percent of Americans use at least one fintech app, and 47 percent use three or more.[3] These services are especially valuable to underserved populations who may lack access to traditional banking services. By enabling fintech's to access consumer data with explicit consent, the CFPB can help ensure that all consumers—not just those with traditional banking relationships—can benefit from modern financial tools.

Open banking frameworks that include fintech's as authorized third parties promote competition and innovation, encouraging competition among financial service providers. This leads to better products, lower costs, and improved customer service. The CFPB has noted that open banking can "foster competition and innovation" by making it easier for consumers to switch providers and access new services.[4]

Fintech's often act as intermediaries that aggregate and standardize data from multiple sources, giving consumers a holistic view of their financial lives. This functionality is essential to consumers for budgeting, credit scoring and financial planning. OLA strongly recommends that any changes to the PFDR rule require that data be made available in a usable electronic format, so that fintech's who are uniquely situated can help consumers achieve better data portability and transparency via secure APIs and user-friendly interfaces.

Currently, authorized third parties face substantial regulatory requirements, including obligations related to data use, retention and consumer disclosures. These safeguards ensure that fintech's operate transparently and responsibly. Moreover, these changes proposed under the PFDR rule will help lead the shift away from screen scraping to increase security and accountability going forward, ensuring that any further changes to APIs enhance data security and consumer trust.

---

[2] Congressional Research Service, *"Access to Consumer Financial Data: Open Banking and the CFPB's Section 1033 Rule,"* September 30, 2025, https://www.congress.gov/crs-product/IF13117

[3] Plaid, "What is 1033? Understanding the CFPB's Section 1033 Rule," January 17, 2024, https://plaid.com/resources/compliance/section-1033/

[4] Consumer Financial Protection Bureau, Required Rulemaking on Personal Financial Data Rights, https://www.federalregister.gov/documents/2023/10/31/2023-23576/required-rulemaking-on-personal-financial-data-rights

Restricting access to consumers' data from third parties would not only limit consumer choice but also stifle a thriving sector that has become integral to modern financial life. For these reasons, OLA encourages the Bureau to allow fintech's to continue as authorized third parties to act on a consumer's behalf as part of any change to the PFDR rule.

Costs Associated with 1033/Consumer Data Rights

In its ANPR, the CFPB asks for feedback on "the optimal approach to the assessment of fees to defray the costs incurred by a 'covered person' in responding to a customer driven request." OLA opposes allowing the imposition of fees on a consumer or their authorized third party to access a consumer's own data. Doing so would not only undermine the statutory intent but would create barriers to consumer empowerment and financial innovation.

Section 1033 of Dodd-Frank reflects the policy that consumers own their financial data and mandates that covered persons "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" in a usable electronic form. The statute does not authorize the imposition of fees for such access. Courts and agencies have long held that regulatory silence does not confer authority, especially when it affects consumer rights. The continuation of the policy of prohibiting fees aligns with the statute's purpose of ensuring consumers can access their own data.

Charging consumers fees to access their data commodifies consumer rights. Allowing fees could incentivize data providers to erect paywalls around consumer data, leading to monopolistic behavior and regulatory arbitrage. This would disadvantage smaller fintech's and third-party innovators, reducing competition and providing less choices for the public.

In addition, charging fees for data access would disproportionately harm low-income consumers and stifle competition in financial services. Free access to data enables consumers to switch providers, compare products, and use innovative financial tools. Imposing fees would create friction and reduce consumer choice.

While some stakeholders argue that fees are necessary to defer an array of costs and enhance data security, these concerns should be addressed through separate regulatory safeguards—not by restricting access through pricing. Furthermore, the Gramm-Leach-Bliley Act and other frameworks already impose data protection obligations.

It is important to note that the rule as currently constituted will already result in substantial costs to fintech's as they will have to undertake system changes needed to adhere to the rule's data-sharing process. Companies will need to conduct significant organizational reviews and where necessary revise consumer documentation, data compliance policies, disclosures, and even previous commercial agreements with vendors that use data. Companies also will need to prepare and maintain systems that can receive and process both data access and revocation requests, track duration-limited authorizations, and delete data when required due to revoked or lapsed authorizations, or when retaining the data is no longer reasonably necessary. These actions will result in substantial costs. Adding new fees on top of that for consumers to access their own data would create situations where many companies may no longer be able to offer certain products or services.

Given these factors, OLA encourages the CFPB to reaffirm its commitment to consumer data rights by explicitly prohibiting fees for consumers or their representatives to access the consumer own data under Section 1033. Doing so will promote transparency, competition, and innovation in financial services while protecting consumers from unfair practices

Impact on Privacy

The PFDR rule would significantly expand privacy rights. However, the current rule goes too far by placing significant limitations on the use of data by third parties. This will have a huge negative impact on the fintech sector's ability to serve consumers and develop new products, and it ultimately will hamper fraud prevention efforts. This especially will be the case if the use of de-identified information is curtailed.

OLA has significant concerns about the current definitions of covered data. The PFDR rule defines covered data as encompassing six categories of information: individual transaction information, both pending and historical; account balances; information to initiate payments to or form a Reg E account, including any checking, savings or similar account held primarily for personal, family or household purposes; upcoming billing information; and basic account verification information.

It should be noted that the rule does not exempt aggregated, anonymized, or de-identified data. Because the use of de-identified and aggregate data by third parties like fintech companies is so prevalent, OLA believes that the Bureau should amend the rule to allow de-identified data to be carved out in some form. If not, many companies will need to expend significant costs in reworking their algorithms and product operations because so many are designed to run off de-identified data.

This rule also will lead to an increase in notices and consent. Companies are constantly struggling to keep up with new laws and regulations that demand proper disclosure. The rule as currently constituted will only add to that burden. One example is the data provider publication requirements that would necessitate frequent updates, meaning companies will have to allocate more hours and resources to compliance and less to serving the public.

Data Security

By expanding the GLBA Safeguard Rule to cover certain third parties, the PFDR rule would create new burdens for many small, innovative companies, especially given the FTC's recent update to the rule. By sweeping third-party vendors into the Safeguard, the PFDR rule will require companies to undergo major operational changes related to encryption at rest and multi-factor authentication (MFA) any time account information access occurs, leading to more requirements for written policies and procedures.

While this may not be a significant burden for more established companies, it will have a burdensome impact on smaller companies that lack the resources to undertake such large-scale operational changes. In addition, this proposal also will lead to more paperwork to review during the diligence process, both in the process of developing contracts with third parties and in the context of mergers and acquisitions, slowing down the ability of consumers to access the credit they need.

The proposed rule also will result in more sensitive data being made available in a portable format, which inevitably raises security risks. The rule, however, leaves unaddressed who would be held accountable for data breaches.

OLA believes there is a need for a clearer liability framework that would help make risk ownership more transparent and enforceable. Current regulatory guidance from the Federal Reserve, FDIC and OCC emphasizes that outsourcing does not absolve financial institutions of their responsibility to protect customers. This creates a mismatch between responsibility and control, as institutions may be held liable for breaches they cannot fully prevent.

The rise of fintech partnerships and cloud-based services has expanded the scope and complexity of third-party relationships. These relationships often involve direct customer interaction, making breaches more impactful and harder to manage under current frameworks. A new data security standard that recognizes these evolving relationships would encourage better third-party risk management throughout the entire lifecycle, from planning and due diligence to termination. This would also better align incentives across the data ecosystem and reduce systemic risk.

Although OLA strongly supports transparency in consumer data, we could caution against proposals that require consumers to be provided with a list of entities that have received their data. These types of requirements would be cumbersome for both companies and the consumers without any real benefit. Companies often share data with numerous entities, including affiliates, vendors and analytics firms; tracking and disclosing every recipient could be logistically burdensome. In addition, revealing data-sharing partners may expose proprietary business relationships or strategies, potentially harming a company's competitive positioning.

Furthermore, implementing these types of systems to track, audit and disclose data-sharing practices can be expensive, especially for small and medium-sized enterprises, meaning the cost may outweigh any benefit to the consumer.

Often discussed in the context of data security are data minimization rules. These can hinder innovation, especially in areas like AI, predictive analytics and personalized financial services. Many financial institutions rely on broader datasets for fraud detection and to develop new financial products as well as for enhancing the user experience through personalization.

Data minimization requirements often lack clarity on what constitutes "necessary" data. This ambiguity may lead to compliance challenges for institutions when they are unsure of what data they can legally collect, creating legal risk due to potential misinterpretation of vague standards and hesitation in adopting new products or services.

Conclusion

Despite their substantial promise, fintech companies continue to face many obstacles due to an antiquated regulatory patchwork structure that is ill-suited for a rapidly changing digital landscape. Existing rules are better suited to an age when information was stored in file cabinets, and customers had to travel to physical location to conduct business. Such standards are obsolete in today's environment and cannot be rectified though a singular regulatory effort.

This is particularly critical for startup companies, enabling them to devote limited resources to expanding their products and services instead of focusing on prescriptive rules unfit for their risk profiles. This approach could also make it easier for firms to operate securely across various jurisdictions and enter new markets.

As more consumers choose nontraditional service providers to meet their financial needs, the regulatory framework must balance the imperative to ensure security and privacy with the goal of fostering innovation.

For innovation to reach its full potential and create the next generation of financial service products, all stakeholders must be able to operate on a level playing field with clear rules and regulations. An open marketplace that does not favor one technology over another or gives any one industry the ability to dominate or dictate trends is necessary to enable innovation to flourish. Such an ecosystem should allow for the teaming of platforms and services that work in concert with each other, giving consumers much more effective access to their financial services.

Fundamentally, consumers should always have the right to access all their data on their terms, for any purpose that they wish, which is why OLA advocates for strong consumer financial data rights and supports efforts to strengthen consumers' access to their financial information. Yet today there exists a significant inequity in a consumer's ability to control their data. The Bureau needs to rectify this imbalance by guaranteeing that consumers have unfettered access to their data and the ability to determine whom they share that data with at no cost.

The consumer's desire to have cutting-edge financial products has played an important role in driving market development, and it will remain the most critical motivation for future innovation. Unencumbered consumer access to their financial data enables greater consumer control over their financial choices, ultimately improving their financial health. It is incumbent on all stakeholders, banks, agencies, app developers, and third-party aggregators to work in concert towards marketplace enhancements that provide this power to consumers.

That is why OLA believes that policymakers should consider a broader approach that recognizes today's technological needs by providing greater flexibility and space to innovate. This will enable companies of all sizes to take a risk-based approach to innovation, tailoring what best works for their own business models, practices and customer needs.

The members of OLA appreciate the opportunity to share our views. We look forward to working collaboratively to reduce barriers and enhance consumer financial options. If you have questions or would like additional information, please feel free to contact me at mday@OLADC.org.

Respectfully submitted,

Michael Day
Policy Director
Online Lenders Alliance