America's Credit Unions

October 21, 2025

Comment Intake—Personal Financial Data Rights Reconsideration
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Personal Financial Data Rights Reconsideration

Dear Sir or Madam:

On behalf of America's Credit Unions, I am writing regarding the advanced notice of proposed rulemaking (ANPR) to reconsider the Consumer Financial Protection Bureau's (CFPB or Bureau) Personal Financial Data Rights Rule (PFDR Rule). America's Credit Unions is the voice of consumers' best option for financial services: credit unions. As not-for-profit, member-owned financial cooperatives, credit unions play a vital role in the financial well-being of individuals, families, and small businesses across the country. We advocate for policies that allow credit unions to effectively meet the needs of their over 144 million members nationwide.

General Comments

America's Credit Unions welcomes efforts to promote consumer choice in the financial services marketplace. Standards for promoting safe and interoperable exchange of consumer financial information can help consumers discover the benefits of establishing a relationship with their local credit union. However, the CFPB's flawed implementation of section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) does little more than burden credit unions with expensive technical requirements and lopsided risk management obligations.

The costs associated with implementing the PFDR Rule are substantial and many credit unions have expressed frustration with policy choices which operate to subsidize nonbank access to sensitive consumer financial information. The PFDR Rule does little to assuage industry concern about managing data security or privacy risks, will likely drive further consolidation within the credit union industry, and could further cement the advantage of large technology companies that are unlikely to prioritize the brick-and-mortar relationships credit unions cultivate with their communities.

The PFDR Rule's failure to meaningfully allocate liability to third parties who mishandle shared data presents an unacceptable risk to credit unions. For smaller community financial institutions, the only recourse against third parties who lose consumer data is to pursue legal claims in court; however, due to the high cost of litigation and the novelty of adjudicating such claims, legal self-help is far from a sufficient remedy. Until now, the CFPB remained aloof to the concerns raised about these facts by small financial institutions during the Small Business

Regulatory Enforcement Fairness Act (SBREFA) process, industry associations,[1] and those raised by the Small Business Administration's (SBA) Office of Advocacy.[2] Accordingly, America's Credit Unions welcomes the CFPB's willingness to reconsider the PFDR Rule and invite public comment on ways to fix it.

While the Dodd-Frank Act calls upon the CFPB to promote fair and competitive markets, the plain language of section 1033 does not reflect an intention to reengineer data sharing mechanisms to alter financial sector competition. Furthermore, the commoditization of financial data driven by the PFDR Rule's vision for open banking could result in the opposite of its intended effect: rewarding the largest, most technologically sophisticated companies at the expense of credit unions and other community institutions focused on relationship banking. To correct the poor policy choices reflected in the current rule, we ask that the CFPB consider the following changes and improvements:

- Establish a framework that permits data providers to charge reasonable fees for third party access;
- Withdraw granular technical performance specifications for the developer interface;
- Limit categories of covered data;
- Create a safe harbor for data providers who rely on evidence presented by third parties about their data security and risk management practices;
- Establish a clear allocation of liability to third parties who mishandle covered data or abuse their consumers' trust;
- Defer to the National Credit Union Administration (NCUA) when evaluating whether a credit union's denial of a third party access request is reasonable;
- Establish a framework for centralized accreditation that leverages the CFPB's supervisory resources to whitelist third parties and alleviate excessive due diligence costs for data providers; and
- Accommodate supervised financial institutions who offer legitimate secondary uses of covered data.

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

The PFDR currently adopts the Dodd-Frank Act's definition of the term "consumer" to extend regulatory coverage beyond individual requests for data to those made by "an agent, trustee, or representative acting on behalf of an individual."[3] Whether Congress intended for the CFPB to

---

[1] *See* Comment from Credit Union National Association and National Association of Federally-Insured Credit Unions, CFPB-2023-0052-0892 (December 30, 2023), *available at* https://www.regulations.gov/comment/CFPB-2023-0052-0892.
[2] *See* SBA Office of Advocacy Letter to CFPB, *available at* https://advocacy.sba.gov/wp-content/uploads/2023/12/Comment-Letter-CFPB-1033-Data-Rights.pdf (Dec. 21, 2023).
[3] 12 U.S.C. § 5481(4).

rely upon an Act-wide reading of the term to grant companies operating in arms-length transactions access to sensitive consumer financial information is doubtful.

The CFPB should adopt a more limited definition of the term consumer in a revised PFDR Rule to better effectuate the intent of section 1033. Courts have found that dogmatic application of statutory definitions must yield when context demands more nuanced interpretation, and even the CFPB has admitted that crafting the PFDR Rule to encompass any representative "stretches the definition of "consumer" past its breaking point."[4] Accordingly, the CFPB should limit the scope of third parties who may request data on behalf of a consumer to those who act in the best interest of the individual.

Agents and trustees are already presumed under common law to owe such duties to their principal.[5] The term representative, read in conjunction with terms agent and trustee, should also be interpreted in a way that demands some minimum level of responsibility.[6] Under the PFDR Rule, however, entities who can request information include platforms and intermediaries, such as data aggregators, who do not have a duty to act in the best interests of an individual whose data they possess.

Limiting the scope of entities who may request access to consumer data would alleviate some of the inherent privacy and security risks associated with data exchange between data providers and third parties operating outside the guardrails of a well-defined, contractual relationship.

Under the PFDR Rule, which eschews negotiated data sharing agreements for a regulatory right of access, data providers shoulder a disproportionate risk management burden in terms of vetting non-depository third parties and responding to consumer inquiries about mishandled or inaccurately reported information. To mitigate these burdens, the CFPB should generally require third parties to act in the best interest of the individual whose data they receive. The CFPB should further affirm that credit unions, as supervised and examined financial institutions, will remain eligible to receive consumer data as third parties under a revised rule.

Allocating Liability to Third Parties

To better allocate liability when shared data is mishandled, the CFPB should require third parties to provide data providers with an indemnification against claims arising under the Electronic Fund Transfer Act (EFTA) and Regulation E which involve initiation of an unauthorized payment using credentials shared by the data provider that can be uniquely linked to the third party (e.g., tokenized credentials). For example, if a payment is initiated using a token shared with a third party and that token is attributable to the third party, then there should be no

[4] *See* Envt'l Def. v. Duke Energy Corp., 549 U.S. 561, 574 (2007); *see also* Defendants' Memorandum in Support of Their Motion for Summary Judgment, 8, *Forcht Bank, NA v. Consumer Financial Protection Bureau,* 5:24-cv-00304, (E.D. Ky.) [hereinafter Def.'s Memo].

question that the third party is solely responsible to the consumer for any unauthorized transaction, regardless of whether the account from which the funds were transferred belonged to the data provider.

Although section 1033 is not generally regarded as a payments regulation, the PFDR Rule's coverage of information sufficient to initiate an electronic payment warrants special treatment. Given this context, allowing data providers to make an indemnity claim against third parties for unauthorized transaction losses based on the attributable characteristics of a specific transaction would be consistent with other payment regulations, such as Regulation CC.[7] Additionally, delimting the scope of third parties permitted to access consumer information based on their agreement to indemnify data providers against such losses would be consistent with the authorities granted to the CFPB under section 1033.[8]

Conditioning access on an appropriate indemnification for downstream liability (separate and apart from a safe harbor, which is discussed below) would alleviate a core defect in the PFDR Rule, which is the absence of any regulatory framework for holding third parties accountable for mishandling shared data. While not all categories of covered data may be appropriate targets for such a framework, data elements that can be attributed to a particular third party might serve as a starting point.

Defrayment of Costs in Exercising Rights Under Section 1033

The PFDR Rule currently prohibits data providers from charging fees to either a consumer or an authorized third party when accessing covered data. Notably, section 1033 contains no statutory prohibition against fees that would preclude reasonable cost recovery for data providers. The CFPB's decision to prohibit fees places burdens on many smaller data providers, including credit unions, who must build and maintain performant APIs to meet "developer interface" requirements. For credit unions, the burden of protecting members' financial data is significant since it involves not only the entire IT infrastructure which supports digital and online banking operations, but also the specific costs associated with due diligence of third parties, undertaking risk assessments, and mitigating data breaches and security incidents that occur beyond the walls of regulated financial institutions. Credit unions also face examination and compliance costs related to supervision of data security.

While a mechanism for reasonable cost recovery would help defray some of the compliance costs associated with the rule, it remains uncertain how such an allowance—without more—would influence competition between those institutions that can afford to pay for data and those that cannot.

---

[7] *See e.g.*, 12 CFR § 229.34(f) (conditioning an indemnity for losses incurred by checks already paid by remote deposit capture on the absence of a restrictive indorsement born on the check).
[8] *See generally*, 12 U.S.C § 5533(a).

The PFDR Rule fundamentally alters marketplace competition between financial institutions such that if nothing else were to change except for a new allowance for fees, small institutions could still find themselves at a disadvantage relative to larger institutions. Because the rule does not outright prohibit screen scraping by third parties, fintechs and other companies might resort to such techniques to avoid fees if introduced in a revised rule.[9] Accordingly, by permitting fees without a clear prohibition on screen scraping, the CFPB risks undermining a core purpose of the rule: to make exchange of consumer data more secure. On the other hand, if the PFDR Rule were amended to require that all data requests pass through consumer or developer interfaces, then fees charged for API access could be used to gatekeep consumer data, which would impair the data portability objectives of the rule.

At least one large bank has signaled its willingness to demand payment for third-party data access—a development that perhaps rationalizes the CFPB's original claims about how the PFDR Rule could alter financial sector competition.[10] As data providers and aggregators recalibrate their strategies in an anticipation of a revised PFDR Rule, the CFPB should monitor markets, but generally disfavor complex price controls which could be difficult to administer or which could prevent reasonable cost recovery needed to accommodate secure, third-party API access. As a point of comparison, the exchange of personal health information is regularly performed by third parties who comply with the Health Insurance Portability and Accountability Act (HIPAA), a law that does not adopt a total ban on fees.[11] The CFPB might consider investigating whether HIPAA's allowance for cost recovery by healthcare companies transferring HIPAA information on behalf of individuals has spurred or hindered competition.

The CFPB should also refrain from adopting rules that aim to directly influence marketplace competition absent clear evidence of a market failure or monopolistic pricing.[12] If the PFDR Rule did not exist at all, it is doubtful that API fees alone would deal a fatal blow to what many industry observers foresee as an inevitable transition to open banking—with or without the CFPB's intervention.[13] But the PFDR Rule has now instigated a race to capitalize on the prospect of *free* data, and even the most well-intentioned and carefully calibrated rules for cost recovery risk subordinating the discipline of the market for the judgment of courts and regulators. In this context, where the PFDR Rule itself creates the problem that must be solved (the question of remuneration for data accessed by regulatory privilege), the CFPB's best course of action may be to adhere as closely as possible to the Executive Order on Reducing Anti-Competitive Regulatory

---

[9] *See* CFPB, Personal Financial Data Rights Reconsideration, 90 Fed. Reg. 40986, 40988 (August 22, 2025) (prohibiting "*data providers* from relying on a third party's use of screen scraping to access the developer interface") (emphasis added).
[10] *See* Payments Journal, "Plaid Agrees to Pay JPMorgan Chase Fees to Access Data" (September 16, 2025) *available at* https://www.paymentsjournal.com/plaid-agrees-to-pay-jpmorgan-chase-fees-to-access-data/
[11] *See* 45 CFR 164.524(c)(4).
[12] *See* CFPB, Required Rulemaking on Personal Financial Data Rights, 89 Fed. Reg. 90838, 90976 (November 18, 2024).
[13] *See* CCG Catalyst, "Open Banking in the US: How Did We Get Here?" (July 23, 2025), *available at* https://www.ccgcatalyst.com/thought-leadership/commentary/open-banking-in-the-us-how-did-we-get-here/.

Barriers, whose preamble states that "[f]ederal regulations should not predetermine economic winners and losers."[14]

Privacy Concerns in the Exercise of Section 1033 Rights

As both data providers and data accessors, credit unions are subject to privacy laws such as the Gramm-Leach Bliley Act (GLBA) and Regulation P, whose applicability to the exchange of nonpublic personal information does not depend on the PFDR Rule. For entities not subject to these laws, and those that do not receive the same exam-based supervision as credit unions, strong consumer consent provisions are necessary to protect the privacy of sensitive financial information shared with third parties.

The CFPB has noted in prior rulemakings that "the nation's largest data brokers boast that they possess information about hundreds of millions of American consumers consisting of billions of data points, with some data updated instantaneously."[15] The current ANPR observes that over the past decade various data brokers have reported substantial data breaches, the cumulative effect of which has been the gradual erosion of consumer privacy and security.[16]

The main tool for addressing consumer privacy concerns is already present in the PFDR Rule—a strong authorization framework which requires a third party to obtain the consumer's consent before collecting specific types of covered data. In conjunction with this process for obtaining consent and validating a consumer's authorization, data providers should be permitted to confirm the consumer's selection of transferred data and, at the time of confirmation, include additional information that may be relevant to the consumer's authorization request—such as a disclaimer that the credit union is not liable for any representations or warranties the third party makes about the security of data it collects.

Data privacy would also be enhanced with a clear revocation process for consumers. The CFPB should maintain the PFDR Rule's general approach of treating a revocation request as "all or nothing" for the purposes of data provider compliance, but should reconsider the current allowance granted to third parties to keep data after revocation under circumstances unrelated to a legal recordkeeping obligation.[17] Specifically, the CFPB should not allow a third party to retain data merely because use or retention of the covered data "remains reasonably necessary to provide the consumer's requested product or service."[18]

---

[14] Executive Order 14267, "Reducing Anti-Competitive Regulatory Barriers" (April 9, 2025).
[15] CFPB, "Protecting American from Harmful Data Broker Practices" 89 Fed. Reg. 101402, 101406 (December 13, 2024).
[16] *See* 90 Fed. Reg. 40988.
[17] *See* 12 CFF § 1033.421(i).
[18] 12 CFF § 1033.421(i)(2).

Information Security Concerns in the Exercise of Section 1033 Rights

One of the most significant concerns for credit unions regarding implementation of section 1033 relates to the security of their members' information. Many credit unions worry that members who share access to account data with unvetted third parties will be more vulnerable to fraud. One study regarding the relationship between fraud and consumer use of data aggregators suggests that these concerns are not unwarranted; a large Australian bank has reported that "customers with logins via an aggregator are two or more times more likely to experience fraud."[19] However, screen scraping or inadequate security at the data aggregator level are not the only threats. The breach of a U.S.-based data broker in December 2023 resulted in one of the largest thefts of consumer data in recent history, involving 2.7 billion records.[20] Third party access to consumer financial data may also increase risk exposures to unrelated fourth parties, such as cloud-based storage and analytics platforms—even if third parties are prohibited from selling data a consumer has shared.[21]

While the data security practices of some third parties may be subject to the FTC's enforcement jurisdiction, the FTC's Safeguards Rule (the standard adopted for nonbanks under the PFDR Rule) is not as comprehensive as the information security standards adopted by federal banking agencies and the Federal Financial Institutions Examinations Council (FFIEC). Moreover, the FTC does not actively supervise companies for compliance with its own Safeguards Rule.

In the absence of a national federal data security standard and national data privacy standards, granting entities who are not subject to substantially similar laws and regulations broad data access privileges would be irresponsible. For this reason, simply requiring third parties to comply with the FTC's Safeguards Rule is wholly insufficient. All parties who collect or hold consumers' personal financial data should be held to the same standards. Like the risks to inaccurate data discussed above, the security and privacy risks related to financial data are no less serious when the data is held at a non-depository institution.

To mitigate data security risks, the CFPB should adopt, in addition to the general Safeguard Framework described in the PFDR Rule, the IT security guidance promulgated by the FFIEC agencies as the appropriate standard for third parties accessing information at depository institutions.

---

[19] *See* Clancy Yeates, "Very concerning correlation: CBA warns against screen scraping," Sydney Morning Herald (March 17, 2020), *available at* https://www.smh.com.au/business/banking-and-finance/veryconcerningcorrelation-cba-warns-against-screen-scraping-20200316-p54am8.html.
[20] *See* Letter from Sen. Chuck Grassley to Jerico Pictures (August 16, 2024), *available at* https://www.grassley.senate.gov/imo/media/doc/grassley_to_jerico-national_public_data_-_national_public_data_hack.pdf.
[21] *See* Nightfall AI, "What Happened in the Snowflake Data Breach?" (August 1, 2024), *available at* https://www.nightfall.ai/blog/what-happened-in-the-snowflake-data-breach.

With respect to the PFDR Rule's allowance for "reasonable denials" of third-party requests to access consumer data based on risk management concerns, the CFPB should clarify in a revised rule that the reasonableness of a data provider's decision to grant or deny access will be determined by the agency responsible for overseeing the data provider's compliance with technical safeguard requirements under the GLBA. For credit unions, the GLBA assigns that responsibility exclusively to the NCUA.

Under the current PFDR Rule, the CFPB disregards the jurisdictional limits of the GLBA to establish oversight of credit union risk management decisions. In other words, the CFPB could, at its discretion, determine that a third party should receive data access even if NCUA examiners voice concern about potential negative consequences. This approach is not only improper based on the GLBA's assignment of data security responsibilities to the NCUA as the appropriate prudential regulator for credit unions, but also impractical. Case-by-case reviews of a credit union's decision to deny certain third parties access could invite inconsistent application of risk management expectations by the CFPB and NCUA, resulting in confusion and potential harm to information security programs.

The CFPB should also consider mechanisms to reduce the costs data providers will incur to ensure a high level of data security. One way to reduce data provider costs would involve the CFPB whitelisting nonbank third parties who represent that they satisfy appropriate data security and risk management requirements. The CFPB could facilitate ongoing accreditation of third parties by administering its own risk management assessments of entities not otherwise subject to examination and supervision by a functional banking regulator. A whitelist would help defray the costs incurred by data providers of conducting potentially numerous risk assessments for third parties who choose to access covered data directly rather than through a data aggregator. A corresponding accreditation process managed by the CFPB would also provide the agency with better understanding of the practices of data aggregators and other third parties who are today largely unsupervised.

Whether or not the CFPB facilitates whitelisting of third parties, the agency should also grant credit unions a safe harbor from liability when a third party represents that it meets appropriate data security standards.

Under the PFDR Rule, a credit union bears the risk of granting a third party access to consumer data because the third party is under no obligation to offer specific contractual warranties, assume liability, or make arrangements for insurance.[22] Instead, the PFDR Rule directs data providers "to take account of their risk management obligations" while simultaneously refusing to enumerate specific and presumptively reasonable grounds for denial.[23] For many credit

[22] *See* 89 Fed. Reg. 90899. The PFDR declines to create either express regulatory authorization for or prohibition against onboarding arrangements that seek third parties' assumption of particular allocations of liability.
[23] 89 Fed. Reg. 90898. The PFDR Rule even hesitates to say definitively whether safety and soundness or information security standards are *per se* reasonable grounds for denial, offering only that they "might" serve as a legal basis for denying a third party access.

unions, the lack of any limitation on liability in the current rule is likely to correspond with high litigation risk in the event a third party experiences a data breach. Even if a credit union follows all legal requirements before enabling access, consumers might still allege negligence during the onboarding process. A comprehensive safe harbor is necessary to give credit unions reasonable assurance that section 1033's right of access is not abused and signal to consumers that they too bear responsibility for managing the risks of enabling third party access.

Secondary Uses of Data

Under the PFDR Rule, third parties are required to limit the collection of covered data to what is reasonably necessary to provide the consumer's requested product or service. This limitation is generally appropriate in cases where the recipient is not a supervised and examined financial institution; however, a redline prohibition against secondary uses of data does little to promote competition or achieve any of the important benefits of making consumer data more portable. Accordingly, the CFPB should reconsider the scope of this prohibition in a revised rule.

Financial institutions that are highly regulated, supervised, and examined should be permitted to obtain consumer authorization for legitimate secondary uses of covered data (such as member budgeting and holistic financial management) when they are third party recipients of consumer information. The authorization for these secondary uses of data should mirror the authorization disclosure described in § 1033.411. If a consumer can accept a financial institution's stand-alone product or service in the marketplace, then they should be able to opt-in to that same product or service in an open banking context.

This consent-based approach would allow consumers to opt-in or opt-out of having their covered data used for targeted advertising and cross-selling. The adoption of this caveat for secondary uses will provide significant consumer benefits and allow financial institutions and their affiliates to utilize the categories of covered data to offer consumers more competitive products and services. It will also allow financial institutions to use covered data to strengthen their relationships with members and add meaningful value to the products and services provided by allowing the development of insights about the members to better serve them, such as using the data to provide the member with personalized "insights" about their linked accounts, such as the savings they could enjoy if they switched accounts. These amendments to the PFDR Rule would help catalyze meaningful competition, particularly in an environment where API access fees are permitted.

While it is reasonable to regulate secondary uses of consumer data disclosed to third parties to ensure the data is not improperly used at the expense of the consumer, permitting reasonable secondary uses of data by supervised and examined credit unions can help deliver benefits to members.

Reconsideration of Covered Data Categories

Under the PFDR Rule, the categories of covered data credit unions must share with third parties goes beyond the scope of section 1033's plain statutory language and must be significantly pared back.

The CFPB should not include pending transaction information as a category of covered data. Sharing such information could be problematic because the status of transactions is continually subject to change, and the exact timing of settlement will not be known to a data provider under most circumstances. Pending transaction information could be outdated immediately following the data request causing, at a minimum, consumer confusion, and potentially serious consumer harm if outdated information is used to make decisions about products and services offered to the consumer. For this reason, the CFPB's intended beneficial consumer use cases of "fraud detection and personal financial management" are not supported by the inclusion of pending transaction information.

The CFPB should limit the amount of historical transaction data that data providers must make available to 12 months. Some credit unions may not store historical information about a consumer account in the same systems that generate current statements for members. Accessing historical information may correspond with greater time and effort for credit unions and it may be the case that certain data elements will be reported differently for different time periods depending on the use of particular systems, formatting, or vendor solutions.

The CFPB should also seriously reconsider its decision to allow third parties to request "information to initiate payment to or from a Regulation E account." Transmission of routing and account numbers outside of secure payment systems could expose credit unions to a significant risk of fraud if the information is lost or mishandled by a third party. Credit union members would also face corresponding privacy risks and potentially greater exposure to identity theft.

While tokenized account and routing numbers (TANs) are industry innovations that help mitigate fraud risk for both consumers and financial institutions, they are relatively new advancements that many small financial institutions have not yet adopted. TANs can be costly, and implementation is dependent upon the financial institution's service partner and their offerings. For this reason, many of the most vulnerable data providers would not be able to take advantage of this innovation and protection from the start causing significant market inequities that could exacerbate the impact of bad actors taking advantage of a new system. A revised rule should exclude this category of covered data to protect financial institutions and consumers until TANs have reached ubiquity in the marketplace.

The final rule should not include terms and conditions as a category of covered data in this rulemaking. The cost and burden for data providers to manage product-level terms and

conditions documents and to make those conveyable through data fields in an API would vastly exceed the benefit to consumers.

The CFPB should reconsider bill pay data as a category of covered data. The final rule envisions a consumer scheduling these payments with their financial institution for extraction to the payee when in reality, the consumer almost always schedules these transactions through the payee's platform. Furthermore, data used in automatic bill pay systems may not reside within a single repository or have standardized formatting, making reporting of this information technically complex.

Standard Setting

As the CFPB considers revising the PFDR Rule, it should aim to retain certain conceptual features that have proven beneficial for standard setting purposes. The CFPB has already recognized the Financial Data Exchange as an approved industry standard setting organization to facilitate implementation of section 1033. A revised rule should preserve this recognition to ensure continuity in technical specifications and minimize the disruption that would inevitably result from identifying a new standard setter. The CFPB should also retain the PFDR Rule's emphasis on a standard setting organization possessing a governance structure that ensures adequate representation of consumers and smaller community financial institution perspectives.

Compliance Dates

America's Credit Unions supports reconsideration of the PFDR Rule's compliance timeframes. The current tiered implementation framework should be adapted to provide large credit unions (e.g., those above $50 billion in total assets) with at least five years for implementation, particularly if a revised rule carries over substantially similar developer interface requirements. Smaller credit unions will also need a longer period to comply if the CFPB chooses to retain the interface requirements.

As the CFPB considers adjustments to compliance deadlines or the tiers used for implementation purposes, it should avoid creating large cohorts of institutions which could bottleneck core provider resources. Smaller credit unions do not receive the same attention from cores and service providers as large banks. Differences in bargaining power and in-house expertise mean that community institutions must often plan around the limited bandwidth of their cores when implementing new regulations, and the CFPB should be mindful of these limitations if it pursues a technically complex rulemaking.

Conclusion

America's Credit Unions is grateful for the CFPB's willingness to revise the PFDR Rule and solicit public comment through the ANPR. We are encouraged by the CFPB's attention to rectifying

flawed assumptions in the PFDR Rule which have contributed to an untenable expansion of section 1033. Safe and interoperable data exchange standards can help credit unions improve consumer experiences, but to achieve this outcome the CFPB must reexamine its prohibition on fees, the allocation of risk management responsibilities placed on data providers, and the guardrails needed to ensure strong data security and privacy protections for consumers.

Thank you for considering our comments. Should you have any questions, please contact me at amorris@americascreditunions.org.

Sincerely,

Andrew Morris
Director, Innovation and Technology