TECHNET
THE VOICE OF AMERICAN INNOVATION

1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

October 21, 2025

The Honorable Russ Vought
Acting Director
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

Re: Personal Financial Data Rights Reconsideration (Docket No. CFPB-2025-0037)

Dear Acting Director Vought:

Thank you for the opportunity to submit comments on the Bureau's proposed reconsideration of the Personal Financial Data Rights Rule. TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes over 100 dynamic American businesses ranging from startups to the most iconic companies on the planet, representing over five million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

As TechNet expressed in previous comments in 2021 and 2023 on prior iterations of this rule, we strongly support the CFPB's goal of empowering consumers to access and share their financial data securely. Consumer-authorized data sharing is the foundation of open banking and a cornerstone of consumer choice and financial innovation. Ensuring that Americans can freely and safely connect their financial accounts to trusted applications is critical to maintaining U.S. leadership in digital assets, artificial intelligence, and next-generation payments systems. At the same time, any rule implementing Section 1033 of the *Dodd-Frank Act* must ensure clarity for consumers and businesses, safeguard data security, and provide realistic compliance pathways. Without these guardrails, the rule risks undermining consumer trust and creating significant operational and legal uncertainty.

Consumers must be confident that their data and privacy are protected no matter where they live, and businesses across industries need certainty about their regulatory responsibilities so they can spend more time innovating and less time hiring compliance lawyers. Private sector efforts are empowering consumers to better manage their financial lives and enjoy new, safe, secure, inclusive, and reliable financial tools. Both consumers and merchants benefit from an open and fair banking system, including innovative, fast, and nominal payment applications,

improved credit underwriting, and personal financial management services. This rule should provide consumers with the right to access and share their financial records and securely request that their financial information be accessed and shared with authorized third parties by aligning data definitions, rights, and responsibilities with existing privacy and data protection frameworks. Businesses likewise need certainty to design compliance systems and avoid conflicting obligations. Ambiguity erodes trust, increases costs, and risks enabling anti-competitive conduct by incumbents seeking to limit consumer access.

TechNet continues to support the implementation of an open finance regulatory regime that establishes a robust consumer data right that promotes the free flow of consumer-authorized data across the financial ecosystem allowing consumers broader access to financial services and control over their financial data. Consumers should have a flexible, consent-based framework to understand how their information will be shared, transmitted, stored, and utilized, and should have clear rules for consenting to such use. And as the CFPB reexamines this rule, it should also take the opportunity to clarify ambiguities around liability for unauthorized access, privacy, credit reporting, and data accuracy to provide clear rules of the road for consumers and for companies.

Clarity for Businesses and Consumers

Consumers need and deserve transparent rules about what data is shared, with whom, and for what purposes. Businesses likewise need certainty to design compliance systems and avoid conflicting obligations. Ambiguity erodes trust and increases costs. The CFPB should take this opportunity to more clearly define "providers," "agents," and "representatives." One helpful clarification would be to establish that any authorized entity that can meet a minimum set of security standards established by an industry-led body and endorsed by the Bureau should be considered a representative of an individual for purposes of implementing Section 1033 access rights. The rule should also ensure that consumers receive plain-language disclosures about who will receive their data and how it may be used.

Additionally, the CFPB should remove or significantly limit the "facilitation" prong in the definition of data providers. As drafted, this category could sweep within scope a broad range of entities — such as online marketplaces, point-of-sale terminals, or applications that merely store payment credentials — that do not hold the categories of "covered data" contemplated by Section 1033. These intermediaries typically rely on regulated financial institutions for transaction and account information. Bringing them within scope would yield duplicative or incomplete data, increase costs, and expand cybersecurity risk without meaningful consumer benefit.

The Bureau should also clarify that payment-method or pass-through digital wallets are not covered data providers. Covering marketplaces, point-of-sale terminals and pass-through digital wallets would yield no useful information or additional benefit given that customers and authorized third parties would be able to obtain the relevant transaction data from the issuers of the debit or credit card themselves.

These tools store payment credentials to facilitate consumer-initiated payments but do not maintain the account balances, terms, or billing information envisioned by the rule. Requiring them to build data-sharing interfaces would provide no incremental consumer benefit while imposing significant technical and legal obligations, especially on smaller or emerging providers. In addition to significantly expanding the reach and burden of the rule, the more entities that are required to comply with the final rule and are thus obligated to provide requested data to consumers and authorized third parties the greater the opportunity for abuse and data theft. Narrowing the rule's reach will align it with the CFPB's focus on addressing concrete consumer harms rather than expanding compliance burdens to low-risk intermediaries.

Data Security and Liability

Financial data is among the most sensitive categories of consumer information, so requiring providers to transmit sensitive financial data to unvetted third parties based on unclear standards increases risks of fraud and breaches. TechNet recommends that the CFPB adopt a clear liability framework that specifies which party is responsible when unauthorized access or misuse occurs. Data providers should not be held liable for harms that arise after information has been lawfully transferred to authorized third parties. Consumers must also have accessible avenues for redress when their information is misused. At a minimum, any final rule should: (i) clarify the Electronic Fund Transfer Act and Regulation E's applicability to ecosystem participants in an open finance regime; (ii) affirm that the FTC's July 2011 guidance regarding "conduit functions" applies to ecosystem participants that are engaging in authorized data access; (iii) establish that prudential regulators' third-party oversight guidance does not form the basis for unilateral restrictions on consumer-authorized data access to nonproprietary financial information; and, (iv) clarify that the *Gramm-Leach-Bliley Act* and its implementing regulations do not require re-confirming permissioning every time a consumer authorizes their data to be shared.

TechNet believes that regulators should look to industry-developed interoperability, portability, and security standards for ensuring a seamless, standardized, and secure experience for responsibly sharing consumer data. However, delegating technical specifications to industry partners risks providers facing looming deadlines before workable standards are finalized. Therefore, we recommend that compliance deadlines be timed related to the issuance of sets of standards, rather than a fixed date. This would help prevent companies from facing statutory deadlines without applicable standards ready or sufficient time to develop compliance processes.

In parallel, the CFPB should not impose additional and duplicative privacy or security standards beyond those already established under federal and state law. Existing frameworks—including the *Gramm-Leach-Bliley Act*, the *California Consumer Privacy Act*, and other state privacy statutes—already provide robust protections for financial data privacy and security. Leveraging these existing frameworks, as the current rule does, strengthens consumer safeguards while preventing overlapping and inconsistent obligations.

Consumer Consent and Data Use

TechNet supports the CFPB's emphasis on informed consent as the basis for consumer data sharing. However, the proposed limits on secondary data uses, such as targeted advertising and cross-selling, could unintentionally restrict consumer choice and limit innovation. Consumers should retain the ability to decide whether and how their data is used beyond the original purpose, provided that consent is clear, informed, and revocable.

The CFPB should empower customers to decide what is shared, with whom, and for what purpose in a fast, easy and secure way. Customers should be provided with clear choice as to the use of their data in a single, transparent consent. The CFPB should allow for more durable, ideally non-expiring, consent mechanisms that allow for broader, transparent consent to be obtained in a single user interaction to cover multiple data uses, thereby reducing customer friction and operational overhead while maintaining user control. Customers should be provided with clear and transparent means to revoke consent and be able to achieve their desired outcomes more efficiently and with less burden.

Blanket prohibitions on secondary data use are not grounded in Section 1033 and would deny consumers the opportunity to benefit from personalized services that save them time and money. Many consumers prefer tailored experiences and are willing to share their data when doing so yields better offers or improved financial management tools. The CFPB should allow authorized third parties to use consumer data for secondary purposes with explicit, informed consent. This approach respects consumer autonomy, aligns with established privacy frameworks, and supports responsible innovation.

Consistent with existing privacy laws and frameworks, the CFPB should acknowledge that data that has been anonymized and/or aggregated should not be subject to the controls of the Section 1033 rule as it is no longer personal information. Third parties should be able to use this data for other purposes such as fraud detection, product research and development, and improving existing features and services that benefit the consumer and drive competition and innovation in the marketplace.

Cost, Fees, and Implementation

Building and maintaining secure application programming interfaces (APIs) for third-party data sharing could require significant financial and personnel resource investments by both providers and recipients. However, these investments may disproportionally burden smaller data recipients. To ensure that providers of all sizes can successfully implement the rule and provide necessary security for consumers, TechNet urges the CFBP to refrain from permitting account access fees or other charges for consumer-authorized data sharing. Such fees are inconsistent with the purpose of Section 1033, anti-competitive in effect, and contrary to consumer interest. Allowing large financial institutions to charge for access to a consumer's own data would undermine the principle of consumer ownership, create barriers for new entrants, and restrict consumer choice. It would also disadvantage

small businesses and innovative service providers that rely on open banking connections to offer low-cost financial tools. The CFBP should make clear that data access fees are not permitted and that consumers have a right to connect their accounts to applications of their choosing without cost. Data belongs to the customer, and control of that data must not be used to entrench incumbents or stifle competition. Preserving open, cost-free access will advance the CFPB's mission of promoting fairness, transparency, and innovation in financial services.

To the extent the agency does contemplate fees, those fees should be strictly defined and capped, limited to covering direct administrative or incremental delivery costs. Any fees must be accompanied by robust oversight, independent audits, and periodic review to ensure these fees remain temporary and do not evolve into enduring barriers to competition or consumer rights.

Implementation must also be realistic and tied to the readiness of technical standards. Building and maintaining secure application programming interfaces (APIs) requires significant investment, particularly for smaller institutions. The CFPB should allow at least 24 months from the release of final technical standards for compliance and should link implementation timelines to the publication of such standards rather than fixed calendar dates. Phased timelines will help ensure that companies of all sizes can develop compliant, secure, and scalable systems without compromising consumer protection.

The Bureau should avoid imposing fiduciary duties on data providers or authorized third parties unless such obligations already exist under law. Fiduciary duties traditionally apply to entities that manage consumer assets or funds, such as banks or investment advisers—not to those that facilitate data exchange. Expanding these obligations would introduce substantial legal risk without improving consumer outcomes and could deter participation in open banking frameworks. Current laws already provide remedies for misconduct, making additional fiduciary designations unnecessary.

We also encourage the Bureau to clarify that Section 1033.211 applies to instant payment rails like RTP and FedNow, and requires information to initiate payments on these rails, where available. Given that consumers often have access to multiple payment options from a single account, this approach would maximize innovation opportunities for Authorized Third Parties while ensuring consumers benefit from the full range of payment services their financial institutions provide. This more comprehensive disclosure ensures that market forces and consumer preferences—rather than provider discretion—determine which payment rails are utilized by consumers and their representatives.

Open banking is about more than access—it is about ensuring that the United States continues to lead in the next generation of financial technology. Restricting data access or allowing large incumbents to impose new barriers would weaken the nation's position in critical fields such as digital assets, artificial intelligence, and digital payments. Consumers benefit when innovative American companies can compete on a level playing field and when the regulatory system encourages secure, consumer-authorized data sharing rather than restricting it.

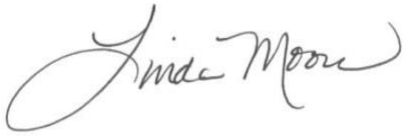
Conclusion

TechNet supports the CFPB's efforts to empower consumers and foster innovation in financial technology. To succeed, the rule should ensure clarity, establish a fair liability framework, safeguard consumer data, and provide realistic compliance timelines. Specifically, the rule should:

- Affirm that consumers own their data and have the right to share it freely with authorized third parties;
- Narrow the scope of covered entities to exclude low-risk facilitators and pass-through digital wallets;
- Clarify the liability framework and avoid imposing new fiduciary or duplicative privacy obligations;
- Prohibit account access fees and ensure cost-free data portability; and
- Adopt phased, standards-linked implementation timelines to enable secure compliance.

By focusing on these principles, the CFPB can deliver a durable, innovation-friendly open finance framework that protects consumers, fosters competition, and upholds America's leadership in financial technology. We look forward to working with the CFPB to build a framework that protects consumers while enabling continued growth in America's financial technology ecosystem.

Sincerely,



Linda Moore
President and CEO