October 21, 2025

*Via www.regulations.gov*

Consumer Financial Protection Bureau
1700 G Street, N.W.
Washington, DC 20552

**RE: Advance Notice of Proposed Rulemaking, Personal Financial Data Rights Reconsideration; Docket No. CFPB-2025-0037**

Ladies and Gentlemen:

Mastercard International Incorporated ("Mastercard") submits this comment letter to the Consumer Financial Protection Bureau ("CFPB") in response to the advance notice of proposed rulemaking on personal financial data rights (the "ANPR")[1] to inform the consideration of issues related to the implementation of Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Section 1033").[2] Mastercard appreciates the opportunity to provide comments on the ANPR.

***Background on Mastercard***

Mastercard is a technology company in the global payments and open finance (encompassing open banking) industries. Mastercard operates the world's fastest payments processing network, connecting consumers, financial institutions, merchants, governments, and businesses in more than 210 countries and territories. Moreover, Mastercard powers feature rich open finance platforms globally. Mastercard Open Finance provides secure and trusted information and services, which power economies and empower people—consumers and businesses alike—with innovative tools to leverage their own data for their own financial benefit. Mastercard's experience facilitating global payments and cross-border transactions also allows us to create interoperability between different open finance markets around the world.

Mastercard believes there is immense value in connecting consumers and small businesses with their financial data and providing them with the tools to do so for their own benefit. Put simply, we believe that consumers and businesses own their data; have the right to control their data; should benefit from the use of their data; and that Mastercard's job is to enable the sharing of that data and to protect it. We also believe that data, particularly data that has been de-identified, plays a pivotal role in allowing industry to innovate constantly to ensure individuals benefit from the use of their data through better experiences, products and services.

[1] 90 *Fed. Reg.* 40,986 (Aug. 22, 2025).

[2] 12 U.S.C. § 5533.

In the United States, Mastercard is a leading data aggregator in the open finance industry and in the use of application programming interface ("API")-based connectivity to access data. We provide a myriad of services to authorized third parties and data providers, big and small. As banks have increasingly made APIs available in anticipation of the compliance dates under the existing Personal Financial Data Rights final rule ("PFDR Rule"), and to meet increasing customer demand, we have been working to enable more secure, enriched and consumer-controlled data sharing. Consequently, our services provide far more than just a conduit between data providers and authorized third parties. We also provide open finance services directly to consumers. With a holistic approach to serving the consumer financial ecosystem, we enable a secure and transparent experience that enriches a consumer's financial life.

***Comments***

The open finance industry has experienced remarkable development over the past several years. This change has enabled consumers to benefit from new opportunities and to leverage their financial data in new and innovative ways. As consumers use and demand more personalized digital tools to save time and money, and look to improve their financial outlook, financial services innovators utilize open-finance solutions to drive stronger consumer engagement and loyalty. The growth of the U.S. open finance ecosystem is so robust because consumer demand for better, faster, less expensive and more efficient financial services has been met by participants in the open finance ecosystem. These participants collectively deliver seamless connectivity and innovative financial products that give consumers control over and access to their financial data. Mastercard believes that ensuring consumers have access to their data is of the utmost importance. Doing so empowers consumers to benefit from the use of their financial data with a wide variety of third-party apps and services that offer new experiences. We also believe that consumer data ownership and access rights are fundamental to open finance as they are foundational to build trust in the broader financial ecosystem.

Mastercard appreciates the CFPB's efforts to reconsider the PFDR Rule. Mastercard's comments address the following topics: (i) a consumer's right to authorize any third party to access the consumer's data and the interpretation of "representative"; (ii) the need for the CFPB to coordinate with the prudential bank regulators to set standards for denial of access based on information security concerns; (iii) privacy concerns and permitted usages of data; (iv) roles in the open finance ecosystem and the necessity for the CFPB clarify and expressly state that a party may serve as both a data aggregator and an authorized third party; and (v) additional issues of concern with the PFDR Rule. Below we discuss our comments in more detail.

I. *A Consumer's Right to Third Party Data Sharing - Interpretation of "Representative"*

Section 1033 provides that a consumer has the right to access information concerning financial products and services used by the consumer. Section 1033 is an acknowledgement that consumers own their financial data and have the right to access and use their data as they see fit. A "consumer" for purposes of Section 1033 includes not only an individual but also an agent, trustee, or representative acting on behalf of an individual.[3] The PFDR Rule interprets Section

[3] 12 U.S.C. § 5481(4).

1033—including the term "representative"—in a manner that requires data providers to make consumer financial information available to any third party authorized by an individual.[4] However, the ANPR seeks comments on how the term "representative" as used in Section 1033 should be interpreted, with a suggestion that "representative" could be interpreted to make it harder for consumers to control their own data. There is no evidence that Congress intended to restrict a consumer's access rights and we do not believe CFPB should do so in a reconsidered PFDR Rule.

Therefore, we encourage the CFPB to interpret the term "representative" broadly and to require data providers to make data available to any entity authorized by an individual. An individual's ability to access and share his or her own financial data with third parties that the consumer chooses is the bedrock principle of open finance. As discussed above, Mastercard believes that individuals own their data and should have a right to use and share their data for their own financial benefit.

Interpreting "representative" in a way that would limit a data provider's obligation under the PFDR Rule to make data available to third parties authorized by an individual would severely limit an individual's ability to use his or her own data in concert with third-party products and services. Indeed, it would be a very odd result if a consumer could directly access his or her data from a data provider (*e.g.*, on the data provider's website) and transmit the data to a third party (*e.g.*, by email) but could not authorize the same third party to access the data from the data provider on the his or her behalf. It is difficult to see what public policy objective that approach would serve, but easy to predict the damage it would inflict on consumer choice and product innovation.

Instead of narrowly defining "representative" to the detriment of consumers or placing undue burdens on third parties that an individual chooses to share their data with, Mastercard believes there should be a clear obligation on data providers to make data available to any third parties that are authorized by an individual.

## II. *Information Security & Coordination with Prudential Regulators*

The PFDR Rule attempted to address information security concerns in various ways, one of which would permit a data provider to reasonably deny access to its developer interface based on a risk management concern, such as an information security issue.[5] The ANPR seeks comments on the threat and cost-benefit of securing consumer financial data and specifically asks whether the PFDR Rule provides adequate protections for the security of consumer data.

Mastercard believes a secure data sharing ecosystem that protects consumers and stakeholders is critical for open finance in the United States. However, lack of clarity related to the expectations of the CFPB and the prudential bank regulators regarding when security-related access denial is appropriate could create uneven consumer experiences and negatively impact use

[4] 12 C.F.R. § 1033.331(b)(1).

[5] 12 C.F.R. § 1033.321(a)(1)(ii).

of open finance products and services. In particular, we believe that some banks will scrutinize authorized third parties against the prudential bank regulators' high standards for risk management of third-party relationships, as documented in the *Interagency Guidance on Third-Party Relationships: Risk Management*[6] on the understanding that their prudential bank regulator expects this of them. Other banks could come to a different conclusion about the expectation of their prudential bank regulator with respect to authorized third parties.

In practice, this ambiguity will mean that a consumer who has a deposit account at two banks may be able to access the consumer's information through an authorized third party from one bank, but not the other. This, in turn, will create a hardship for the consumer, *e.g.*, when applying for a loan from a lender, the consumer has authorized access to the consumer's data or when using a personal financial management tool. To prevent this potentially bad result from harming consumers, Mastercard encourages the CFPB to work closely with the prudential bank regulators to harmonize risk management requirements related to consumer-permissioned financial data sharing and to further clarify instances where security risk-related data access blocking is appropriate. In particular, the CFPB and the prudential bank regulators should consider issuing interagency guidance to clarify that the existing third-party risk management guidance issued by the prudential bank regulators does not apply as between a bank and an authorized third party and to provide clarity on the types of considerations banks and other market participants can use to evaluate when security risk-related data access blocking is appropriate.

## III. *Privacy Concerns and Permitted Usages of Data*

The ANPR states that a major privacy threat to consumers is when consumers are unaware of ongoing licensure or sale of their data. The PFDR Rule imposes a number of requirements intended to protect consumer data, including the requirement for third parties to obtain a consumer's express informed consent to access covered data on the consumer's behalf and a prohibition on any secondary collection, use of retention of data beyond what is "reasonably necessary" to provide the consumer's requested product or service. The ANPR seeks comments on the threats to data privacy as a result of unwitting licensing or sale of sensitive personal financial information and on any modifications to the PFDR Rule's provisions.

The PFDR Rule imposes new financial privacy regulations on the collection, use and retention of covered data where other laws and regulations already address such activities from a financial privacy perspective. Specifically, authorized third parties and data aggregators are already subject to the Gramm-Leach-Bliley Act and its implementing regulation, Regulation P, either as a result of providing financial products and services to consumers or acting as a service provider to a person that does. Regulation P imposes limitations on the disclosure of nonpublic personal information to nonaffiliated third parties by financial institutions and their service providers and limitations on the use and disclosure of nonpublic personal information by service

[6] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, *Interagency Guidance on Third-Party Relationships: Risk Management*, 88 *Fed. Reg.* 37,920 (June 9, 2023).

providers that receive nonpublic personal information under certain exceptions to the restrictions on disclosure. Further, Regulation P and the Federal Trade Commission's Safeguards Rule[7] already impose information security requirements on authorized third parties and data aggregators. In addition, a third party that is a consumer reporting agency already is subject to the Fair Credit Reporting Act and its restrictions on use of data.

However, instead of utilizing existing law and regulation, the PFDR Rule subjects authorized third parties and data aggregators to an additional layer of financial privacy regulations that do not apply to other types of financial services providers. This is despite the fact that the consumer financial information these parties collect is exactly the same information that they could collect directly from consumers and that consumers have willingly provided to financial services providers for many years in paper form by mail and in electronic form by fax, email and website upload. And while the PFDR Rule includes some exceptions for data usage, such as for fraud prevention, servicing, and improving the product or service requested by the consumer, the PFDR Rule's restrictive data use prohibitions will ultimately harm the very consumers they seek to protect due to less consumer choice and stifled financial services innovation.

Accordingly, we ask that, in this rulemaking process, the CFPB revise the PFDR Rule to rely on the existing laws and regulations that protect consumer financial data on collection, use and retention instead of enacting a new privacy regime just for data received via open banking data sharing. This is essential to maintaining a level playing field in the regulatory treatment of these activities irrespective of whether consumers give their financial data directly to a provider of financial services or authorize a provider of financial services to retrieve the consumer's financial information via open finance. Relying on the existing financial privacy protections that apply to the collection, use and retention of covered data would also provide legal certainty and maximize competition.

However, if the CFPB determines that it will retain restrictions on collection, use and retention in the PFDR Rule, despite that these restrictions operate to the detriment of consumers, Mastercard encourages the CFPB to amend the PFDR Rule in four key ways that will mitigate consumer harm: (a) exempt de-identified data from the definition of covered data; (b) allow model development and validation as a reasonably necessary use of covered data; (c) expand the existing exemption for uses of covered data to prevent fraud such that a reasonably necessary use of covered data is to enhance the safety and security of the open finance ecosystem; and (d) allow consumers the choice to opt-in to any use of their data for which they provide consent.

*A. De-identified Data*

The PFDR Rule does not, but should, carve-out de-identified data from the definition of covered data so that authorized third parties and data aggregators may use de-identified data without limitation. Not doing so works against consumer interests by inhibiting the improvement of fraud prevention services and stifling innovation overall by limiting the improvement of existing products and the development of new services. De-identified data is

[7] 16 C.F.R. Pt. 314.

used widely in the financial services industry for business purposes that benefit consumers, including to develop new or enhanced products and services, and to provide products and services that benefit from an understanding of consumer financial behavior without the need to identify any consumers. For example, such data can be used to mitigate insufficient funds risk in recurring payments or to develop financially inclusive credit decisioning models.

Regulation P excludes from its scope "[i]nformation that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses."[8] State privacy laws also exclude de-identified data from their scope. In order to address the risk of re-identification, state privacy laws have adopted an approach of requiring entities to (i) take reasonable measures to ensure that a person cannot associate the de-identified data with an individual, (ii) publicly commit to maintain and use the data only in de-identified form and not attempt to re-identify the data, and (iii) contractually obligate recipients of the de-identified data to abide by the same requirements. This aligns with long-standing guidance from the Federal Trade Commission and is an approach Mastercard would support in a revised PFDR Rule.

The lack of a carve-out for de-identified data in the PFDR Rule creates an inconsistency between the PFDR Rule and other settled laws governing consumer data use. We urge the CFPB to maintain consistency and provide legal certainty by expressly permitting the use of de-identified data when it reissues the PFDR Rule. Doing so would create a level playing field among financial services providers and entities providing products in other industries that are subject to privacy regulations.

*B. Model Development and Validation*

The CFPB should also clarify that a "reasonably necessary" use of covered data includes model validation and self-testing to minimize bias in models and analytics used to provide products and services. Models and analytics can be used by authorized third parties to expand credit opportunities to underbanked consumers. Use of covered data to develop and validate models is critical to continued growth and innovation in the open finance ecosystem industry. We do not believe that the models offered today would have been capable of being developed without the use of covered data. Additionally, the development of future models with which consumers can use their data and from which they benefit will be nearly impossible to provide under the PFDR Rule without clarification that "reasonably necessary" use of covered data does include the development and validation of models.

*C. Fraud*

The PFDR Rule contains an exemption from the covered data use limitation for uses that are reasonably necessary to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability. We support the continued inclusion in the PFDR Rule of

[8] 12 C.F.R. § 1016.3(q)(2)(ii)(B).

this exemption and urge the CFPB to ensure that it is broad enough to be technology neutral and encompass the use of covered data in future fraud models.

Examples of fraud prevention services include the use of data from a cross section of consumers' open finance activity from multiple financial institutions to indicate patterns of behavior that can demonstrate systemic issues in financial ecosystem security, *e.g.*, the security of, or threat vectors to, API channels. Permissioned identification information is used today for identity and account verification and for identifying and reporting suspicious activity as well as to address synthetic identity risk (*i.e.*, the risk that an identity is based on fabricated or synthetic credentials not associated with a real person). Accordingly, we urge the CFPB to make clear that a permitted use of covered data is to enhance the safety and security of the open finance ecosystem and that this use is "reasonably necessary" to provide the consumer's requested product or service.

### *D. Opt-In*

Finally, the CFPB should give consumers the right to allow their data to be used for any purposes for which they provide consent, so long as the uses have been fully and accurately disclosed to them. Such an explicit opt-in approach would be consistent with the policy underlying Section 1033 because it would give consumers ultimate control over their financial data and could be done through a transparent process.

This approach is also important to enable authorized third parties or data aggregators to innovate and provide additional consumer-benefitting services and tools that are broader in scope than those reasonably necessary to providing a requested product or service. For example, a data aggregator may have a tool available to consumers that would give consumers a consolidated view of linked accounts and account access by authorized third parties, so that consumers could control and manage access to their data in one centralized location. Consumers could use a tool like this to manage consents, account-linking, data share authorizations, and data sharing revocations.

## IV. *Roles in the Open Finance Ecosystem*

The PFDR Rule defines roles for participants in the open finance industry and attaches responsibilities and requirements to each role. Whether intentionally or otherwise, this approach creates the impression that a party may only perform a single role. However, in practice, parties perform the functions associated with multiple roles in the market today. For example, a financial institution may be both a data provider and an authorized third party or an intermediary can be a data aggregator or an authorized third party or even both at the same time.

One way in which the PFDR Rule's construction has an artificially limiting effect is the manner in which it largely restricts data aggregators to a service provider role as compared to other third parties that have a direct consumer relationship because of the product or service the consumer requested. However, the business model of some data aggregators encompasses more than the CFPB contemplated, and some data aggregators currently do, and in the future could, provide important value-added services to consumers in addition to authorized third parties. The lack of clarity in the PFDR Rule on when data aggregators may also be considered authorized

third parties when offering products and services directly to consumers creates complexity in the marketplace. These factors also limit the way banks and other third parties may view a data aggregator, with the result being that the industry may have a narrow view of roles different entities can play under the PFDR Rule. Additionally, banks and other third parties could seek contractual terms that arbitrarily limit the ability for market participants to provide products and services directly to consumers or limit the use of consumer data – even when authorized by a consumer.

We believe that the CFPB should permit maximum flexibility for participants to serve in various roles because the roles in the open finance ecosystem continue to evolve rapidly and because it will enhance the effectiveness of consumer disclosures. In doing so, the CFPB can develop a regulatory framework that allows the ecosystem to advance and innovate while ensuring consumers receive accurate and simplified disclosures. Toward this end, Mastercard requests that the CFPB expressly clarify that data aggregators may be authorized third parties so long as they comply with any obligations that apply to authorized third parties.

Mastercard also requests that the consumer-facing disclosure requirements under the PFDR Rule be simplified to reflect clearly (i) which parties have access to consumer data and (ii) for what purposes each of the parties has access. For example, the CFPB could state that, while third parties operating as data aggregators may perform the authorization procedures on behalf of third parties, they may also do so on behalf of the consumer when operating as an authorized third party—so long as the consumer-facing disclosures make this clear. In this regard, the CFPB could expressly allow for a combined authorization in which a consumer permits two third parties to access and use the consumer's information. This would allow companies to retrieve consumer data on a permissioned basis for fintechs and other financial institutions that provide services to consumers and to use the retrieved consumer data on a permissioned basis to provide value-added services to consumers.

## V. *Additional Areas of Concern*

### A. *One-Year Maximum Reauthorizations and Payments Use Cases*

The PFDR Rule sets the maximum duration of an authorization at one year after the consumer's most recent authorization and requires that a third party obtain a new authorization annually to continue to collect covered data beyond each one-year period. We recognize the importance of consumers periodically being made aware of where their data is being used and for what purposes. However, we encourage the CFPB to use the current rulemaking process to allow consumers to decide the duration of their authorizations and to exempt recurring payment use cases.

Consumers should decide what authorization duration is best for them. That may be one year for some products or services, but consumers may find that a longer authorization period is more convenient for other products or services. In addition, having any duration limit on an authorization is problematic for recurring payment use cases. In a recurring payment use case, a consumer, on an ongoing basis, authorizes payments to be made from the consumer's account (*e.g.*, recurring bill payments for mortgages or utility bills). In lieu of reauthorization for recurring payment use cases, we encourage the CFPB to consider alternative approaches to

remind consumers of the way their data is being used. For example, the CFPB could require an annual notice to be given by each authorized third-party using consumer data for payments data that describes the purpose for which such authorized party is accessing the covered data and enables the consumer to revoke the related authorization. Such an annual notice could be defined by qualified industry standards bodies to ensure consistency. This would provide the same transparency as the consumer would receive through a reauthorization but would be a more practical way to reduce the risk of consumer harm.

B. *Clarifying Covered Data*

Section 1033.211 of the PFDR Rule defines "covered data," which must be made available by data providers, using six broad categories with examples. We believe these categories cover most data from covered accounts used in the market today and we do not think these categories need expansion. However, we urge the CFPB to use the current rulemaking process to be more granular in its approach to defining the covered data in these categories to ensure that consumers can access the data needed today to receive the products and services they request. Specifically, the CFPB should clarify that "covered data" includes the following data elements: (1) an electronic copy of a consumer periodic statement; (2) elements that consumers needs for full use of their account data, including information that identifies whether an account is a personal or business account, last activity date, transfer limits, consent notification objects, persistent user identity and reward membership data; (3) elements to understand transaction data, including merchant identity for purchase transactions, address of payee for funds transfer transactions and phone number of payee for funds transfer transactions. Additionally, we encourage CFPB to provide clarity related to Terms & Conditions as there has been widespread confusion in the marketplace on this topic. Specifically, clarity is needed to understand if specific data elements from Terms & Conditions should be provided such as a consumer's credit limit, or whether a full machine-readable Term & Conditions document should be provided. All of this information is the consumer's data and should be available to the consumer directly and through developer interfaces so they can share their data with authorized third parties.

C. *Qualified Industry Standards*

Mastercard believes uniform technical standards that create interoperability, and which are defined and certified by industry standards bodies with balanced governance, are critical to a functioning open finance ecosystem. In fact, other open banking frameworks around the world have stumbled significantly by failing to provide clear regulatory direction on technical standards. This has resulted in fragmentation with different incompatible standards and implementation patterns, increased cost and complexity in the market and poor consumer experiences. In that regard, we believe that industry standard-setting bodies are best positioned to develop and maintain standards that meet the needs of the market and facilitate innovation. We encourage the CFPB to provide clarity and certainty about the role technical standards will play under a revised PFDR Rule.

Mastercard is supportive of API standards developed by the Financial Data Exchange ("FDX"). FDX maintains the market's most widely used technical standard in North America for user-permissioned financial data sharing integrations.

We encourage the CFPB to maintain the official recognition of FDX as an issuer of qualified industry standards and to maintain the recognition process for qualified industry standard setting bodies that is in the PFDR Rule. However, for qualified industry standards bodies to be utilized fully in relation to the PFDR Rule, Mastercard encourages the CFPB to make demonstrated conformance to qualified industry standards a safe harbor for compliance with the requirements in the PFDR Rule, instead of using conformance with qualified industry standards as indicia of compliance. A full safe harbor for compliance will provide certainty and clarity to the market and will maximize uniformity and the quality of the consumer experience.

If the CFPB determines not to maintain the current approach to recognizing qualified industry standards bodies, Mastercard encourages CFPB to require demonstrated conformance to a widely used standard issued by an industry-led standard setting body that meets the attributes of openness, balanced decision-making, consensus, due process and appeals, and transparency, and to provide a safe harbor for demonstrating conformance to such standards. While not ideal, such an approach will provide clear regulatory direction to the market.

* * *

Mastercard appreciates the opportunity to provide comments on the ANPR. If there are any questions regarding our comments, we would welcome a conversation with the CFPB. Please do not hesitate to contact us.

Sincerely,

Tom Carpenter
Senior Vice President
Global Open Finance Policy

cc: Tina Woo, Senior Managing Counsel, Regulatory, Mastercard