ANPR Response

Cover Letter

October 20, 2025

CONSUMER FINANCIAL PROTECTION BUREAU
[Docket No. CFPB-2025-0037]

To the Consumer Financial Protection Bureau:

On behalf of MX Technologies, Inc. (MX), we appreciate the opportunity to provide our feedback on the Consumer Financial Protection Bureau's (CFPB's) advanced notice of proposed rulemaking regarding its reconsideration of the Personal Financial Data Rights Rule (PFDR Rule). We believe this is a pivotal moment for the U.S. financial services industry, and that the preservation of the PFDR's key elements is necessary to foster a more competitive and consumer-centric ecosystem.

As a leading provider of financial data aggregation and connectivity services, MX has a deep understanding of the intricacies of the financial data ecosystem and the critical role that Open Banking plays in fostering a thriving economy where consumers can gain access to financial products and services that meet their needs.

MX's mission is to empower the world to be financially strong. MX believes that consumers must have the ability to access, direct, and control their financial data in order to make informed financial decisions that lead to financial strength.

The United States Government Accountability Office defines "financial literacy," as "the ability to make informed decisions to take effective actions regarding money",[1] and Secretary of the Treasury Scott Bessent notes that "[i]t is [his] firm belief that expanding financial literacy among our citizens will fundamentally shape future generations."[2]

As noted by President Trump, however, "our financial system can be complex and difficult for many Americans to navigate as they strive to make informed financial decisions." [3] This complexity is exemplified by the fact that the average consumer in the United States has at least five to seven financial accounts across financial institutions and fintechs.[4] Without access to, and a unified view of, their financial information, it is nearly impossible for consumers to make truly informed financial decisions.

[1] GAO-24-106381 Highlights, FINANCIAL LITERACY
[2] Remarks by Secretary of the Treasury Scott Bessent Before the Financial Literacy and Education Commission | U.S. Department of the Treasury
[3] Message on National Financial Capability Month
[4] How to Keep Consumers from Breaking Up with Banks | MX

Consumers need access to digital financial technology that will bring disparate financial information together and provide the tools and insights needed to effectively understand their finances and make informed financial decisions. President Trump noted that "as part of [his] recent effort to strengthen American leadership in digital financial technology, [the] Administration is supporting the responsible growth and use of digital assets, blockchain technology, and related technologies across all sectors of the economy."

Open Banking Supports American Innovation

MX supports the Trump Administration's mission to promote innovation in the financial sector and financial literacy among American consumers by developing products and services that provide participants of all sizes in the financial marketplace, including banks, credit unions, and fintech companies, with tools that they can use to help consumers access their financial data, better understand it, and identify actions to take to improve their financial well-being and financial literacy. As President Trump has recognized, "[r]esearch shows financial literacy leads to greater investments, higher retirement savings, and ultimately more household wealth."[5] In order to build the financial literacy that will lead to these meaningful outcomes, consumer financial information must be accessible to American consumers and the financial service providers they choose to provide their digital financial technology.

The financial technology (fintech) sector and the broader financial data ecosystem are not just important tools for consumer financial literacy – they are also vital engines of economic growth and innovation in the United States. The U.S. open banking market, already a significant force at $7.08 billion, is projected to grow to an impressive $35.79 billion by 2031.[6] This growth is not just a statistical trend. It reflects the deep integration of fintech into the lives of everyday Americans and businesses.

For decades, the financial services industry has been characterized by a complex, often fragmented, landscape with more than 8,000 financial institutions and more than 12,000 fintech companies. This complexity, while a strength in many ways, has also made it challenging to ensure seamless, secure data flow between all market participants. Too often, this prevents consumers and financial providers alike from truly understanding consumers' finances.

Reducing this complexity and providing all market participants with the ability to understand a consumer's true financial position – with the consumer's consent – presents an enormous opportunity to improve credit underwriting, increase access to financial

[5] Presidential Message on National Financial Literacy Month, 2025 – The White House

[6] United States Open Banking Market Assessment, Markets and Data, 2024

services for traditionally underserved communities, and improve consumers' ability to take control of their finances.

Open Banking is the key to unlocking this potential by enabling interoperable standards that allow for the secure and efficient sharing of financial data. This framework promotes innovation, increases competition, and ultimately empowers consumers. The success of this ecosystem hinges on a clear and consistent regulatory approach that champions the consumer as the owner of their own financial data.

Open Banking is also key to promoting healthy competition within the financial sector, benefiting both consumers and smaller institutions. Traditionally, large established banks have had a significant market advantage due to their vast resources and control over customer data. Banks' unwillingness to provide this data to their customers — or to third parties that consumers have permissioned to access their data — in a usable format stifles innovation, making it difficult for smaller companies and startups to enter the market with competing products and services.

This is particularly true for community banks and credit unions, which are often key economic pillars of local communities. With the right technology, these institutions can leverage Open Banking to compete with larger banks by offering innovative services and more personalized lending solutions. By enabling consumers to securely and efficiently share their permissioned data, Open Banking helps these institutions provide better services, such as streamlined loan application processes. The continued viability of community banks and credit unions is crucial for local economies, where they are often critical partners to the small businesses that serve as primary drivers of growth and employment in many small communities across the country.

Furthermore, the rise of fintechs has created an entire category of novel tools and services that were previously unimaginable. Many of these innovative, customer-friendly products are built on the premise of free access to financial data. For example, personal financial management apps like You Need A Budget (YNAB) and Rocket Money provide consumers with a holistic view of their finances by aggregating permissioned financial data from various accounts, allowing for better budgeting and financial planning. Similarly, applications like Splitwise simplify group expenses by enabling seamless tracking and settlement of shared costs. These services, and countless others, rely on the ability of consumers to efficiently provide their data in a usable format. Without a clear framework that enshrines consumers' right to data portability, the business models of these innovative fintechs would become unprofitable, effectively killing new ideas that benefit the consumer before they can gain a foothold in the market.

While some have argued that enabling consumers' access to their own financial data by requiring data providers to assume the cost of implementing and maintaining data access APIs is inappropriate and without data provider benefit, that argument is without merit as it rests on a faulty premise. In fact, data providers *do* benefit from Open Banking. Certain data providers have made data access APIs available to authorized third parties for years now, without imposing fees. These sophisticated financial institutions do not take on these types of investments without good reason, including, but not limited to:

- Reducing potential exposure or misuse of consumer login credentials and associated fraud costs by moving from screen scraping (i.e., accessing consumer-permissioned data by using the consumer's login and password) to token-based API access for authorized third parties;
- Gaining insight into which authorized third parties are accessing consumer-permissioned data through the API, which enables both enhanced security controls (e.g., the data provider has the ability to shut down access for any authorized third party at any time) and intelligence into areas where the data provider could improve its financial offering to preserve its consumer relationships (e.g., knowing that a consumer is applying for a mortgage refinancing through an authorized third party could enable the data provider to offer a competitive refinancing package to the consumer to preserve the business);
- Enhancing overall data protections and liability exposure by requiring the execution of bilateral agreements with authorized third parties as a pre-requisite to providing data access, which establishes clear access, security, and liability parameters; and
- Creating better experiences for its consumers (e.g., as stated by Sairam Rangachari, then Head of Open Banking, Treasury Services at J.P. Morgan, "For us, Open Banking is about how we take more of our experiences to our customers and how we partner with the market to create better experiences. Historically, companies and banks have tried to create active experiences and make customers come to them. We are looking at how we can also take our banking products to our customers, even if they are not on our website. I think APIs are going to create a faster, more efficient way of doing this.")[7]

Data Access Fees Undermine Consumer Rights

We strongly support the existing PFDR Rule's prohibition on fees for data access. The law requires data providers to provide consumers with their data "in an electronic form usable by consumers."[8] There is near universal agreement in the industry that APIs are the most

[7] The Open Banking Transformation, JP Morgan Treasury Services
[8] 12 U.S.C. § 5533(a)

secure and efficient means to satisfy this requirement, and the PFDR Rule appropriately mandated this means of ensuring compliance with the statutory mandate. Regulated institutions do not get to put conditions on compliance with the law based on consumers' willingness to pay a fee for such compliance. Suggesting that data providers can assess a fee to cover their costs of complying with Section 1033(a)'s mandate is, therefore, as absurd as suggesting that financial institutions can condition the delivery of required periodic disclosures on a consumer's payment of a fee.

As we state below in our answers, a fee for access fundamentally contradicts the nature of a right. A consumer's financial data belongs to the consumer, and financial institutions are merely the custodians of that information. Allowing financial institutions to charge fees would not only obstruct a consumer's right to their own data but also create an anti-competitive environment where large banks can use fees as a gatekeeping mechanism to stifle innovation and crush smaller players in the market. This would also have a cascading negative impact on established technology companies and the burgeoning cryptocurrency sector, both of which rely on seamless, low-cost bank account links to function.

We also commend the current rule's focus on transitioning the industry away from less secure practices like screen scraping toward more secure, standardized APIs. The Financial Data Exchange (FDX) has been instrumental in developing these standards, which are essential for ensuring a secure and interoperable ecosystem. By supporting the free flow of data through these secure channels, the government can protect consumer privacy, foster market innovation, and ensure the U.S. remains a global leader in financial services.

Recommended Modifications to the PFDR Rule

A. The Secondary Use of Data

We believe the sale of data rarely, if ever, benefits consumers and should continue to be prohibited in the rule. However, we also believe that the current language in the PFDR Rule is too restrictive regarding secondary uses of consumer data.

The rule limits the collection, use, and retention of covered data to what is "reasonably necessary" to provide the consumer's requested product or service, even where broader use may ultimately benefit the consumer without any sale of covered data. This interpretation is too narrow, explicitly prohibiting practices like targeted advertising and cross-selling, all of which could lead to more tailored and beneficial financial products being offered to consumers. These restrictions stifle innovation and limit the ability of financial institutions, fintech companies, and other third parties to develop new products and services based on consumer-permissioned data. If a consumer gives informed

consent, they should be able to authorize uses of their data that add value for the consumer.

These beneficial use cases can unlock a range of powerful benefits for consumers:

- **Fraud prevention and product improvements**: The use of broad, consented data sets is essential for developing more sophisticated machine learning models. By analyzing a consumer's entire financial footprint, banks can more effectively detect and prevent fraud, such as account takeovers or unusual spending patterns, in real-time. This protects the consumer from financial loss and also helps companies identify and stop new fraud tactics as they emerge. Similarly, data analysis helps companies improve the design and functionality of their financial products, making them more user-friendly and secure.
- **Better, more tailored offers**: Companies can use transaction data and spending patterns to create personalized credit card and loan offers, rewards programs, payroll deposit switching, and other financial management tools that are more relevant to a person's lifestyle. For example, a card issuer could use a consumer's spending data to offer a special promotion at a favorite grocery store or a higher cash-back percentage on travel if their data indicates frequent travel. This creates a more financially beneficial and seamless experience for the consumer.
- **Public interest uses**: Properly anonymized and aggregated consumer data can be a powerful tool for public good. For instance, anonymized and aggregated data can be used by researchers to analyze economic trends, inform public policy decisions, and improve access to the financial system by helping lenders build more complete credit profiles for consumers with thin credit histories. These applications benefit society as a whole while respecting individual privacy by ensuring the data is stripped of personally identifiable information.

To ensure both consumer protection and beneficial innovation, a more nuanced approach that empowers consumers to authorize — and maintain permissions for — additional data uses is needed, rather than imposing a sweeping ban that limits uses beneficial to both consumers and society.

B. Re-authorization Requirements

Similarly, we believe the current rule's re-authorization requirements are too cumbersome for consumers. The current rule requires third-party data recipients to obtain a new authorization from a consumer at least once every 12 months to continue collecting data. This creates an unnecessary and burdensome administrative hurdle to the detriment of consumers and service providers alike.

This annual re-authorization process could disrupt the continuous services provided by third parties, such as long-term financial planning, budgeting and tax tools, or fraud monitoring, which rely on a consistent flow of updated data. Such a strict requirement is counterproductive to the PFDR Rule's stated goal of fostering a more dynamic and consumer-friendly financial services market.

C. The Role of Standards

The U.S. financial data ecosystem is considerably larger and more complex than any other jurisdiction. The efficient and secure transmission of data between all these players is dependent on interoperable standards. The Financial Data Exchange (FDX) has been very successful in establishing consensus standards over the past seven years. With an MX executive serving as the co-chair of the board, and the MX team being active members of the organization, MX believes that FDX can expand further, with certification mechanisms that could provide safe harbors for market participants, educating the compliance load for the marketplace, and the administrative burden for regulatory bodies.

Standards are also essential in making this ecosystem function effectively. While this ANPR does not specifically address Standard Setting Organizations (SSOs), we believe that existing standards play a critical role in the success of the ecosystem. Standards serve to (1) ensure access to ongoing innovations as the industry expands into Open Finance, stablecoins, and other digital assets, (2) enable market participants of all sizes to enable secure access with less cost, and (3) bring clarity around conformance beyond indicia of compliance.

The U.S. government has a critical role to play in protecting this burgeoning ecosystem and ensuring its continued growth. This requires decisive action, but with a light touch, to establish clear rules of the road. The PFDR Rule takes a significant step in this direction by enshrining permissioned data sharing as a statutory right. MX believes that the proper promulgation of the PFDR Rule will be a critical step towards a more competitive and consumer-centric financial ecosystem in the United States. We strongly support the prohibition on data access fees and the transition to secure, standardized APIs, both of which are essential for fostering innovation, protecting consumers, and ensuring the continued growth of the U.S. Open Banking market.

We appreciate the opportunity to contribute our feedback and look forward to further collaboration.

Respectfully submitted,

Jane Barratt, Chief Advocacy Officer, MX
Maisie Bilotti, Senior Director, Advocacy, MX

Table of Contents

Questions & Answers

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

1. What is the plain meaning of the term "representative?" Does the PFDR Rule's interpretation of the phrase "representative acting on behalf of an individual" represent the best reading of the statutory language? Why or why not?

The plain meaning of "representative" is "one who stands for or acts on behalf of another."[9] Accordingly, to be a "representative" of a consumer, a person or entity need only be acting for that person pursuant to actual authority. This is consistent with the position of the Treasury Department during President Trump's first term, which observed that:

> "This definition is best interpreted to cover circumstances in which consumers affirmatively authorize, with adequate disclosure, third parties such as data aggregators and consumer fintech application providers to access their financial account and transaction data from financial services companies. Otherwise, narrowly interpreting Section 1033 as applying only to direct consumer access would do little to advance consumer interests by eliminating many of the benefits they derive from data aggregation and the innovations that flow through from fintech applications."[10]

In addition to the plain meaning of the term, the PFDR Rule's interpretation of the phrase "representative acting on behalf of an individual" represents the best reading of the statutory language for the following reasons:

- First, had Congress intended anything other than the plain meaning, it would have expressed that intent in the language itself. For example, the Fair Credit Reporting Act, which provides consumers with a right to request their file from consumer reporting agencies, defines "consumer" to mean a "natural person." 15 U.S.C. § 1602(i). By contrast, the Gramm Leach Bliley Act (GLBA), which allows consumers to consent to financial institutions' disclosure of their information to third parties, defines "consumer" to include both the individual and a "legal representative."[11] By defining "consumer" to include an "agent, trustee, or representative acting on behalf of an individual," Congress acted deliberately to adopt a broader definition than just an individual or their "legal representative."

[9] Black's Law Dictionary 1416 (9th ed. 2009).

[10] A Financial System That Creates Economic Opportunities - Nonbank Financials, Fintech, and Innovation.

[11] Gramm-Leach-Bliley Act (15 U.S. Code § 6809(9)).

- Second, to read "representative" more narrowly to include only one acting in a fiduciary duty would render the term superfluous and contradict the statutory structure.

- Third, while most consumers had access through online banking portals to the types of data covered by Section 1033 at the time of its passage, consumers did not have a clear right to obtain this data from covered persons in "an electronic form usable by consumers" or in a "standardized format . . . including through the use of machine readable files."[12] To effectuate this right, consumers must rely on third parties, acting on their behalf, who have the technology to turn the raw data into actionable information. Indeed, at the time of Section 1033's enactment, consumers already relied on authorized third parties to make sense of their financial data.[13] As the Treasury Department recognized during President Trump's first administration, Section 1033 is best read as Congress's directive to codify this market practice into a right, subject to regulation by the CFPB.

2. Are there other provisions in Federal statutes or financial services market practice in which third parties authorized to act on behalf of an individual encompass, on an equivalent basis, both those having fiduciary duties and those who do not?

Within the Dodd-Frank Act itself, the language used demonstrates the clear intent by Congress for a consumer to authorize third parties, fiduciaries and non-fiduciaries alike, on an equivalent basis, to act on the consumer's behalf. Had Congress intended for consumers to only authorize third parties having fiduciary duties to access data on their behalf, they could have used the term "legal representative", as used in several instances in the Dodd-Frank Act to refer to relationships involving fiduciary duties, including in defining a "retail customer" to include a "natural person, or the legal representative of such natural person" and in whistleblower representation provisions.[14] [15] Congress instead opted for the broader term "representative" in providing for a consumer's right to authorize a third party to access their financial data on the consumer's behalf.

The language in the Dodd-Frank Act can be compared to that used in other legislation to designate a party as having fiduciary duties, including the following:

- In the Federal Deposit Insurance Act, mortgage loans to persons "acting in a fiduciary capacity" are prohibited.[16]

---

[12] 12 U.S. Code § 5533(c).

[13] Intuit's New Version Of Quicken Gets Mintified With Financial Data Insights And More | TechCrunch.

[14] *See* https://www.congress.gov/111/plaws/publ203/PLAW-111publ203.pdf, pg. 367.

[15] *See* https://www.congress.gov/111/plaws/publ203/PLAW-111publ203.pdf, pg. 450.

[16] 12 U.S.C. § 1831b.

- The National Bank Act authorizes recovery of interest in excess of that allowed by a person "or his legal representatives".[17]
- Similarly, the Federal Credit Union Act permits the recovery of interest by a person "or his legal representatives".[18]
- Finally, in the Employee Retirement Income Security Act (ERISA), the term "fiduciary" is defined in a detailed, highly technical manner.[19]

Conversely, the use of the generic term "representative" in Section 1033 should not be interpreted as having the same meaning as the terminology used in the Dodd-Frank Act itself and in other federal statutes.

3. Does the statutory reference to an "agent, trustee, or representative" indicate that "representative" is intended to encompass only those representatives that are serving in a fiduciary capacity? If a "representative" under 12 U.S.C. 5481(4) is interpreted to be an individual or entity with fiduciary duties, what are the distinctions between an "agent" and a "representative" for purposes of section 1033?

No. A "trustee" generally has a fiduciary duty to the beneficiary of the trust, but an agent or representative does not typically have fiduciary duties. If fiduciary duties were applied to all these entities equally, there would be no distinction between these entities, and consequently, no reason to list them. Congress could have defined "consumer" as an "individual or one acting on behalf of that individual in a fiduciary capacity." It did not.

4. In seeking the best reading of the statutory language, what evidence or interpretive principles should the Bureau consider with respect to the term "representative?"

In seeking the best reading of the statutory language, the Bureau should consider the following evidence and interpretative principles:

- Evidence:
    - At the time of the passage of Section 1033, consumers already had broad legal rights to access the types of data covered by Section 1033 and common industry practice gave consumers online direct access to this data. There would be no need for Congress to duplicate consumer rights already granted or otherwise made available elsewhere if direct consumer access to this data was all that Congress intended.

[17] 12 U.S.C. § 86.
[18] 12 U.S.C. § 1757.
[19] 29 CFR § 2510.3-21.

- Section 1033 isn't merely limited to access; it calls for covered consumer financial information to "be made available in an electronic form usable by consumers."[20] Consumers would derive little value from direct access to an electronic form of this data. It is only when consumers can authorize their service providers to access this data directly (just as financial institutions can make that same data with their service providers under Regulation P) that the data becomes, in a practical sense, "usable by consumers." At the time of the passage of Section 1033, online personal financial management tools like Mint and Quicken had millions of users who authorized the providers of these tools to connect directly to over 12,000 banks and credit unions in the U.S.[21], making it clear that Congress was aware of how a consumer's "representative" could use electronic data provided in a standardized format to provide innovative consumer-permissioned services that benefit the consumer.

- Interpretive Principles:
  - The *Ordinary-Meaning Canon* requires that words "be understood in the ordinary, everyday meanings."[22] "Representative" means "one who stands for or acts on behalf of another."[23]
  - The *Surplusage Canon* requires that every word and every provision be given effect – "[n]one should needlessly be given an interpretation that causes it to duplicate another provision or to have no consequence."[24] If "representative" is interpreted to mean the same as trustee or agent, it would merely be a duplicate and have no consequence.
  - The *Whole Text Canon* requires that the text be considered as a whole.[25] The fact that (i) the Dodd-Frank Act uses the specific terms "legal representative" and "fiduciary" in other sections of the Act indicates that Congress did not intend fiduciary prerequisites to apply to the term "representative," and (ii) Section 1033 itself calls for covered information to be shared in "an electronic form usable by consumers" which should be represented in a "standardized format . . . including through the use of machine readable files,"[26] indicating that Congress intended for the data to be used by authorized third parties with the technology to "machine read" the data and make it useful for consumers.

[20] 12 U.S.C. § 5533(a).
[21] See supra note 12.
[22] 12 Canons of Statutory and Constitutional Text Construction.
[23] See supra note 8.
[24] 12 Canons of Statutory and Constitutional Text Construction.
[25] Id.
[26] 12 U.S.C. § 5533.

5. If a "representative" under 12 U.S.C. 5481(4) is interpreted to mean an individual or entity with fiduciary duties, to what extent would it limit customers' ability to transfer their transaction data to third parties under section 1033 or the ability of financial technology and other third-party service providers to compete with incumbent market participants?

Interpreting "representative" to mean only fiduciaries would have a material detrimental impact on consumer rights and the competitive landscape. As noted by President Trump's Treasury Department in 2020 when speaking to the proper interpretation of the term "representative:"

> "[N]arrowly interpreting Section 1033 as applying only to direct consumer access would do little to advance consumer interests by eliminating many of the benefits they derive from data aggregation and the innovations that flow through from fintech applications."[27]

Such a narrow interpretation of the term "representative" would effectively allow data providers to selectively permit access by third parties via API, which would impede those financial technology and other third-party service providers in their ability to compete with incumbent market participants. In this manner, data providers could choose "winners" and "losers" by providing or not providing API access. Consumers still wishing to use the services provided by those third parties disallowed by data providers would have to provide that data in one of two ways: (1) manually or (2) by permitting screen scraping. Providing the data manually would, in theory, require requesting or downloading the data from a myriad of data providers and then transmitting that data by email or by upload, potentially on a recurring basis depending on the specific service offered, to the desired service provider. It is unlikely that a consumer faced with this burdensome process would engage in updating their data in a way that makes the third-party service useful or engaging at all. Additionally, such a process would degrade the quality and dependability of the data and introduce unnecessary data security risks. Alternatively, the consumer could permit screen scraping, which is nearly universally viewed as a less secure, less desirable option than direct access via API.

At the same time, requiring a fiduciary relationship between "representatives" and consumers would offer little consumer benefit. The PFDR Rule was drafted to provide consumers with broad protections by requiring third parties accessing covered data on a consumer's behalf to assume responsibilities that approximate common law fiduciary duties in order to be considered "authorized," as illustrated in the following table:

[27] See supra note 9.

Fiduciary Duty	Common Law Responsibility	Corollary 1033 Responsibility
Duty of Loyalty	Avoid conflicts of interest and self-dealing.	Only access and use data as is reasonably required to provide the services requested, disclosed, and consented to by the consumer.
Duty of Care	Act with competence and diligence.	Commit to meet the third-party obligations detailed in Section 1033.421 and certify compliance prior to data collection (e.g., data use limitations, maximum duration of consent, reauthorization requirements, accuracy requirements, data protection, etc.)
Duty of Obedience	Follow lawful instructions.	Terminate data access and delete data (where applicable) at the consumer's request.
Duty of Disclosure	Share relevant information.	Disclose the name of third party / data aggregator, the name of the data provider, a description of the requested services, categories of data to be accessed, a compliance certification, a description of the duration of data collection, and a description of the revocation method.
Duty of Confidentiality	Protect sensitive information.	Must secure the data in accordance with GLBA safeguards requirements.
Duty to Account	Keep accurate records.	Keep accurate records of consents obtained, categories of data collected, reasons for collecting, names of parties, status of authorization, etc.

Limiting the definition of "representative" would hinder the consumer's ability to choose and work with their preferred financial technology or other third-party service provider, or potentially eliminate the consumer's choice altogether if those third parties cannot adequately compete without necessary access to data. In either case, the result is that the incumbent market participants' positions are strengthened. While the third-party responsibilities under the PFDR Rule provide significant protections and benefits to the consumer, imposing additional burdens on consumers or limiting consumers' choices in this way would have the net detrimental effect on consumers of limited choice and little, if any, accompanying additional consumer protections.

6. Does the requirement in section 1033 for the Bureau to prescribe standards promoting the development and use of standardized formats for information made available under section 1033 illuminate the types of entities that should be considered "consumers" or have any other implications for how "representative" under 12 U.S.C. 5481(4) should be interpreted?

Yes. See the second bullet point under "Evidence" in our response to Question 4 above.

7. If a "representative" under 12 U.S.C. 5481(4) is interpreted not to be required to have fiduciary duties, what elements are required in establishing that the individual is a "representative" acting on behalf of the consumer?

The requirements detailed in the PFDR Rule clearly outline what is required to be deemed an authorized "representative" acting on behalf of the consumer. These requirements ensure that third parties will only be deemed an authorized "representative" after they have obtained the individual consumer's "express informed consent."[28] Specifically, an authorized third party must clearly disclose to the consumer (1) who it is; (2) which data provider(s) it will seek information from on behalf of the consumer; (3) a description of the product or service it is providing and a statement that it will only collect, use, and retain data reasonably necessary to provide that product or service; (4) the specific categories of data that it will collect; (5) a certification that it will comply with all the obligations the PFDR Rule imposes on third parties related to data use, data security, accuracy, and revocation rights; (6) a description of the duration of the third party's collection of data; and (7) a description of how the individual consumer can, at any time, revoke the third party's access to data.[29]

Only after a third party has disclosed this information and obtained the individual consumer's affirmative consent will it be deemed an authorized "representative." Further, while third parties must demonstrate that they have received this authorization before data providers have an obligation to provide access to their customers' data, the rule also permits data providers to confirm with their customers independently that the third party is, in fact, an authorized "representative" of the customer and that the customer has directed the third party to obtain the data on his or her behalf.[30] Accordingly, under any ordinary understanding of the term, the PFDR Rule ensures that only authorized "representatives" of individual consumers can obtain direct access to consumers' data.[31]

---

[28] 12 CFR 1033.401(c).

[29] 12 CFR 1033.411(b).

[30] 12 CFR 1033.331.

[31] *See, e.g.,* Restatement of the Law (Agency) § 2.10 ("An agent acts with actual authority when, at the time of taking action that has legal consequences for the principal, the agent reasonably believes, in accordance with the principal's manifestations to the agent, that the principal wishes the agent so to act."); *id.* § 3.01 ("Actual authority, as defined in § 2.01, is created by a principal's manifestation to an agent that, as reasonably understood by the agent, expresses the principal's assent that the agent take action on the principal's behalf.").

8. Are there any legal precedents or other considerations relevant to the above questions based on the applicability of the same definition of "consumer" to other Dodd-Frank Act provisions?

Yes. The definition of "consumer" in 12 U.S.C. § 5481(4) applies throughout the Dodd-Frank Act, and in multiple provisions, Congress chose to use narrower terms like "legal representative" when it intended to confine access to fiduciaries. The deliberate use of the broader "representative" in Section 1033 should be given effect under the canon of consistent usage, meaning it encompasses any authorized third party acting on behalf of a consumer. Limiting the term to fiduciaries would not only contradict this broader statutory definition but also create inconsistencies across the Act, as Congress clearly knew how to impose fiduciary limits and did so elsewhere. Courts have long cautioned that where Congress varies its wording across provisions, the difference must be presumed intentional. That principle, combined with the overall purposes of Dodd-Frank to promote competition, transparency, and consumer control, reinforces that "representative" under Section 1033 must be read broadly, not narrowly.

While we are not aware of specific legal precedent interpreting the definition of "consumer" in 12 U.S.C. § 5481, it is important to note that the CFPB has, throughout its entire history, interpreted the term "consumer" to include an authorized third party for purposes of the "consumer's" right to submit a complaint to the CFPB under 12 U.S.C. § 5534(a).[32] Of course, it has also consistently interpreted the term to include authorized representatives in relation to the exercise of consumers' rights under Section 1033, 12 U.S.C. § 5533.[33] The CFPB's consistent interpretation of the term "consumer" to include any authorized "representative" and not merely an individual in a fiduciary relationship is excellent evidence of the law's actual meaning.[34]

[32] See, e.g., CFPB, Consumer Response Annual Report for 2020, at [ ] (available at https://files.consumerfinance.gov/f/documents/cfpb_2020-consumer-response-annual-report_03-2021.pdf) (stating that "[t]he Bureau accepts complaints from authorized third parties" and citing the definition of "consumer" codified at 12 U.S.C. § 5481(4)); CFPB, Government Portal Section 1013(b)(3) Agency Confidentiality and Data Security Agreement (available at https://portal.consumerfinance.gov/government/resource/1674051907000/MosGovernmentPortalAgreement), § 1.3 (defining "Authorized third party representative" as "a Person who possesses Third Party Authorization."), id. § 1.15 (defining "Third Party Authorization" as "a signed, written document or oral statement made by a consumer granting a representative or agent the authority to submit a complaint on the consumer's behalf and, if applicable, perform specified actions related to such complaint.").

[33] See CFPB Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (Oct. 18, 2017) (available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf).

[34] See Loper Bright Enters. v. Raimondo, 603 U.S. 369, 386, ("[T]he longstanding 'practice of the government—like any other interpretive aid—can inform a court's determination of what the law is.").

B. Defrayment of Costs in Exercising Rights Under Section 1033

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

Yes, we believe that the current text of the PFDR Rule regarding the prohibition of fees is the best reading of the Dodd-Frank Act. Fundamentally, a fee for access to data directly contradicts the rights guaranteed by Section 1033. The intent of the statute is to provide consumers with a set of rights around the movement and transfer of their financial data. It follows that the statute intends to clarify that data belongs to the consumer. Banks, and indeed all entities in possession of a consumer's data at any given time, are simply the custodians of that information. Charging a fee to access it is, therefore, a tax on a consumer's right to their own data and their ability to share it with the services of their choice.

The primary objective of the CFPB, as established at its inception, is to "seek to implement and, where applicable, enforce Federal consumer financial law consistently for the purpose of ensuring that markets for consumer financial products and services are fair, transparent, and competitive."[35] A prohibition on fees is a direct and necessary step to prevent incumbent institutions from using fees as a gatekeeping mechanism to stifle competition and innovation.

Large, established banks could, if so inclined, use these fees as a weapon to maintain their market dominance and prevent smaller financial institutions and fintech startups from competing on a level playing field. Large banks do not have to pay these fees when they use consumers' data for their own in-house products, giving them a significant cost advantage. This makes it difficult for a smaller company to offer a competing product at a comparable price. The uncertainty and potential high cost of data access can discourage startups from even attempting to enter the market. The business models of many innovative fintechs are built on the premise of free data access. Fees can make these models unprofitable, effectively killing new ideas before they have a chance to take hold.

For smaller financial institutions like community banks and credit unions, charging for data access may seem like a promising new revenue stream. However, a closer look at the financial data ecosystem reveals that this strategy could lead to a net loss. Smaller institutions have a limited customer base. If they implement API fees, the cost for data aggregators to connect and maintain those API connections may outweigh the potential value, leading aggregators to prioritize larger institutions. Many of these smaller institutions are now adopting a "data-in" approach, using external data to offer tools and insights to their customers. In this scenario, the cost of data access fees will likely be

[35] 12 U.S.C. § 5511(a)

passed on to them by their data aggregators. This would increase the cost of aggregation services, ultimately costing the smaller institutions more than they could ever earn from their own data access fees.

This could accelerate an already concerning trend in the banking sector, where the number of FDIC-insured banks has dropped from over 8,000 in the year 2000 to just under 4,000 today[36], as smaller institutions are purchased and consolidated into the larger financial institutions. Indeed, in our own consumer research, we have seen a drop in the number of connected accounts per consumer, as institutional consolidation accelerates and barriers to entry proliferate across the financial data ecosystem in the United States.[37]

While banks argue that they should be compensated for the cost of maintaining secure data systems to protect their customers' data, we contend that this is a fundamental obligation of a financial institution. Consumers do not pay an extra fee to access their data at an ATM, to use a bank's online portal or mobile app, or to get account information from customer service. Charging a third party that is acting as a permissioned representative of the consumer for the same data is therefore not about covering costs, but about erecting a new barrier to entry to protect market share.

Data access fees would not only affect small fintech startups but also have a cascading negative impact on established technology companies and the burgeoning cryptocurrency sector, which are deeply integrated with the traditional financial system. Many widely used tech services rely on data aggregation to function. For example, accounting software like QuickBooks and financial dashboards for small businesses rely on a continuous feed of data to pay employees and suppliers, secure credit and automate reconciliation and tax preparation. New fees for every "API call" would increase the cost of these services, which would likely be passed on to the small businesses that depend on them. The entire crypto ecosystem, from exchanges like Coinbase and Kraken to DeFi applications, relies on seamless, low-cost bank account links for on-ramping and off-ramping fiat currency. If every deposit or withdrawal incurs a fee from a bank, it would make these transactions more expensive and less appealing to consumers, thereby impeding the growth of the digital asset economy and undermining the U.S. as a "safe harbor" for crypto innovation. In a similar vein, one could easily imagine a situation in which a large bank could use data access fees to favor one fintech in which it has a vested interest over another unrelated fintech by charging one company more than another, effectively putting the bank in the position of choosing a market winner.

[36] FDIC Annual Historical Bank Data
[37] Cheat Codes to Win and Retain Customers | MX

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

Yes. As stated in the answer to Question 9, the PFDR Rule was correct to conclude that permitting fees would obstruct the data access right. The Dodd-Frank Act grants consumers a right to their financial data, and a right is something one is entitled to without payment.

A fee for data access fundamentally changes a statutory right into a paid service. This contradicts the intent of the law, which is to establish that the data belongs to the consumer, and financial institutions are merely custodians. By charging a fee, a bank would be taxing a consumer's ability to exercise their right and share their own data with services of their choosing, which directly obstructs the very purpose of the data access provision.

11. What is a reasonable range of estimates regarding the fixed costs to "covered persons" of putting in place the standards required by sub-section D of section 1033 and the operational architecture to intake, document, and process requests made by consumers, including natural persons and persons acting on behalf of a natural person (i.e., an agent, trustee, or representative)? How do these estimates vary by the size of the covered financial institution?

Costs for implementing the new standards under Section 1033(d) will vary significantly among institutions. Larger institutions may face fewer burdens since many already have the necessary infrastructure – and in fact already implemented APIs and allowed consumer permissioned third party access, in some cases for years – while smaller institutions will likely incur substantial costs to establish new operational processes and rely on third-party providers. Implementing open banking APIs presents a vastly different cost structure depending on whether a financial institution chooses an in-house development approach or leverages a third-party provider. Developing and maintaining APIs in-house requires significant investment in specialized personnel, infrastructure, security, and ongoing compliance updates, which can be prohibitive for many institutions, especially smaller ones. Conversely, relying on third-party providers, particularly core providers who offer "plug-and-play" compliant APIs at scale, dramatically reduces these costs. If these core providers universally offered such solutions holistically, and at a reasonable cost, the overall expense of implementing open banking APIs across the entire financial ecosystem would decrease substantially, fostering broader adoption and competition.

The burden on smaller institutions is disproportionately high and is worsened by additional restrictions, such as limits on secondary data use and reauthorization

requirements. These provisions add complexity, increase costs, and give an unfair competitive advantage to larger banks, potentially stifling innovation and consumer choice. The wider economic impact of this competitive disadvantage is significant. If main street community banks and credit unions cannot compete long term in the digital economy, the U.S. will see accelerated consolidation and flight of assets to larger institutions; with a reduction of lending capacity for local small businesses.

13. How is the range above affected by the need of the "covered person" to confirm that an agent, trustee, or representative acting on behalf of an individual has actually been authorized by the consumer to act on their behalf?

The process of verifying that a representative has been properly authorized to access a consumer's financial data does not increase the marginal cost per request. This is because the standards established by a CFPB-approved Standard Setting Organization (SSO), like the Financial Data Exchange (FDX), provide the necessary tools to streamline this crucial step.

The core of this efficiency lies in the token origination process. Instead of a financial institution needing to manually verify each request, the SSO's standards allow for a digital, automated validation. By integrating this validation at the point of token origination, the process becomes highly efficient and scalable. This means that whether a financial institution is handling one request or a million, the marginal cost per request remains low and is not affected by the authorization verification. The process is designed to be seamless, secure, and automated, ensuring that the burden on financial institutions is minimal.

14. Is there any legal precedent from other Federal statutes, not involving Federal criminal law or provision of services by the U.S. Government, where there is a similar omission of explicit authorization to the agency to set a cost sharing balance in effectuation of a new statutory right and, if so, what principles has the court allowed the agency to use in establishing a proper balance?

The absence of explicit authorization for fee-setting in Section 1033 demonstrates that Congress did not intend for consumers to be charged for data access. When Congress wants an agency to set or recover costs, as seen in other financial regulatory laws, it provides clear statutory authority. The lack of such language here signifies that data access is a statutory right, not a paid service, and that Congress intended for costs associated with data access to be paid for, like any other cost associated with offering or providing the product, in a manner compliant with the law. Consumers already fund financial institutions through existing account and service fees, and imposing an additional charge would convert a regulatory obligation of data providers into a paid

service that they could choose to provide only to those consumers willing to pay for their own data. This would not only obstruct the law's pro-consumer intent but also stifle competition.

15. Absent any legal precedent from other laws, should covered persons be able to recover a reasonable rate for offsetting the cost of enabling consumers to exercise their rights under section 1033? Why or why not?

Charging a fee directly contradicts the very concept of a right. A right, by its nature, should be free to exercise. Imposing a cost converts a statutory right into a paid privilege, which directly undermines the consumer-empowering and pro-competition goals of Section 1033. While banks could incorporate the overhead costs of providing API services into their general account fees, just as they do with all other business expenses, charging a direct fee for each instance of a data request would transform a statutory right into a paid privilege. This direct charge is contrary to the intent of the rule, as a right, by its nature, is something one can exercise freely, without a direct transaction cost. Such fees would undermine the pro-competition and consumer-empowering goals of the regulation, creating a significant barrier to accessing one's own financial data.

If fees of any kind are to be considered, permitting a "reasonable rate" for cost recovery is a fundamentally flawed approach that would lead to prolonged litigation and market uncertainty. The terms "reasonable" and "cost" are highly subjective and lack a clear, objective definition in this context. Financial institutions argue that their costs for facilitating data access include the entirety of their IT and cybersecurity infrastructure. For example, some banks have stated that every API call or data transfer incurs a portion of their multi-billion dollar technology and security budgets, which they claim is a "cost" of Open Banking. This broad definition could allow them to justify exorbitant fees that serve to obstruct third-party services.

Without a clear standard, what is "reasonable" to a large bank may be an insurmountable fee for a small fintech startup. This creates a regulatory environment that is impossible to enforce consistently and would inevitably lead to endless legal challenges over what constitutes a fair price, effectively crippling innovation for years.

16. If covered persons should be able to recover a reasonable rate for offsetting the costs of enabling consumers to exercise their rights under section 1033, should the Bureau place a cap on the upper bounds of such rates that can be charged? If so, what should the cap be on such rates, and why? If not, why not?

If data access fees are permitted — and we maintain they should not be based on statutory language — a strict regime should be put in place allowing only for capped cost

recovery of technical API operations that are applied with absolute uniformity to all authorized third parties. This framework would allow financial institutions to charge only for the direct, marginal costs of processing a data access request through a secure API, while excluding all fixed costs associated with their broader technology and security infrastructure. Ensuring that fees are assessed, applied, and invoiced in a uniform manner prevents banks from using fees as a gatekeeping mechanism (e.g., a means to both exclude disfavored parties and to prop up parties that are favored due to some type of strategic relationship with the data provider).

Additionally, if fees are allowed, a strong transparency regime is essential. Institutions should be required to disclose these fees to their customers and regularly report their fee structures and transaction volumes to the CFPB for publication. This public reporting would allow the general public and competitors to monitor and compare fees, ensuring that rates remain competitive and providing consumers with a clear understanding of what they are being charged for access to their own data. This system of public scrutiny would serve as a crucial check against anti-competitive pricing.

17. If consumers ought to bear some of the cost in implementing requirements under Section 1033, should that be shared by every consumer of a covered person, including those who may not wish to exercise their rights under Section 1033?

Consumers should not be charged a fee for data access because they are already paying for their financial institutions' operational and technological costs, including the costs associated with regulatory compliance, through existing account fees, service charges, and interest payments. These revenue streams, which are paid by all customers, already cover the infrastructure needed to provide financial services in compliance with applicable law.

Open Banking is a channel, similar to branches, call centers, online banking, or mobile apps. The operation costs for branches, call centers, online portals, and mobile apps are built into existing fees. Why would this new channel be different? As the industry and technology evolves, costs will continue to grow, especially with the rise of agentic AI and the potential for on device access. This may change not just the cost implication, but also security parameters, privacy frameworks, consent language, and liability requirements.

C. Information Security Concerns in the Exercise of Section 1033 Rights

18. Does the PFDR Rule provide adequate protections for the security of consumer data? Why or why not?

Yes, the PFDR's incorporation of the requirements of Section 501 of the Gramm-Leach-Bliley Act (GLBA) (for entities subject to that act) or the FTC Standards for Safeguarding Customer Information 16 CFR pt. 314 (for entities not already subject to GLBA) provides adequate security requirements for the parties involved. The FTC Safeguards Rule, which implements Section 501 of the GLBA for most nonbank financial institutions, is specifically designed to "protect the security and confidentiality of [individual consumers'] nonpublic personal information."[38] Incorporation of this data security standard, therefore, ensures that any data provider or authorized third party (whether bank or nonbank) will be required to meet the same data security obligations that they would have to meet if they had obtained the data directly from the individual consumer, as opposed to from the data provider with the consumer's express authorization. Further, incorporation of the GLBA/Safeguards Rule standard ensures that Section 1033's data security standards will evolve along with evolving data security standards that apply generally to customer's financial information.

In addition to these requirements, the PFDR Rule contains numerous features that will promote data security for consumer's financial information, relative to a world without the PFDR Rule.

The rule seeks to enhance data security and consumer control by mandating a transition away from screen scraping. Screen scraping, which often requires consumers to share their private account credentials, poses risks such as data over-collection, potential security breaches, and a strain on data providers' systems. To mitigate these risks, the rule would compel data providers to establish and maintain more secure developer interfaces, which do not rely on consumer credentials. This shift toward modern, secure data-sharing methods has broad support among industry stakeholders.

A cornerstone of the new framework is the requirement for a consistent data security program, leveraging the GLBA Safeguards Framework. Both data providers and authorized third parties would be required to implement a security program that meets this framework's standards. This ensures that consumer data is protected throughout its lifecycle. For instance, data providers must apply an information security program to their

[38] 15 U.S.C. § 6801(a); *see also* 12 CFR 314.1 ("This part, which implements sections 501 and 505(b)(2) of the Gramm–Leach–Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.").

developer interfaces, and third parties must certify to consumers that their own systems for collecting and retaining data also meet the GLBA Safeguards. Furthermore, to manage risks, data providers would be allowed to deny a third party access to their interface if there are specific, known security concerns, such as a failure to maintain adequate security practices.

To safeguard consumer privacy, the rule also places limitations on how third parties can collect, use, and retain data. The framework is designed to give consumers full control, with requirements for clear authorization and an easy-to-use revocation process. The rule also includes other security measures, such as the use of tokenized account numbers, which can help mitigate fraud by allowing providers to revoke payment credentials on a targeted basis if compromised.

20. How do the fixed costs above relate to the number of clients serviced by the covered person or a person acting on behalf of an individual consumer? Is the market providing reasonably priced solutions to meet the provisions of the PFDR Rule for covered persons with few customers?

The price would not scale directly with the number of consumers serviced. The establishment of a security program to meet the requirements in the PFDR Rule could involve initial investment depending on the maturity of a financial institution's existing security infrastructure, and would involve relatively smaller, incremental expenses on the number of consumers.

21. In what way does the existence or non-existence of a fiduciary relationship affect the incentives in doing cost-benefit analysis regarding the level of information security established?

The existence of a fiduciary relationship should not impact the incentive to create and maintain a robust information security program. Information security programs are established to meet regulatory, contractual, and business requirements. These factors should ensure adequate investment in information security regardless of fiduciary status.

23. In the case of large-scale data breaches, what is the general cost per client in protecting such clients from the risks created by the breach, and how well-cushioned must working capital reserves be to respond to such breaches?

According to IBM's "Cost of a Data Breach Report 2025", the cost per compromised customer record is $160. This figure represents a global average across industries.[39]

[39] IBM Cost of a Data Breach Report 2025

Significant, well-documented breaches have affected large traditional financial institutions over the last decade. MX, by contrast, has not had a breach of our systems that has compromised customer data in its history of operations. In fact, we are not aware of any publicly disclosed data breaches at any of the top four data aggregators (Plaid, MX, Finicity, and Yodlee) that financial institutions claim are such a security risk with which to share customer data.

Any argument that large banks make about the need for data access fees to build up capital reserves to cover the cost of breaches caused by data aggregators is, to date, specious. Banks already maintain capital reserves in addition to specific insurance policies for data breaches to ensure coverage in the event of a data breach within their own walls. Of course, this could change in the future, and the modified rule could do a better job of addressing industry's calls for a clear liability framework for lost, stolen, or misused data. In principle, we believe that liability and associated costs should "follow the data" (i.e., fall on the party in possession of the data at the time of breach). Additional clarity in Rule 1033 around liability could reduce insurance and legal costs in the event of data breach in all locations in the financial data ecosystem.

24. What has been the experience of covered persons with secure storage and transmission of consumer financial data and how effective have such institutions been in establishing controls and information security protocols?

Generally, within the broader financial ecosystem, MX has experienced a high level of scrutiny and expected diligence for data protection and information security programs. Data providers, clients, and partners typically expect strong controls to be in place to protect consumer financial data in transit and at rest.

Consistent with the preamble to the PFDR Rule and with widespread industry consensus, secure transmission of consumer data between data providers and authorized third parties via API is the optimal means of transmitting consumer data from a data security, cost, accuracy, and efficiency standpoint. In this respect, we are concerned that an inappropriately narrow interpretation of the "consumer" that effectively prohibits this direct transmission or the imposition of fees for access to APIs by data providers may promote less secure means of data transmission, including screen scraping or transmission of data by individual customers via email or downloading of information.

26. What are the costs and benefits of the PFDR Rule's reliance on existing information security standards in the GLBA?

GLBA security standards have been a fixture in the financial sector for many years and, generally, have been a benefit to the broader industry to improve the information security

posture of organizations. GLBA has provided a baseline standard for financial institutions to meet, and regulatory enforcement has ensured consistent application across the industry. We believe that the rule should allow data providers to rely on third-party audits validating compliance with the Safeguards Rule.

27. To what information security standards ought entities adhere when accessing consumer financial data held by a covered person, and who is best positioned to evaluate whether these entities are adhering to such standards?

Entities that access consumer financial data should use industry standard security frameworks that are relevant for their organization. The industry should settle on security standards, certifications, or attestation report options that an organization may meet to allow for a more scalable ecosystem. Available options could include SOC 2 Type 2 report, ISO 27001, PCI DSS, or NIST CSF. These security frameworks are already well known and adopted throughout the industry, and allow for a baseline standard to be applied throughout the ecosystem. These industry-led efforts, alongside the security mandates in Rule 1033, successfully build the protective scaffolding of security infrastructure that consumers deserve in this space.

Accredited auditors, overseen by the respective industry frameworks, are best positioned to evaluate compliance against the PFDR Rule's standards. Instead of filtering security approval through government agencies with limited resources, leveraging independent assessors provides for faster and easier access for entities of all sizes to achieve compliance. Data providers and aggregators' reasonable reliance on an auditor's certification of compliance with such standards should entitle these entities to a safe harbor from any liability for actions taken in compliance with the rule. This is also an area where a standard-setting body, like FDX, could play a facilitating or certifying role.

28. What are the costs and benefits of the PFDR Rule's provisions designed to reduce the use of screen scraping? What changes would better protect the security of consumer credentials?

Enforcing the currently-written PFDR Rule to ensure data providers make consumer data available through APIs will result in a safer, more secure environment by reducing the prevalence of screen scraping. APIs provide many benefits, including more reliable connections, greater auditability, and the ability to use standardized formats such as specified by FDX. Screen scraping exposes consumers to additional risk and opens up more opportunities for fraud.

MX believes the introduction of data access fees will result in an increase in screen scraping as entities attempt to avoid paying associated fees. The PFDR Rule's provisions

around no fees must be maintained in order to ensure greater access to data within the industry.

29. Does the PFDR Rule provide adequate protections for consumers and covered persons to ensure that the request for a consumer's information is in fact knowingly authorized by the individual consumer and that the information is in fact being made available to the consumer as opposed to a malicious actor?

Yes, the PFDR Rule provides a multi-layered framework of protections designed to ensure that a request for a consumer's information is knowingly authorized and that the data is made available to the correct parties, not malicious actors. These protections involve a combination of consumer-facing authorization procedures and provider-side security and authentication measures.

The PFDR Rule establishes a framework for ensuring consumer data authorization and preventing access by malicious actors. It requires third parties to obtain a consumer's express, informed consent through a clear, separate authorization disclosure that details who is requesting data, what data will be accessed, and how to revoke permission.

To prevent malicious access, the rule mandates a multi-step authentication process where data providers verify both the consumer's and the third party's identities without the consumer having to share their credentials with the third party. A key protection is the prohibition of screen scraping, which eliminates a major security risk. Furthermore, data providers are empowered to deny access to third parties that fail to demonstrate adequate data security practices or proper identification.

Overall, the PFDR Rule aims to empower consumers with control over their data while simultaneously fortifying the entire ecosystem against security risks and unauthorized access.

D. Privacy Concerns in the Exercise of Section 1033 Rights

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

Yes, the PFDR Rule, as finalized by the CFPB, provides a framework that significantly enhances consumer privacy protections, focusing on notice, choice, and security. It represents a major step toward a more secure and consumer-centric financial ecosystem by moving away from less transparent data-sharing practices. In the absence of a federal privacy law, the rule achieves this through several key provisions that give consumers a better understanding of the data that is being shared and more control over its collection, use, and retention by those who receive it.

The PFDR Rule's most crucial privacy protection is its requirement for express, informed, and standardized consent from consumers. This means that a third party, like a fintech app, cannot access a consumer's financial data without providing a clear and conspicuous disclosure. This disclosure must explain exactly what data is being collected, why it's needed, and for what purpose it will be used.

The rule also imposes restrictions on how third parties can use the data they collect. A central tenet is the prohibition on selling consumer data, which prevents the information from being used for purposes outside the consumer's explicit consent. At MX, we believe privacy is about empowering consumers with full control over and clear visibility of what is happening to their data. The PFDR Rule aligns with this philosophy by making consumers the central point of authority. It provides a framework that allows individuals to access, understand, and direct their own financial data. This not only protects privacy but also fosters a more dynamic and secure financial ecosystem where consumers have the power to make informed decisions about who they share their data with.

The rule's benefits extend beyond consumer notice, consent, and security. It is designed to empower consumers and foster a competitive market in three critical ways:

- **Data Portability:** The PFDR Rule is fundamentally about data portability. It ensures that consumers can seamlessly move their financial data from one provider to another. This is a game-changer because it makes it easier to switch financial institutions or try new fintech products. This ease of movement encourages competition, forcing traditional banks and new fintechs to innovate and offer better services to attract and retain customers.
- **The Right to Revoke:** A non-negotiable component of true data control is the ability to revoke access at any time. The rule mandates that third parties must provide an easy-to-use mechanism for consumers to turn off data sharing. Furthermore, once consent is revoked, the third party is required to stop collecting new data and, in most cases, delete the data it has already collected. This puts the consumer in the driver's seat, ensuring their privacy rights are not a one-time decision, but an ongoing control mechanism.
- **Fostering Competition:** The PFDR Rule is a rare and powerful example of a regulation that successfully champions both consumer privacy and industry competition. Typically, privacy regulations can be a double-edged sword: while they protect consumers, they can also inadvertently create "walled gardens" by limiting data portability. This can entrench dominant players who already have a wealth of consumer data, making it difficult for smaller companies and startups to compete. In contrast, the PFDR Rule directly addresses this by making data

portability the central mechanism of its privacy framework. Instead of simply restricting data, the rule requires financial institutions to provide consumers with direct, secure access to their financial data via standardized APIs. This empowers consumers to take their data to new providers, whether it's a competitor bank or an innovative fintech. By doing so, it simultaneously enhances privacy — because the consumer is in control of their data and its use — and fosters a more dynamic, competitive market where new entrants can build better products and services, ultimately giving consumers more choice.

By moving from a less transparent system to one built on informed consent, data control, and standardized access, the rule empowers consumers, drives competition, and sets a new, higher standard for data protection in the financial services industry.

31. How prevalent is the licensure or sale of consumer financial data by bank and non-bank financial institutions, where customers either have the right to opt into or opt out of having their data licensed or sold? What is the approximate balance between such regimes where the customer is given a choice?

At MX, the security and privacy of our clients and consumers comes first. MX has never, and will never, sell consumer data to third parties. We believe that consumer-permissioned data sharing is foundational to a healthy financial data ecosystem that is based on value creation for the consumer, rather than value extraction by others without consumer authorization.

The prevalence and nature of data licensing and sale by financial institutions has been historically characterized by an inadequate balance of consumer choice. The balance between opt-in and opt-out regimes has been skewed. While a true opt-in model — where a consumer must explicitly agree to data sharing — is widely considered the gold standard for privacy and trust, it is not the historical norm in the U.S. financial sector. The GLBA's opt-out model applicable to most types of nonpublic consumer data is less protective, as it relies on the hope that consumers will navigate a complex process to revoke a pre-assumed consent.

The current PFDR Rule represents a fundamental shift. It is a direct response to the limitations of the existing framework and provides a crucial solution from a perspective that champions consumer control. The rule conditions data providers' disclosure of consumer data to instances in which the individual consumer has provided informed consent, which provides more control for consumers than provided under existing GLBA opt-out regimes. This moves the industry toward a true opt-in framework for data sharing.

From MX's perspective, this is not just a regulatory change but a philosophical one. The ultimate goal of privacy is not to prevent data from being shared, but to give consumers

the power to decide what is shared, with whom, and for what purpose. By mandating standardized, informed consent, and by placing strict conditions on the continued collection, use, and retention of data, the PFDR Rule empowers consumers to be in control of their digital financial lives. While there is opportunity to provide additional clarity and direction on secondary use cases that create benefit for the consumer, this is a significant improvement over previous regimes where the customer's "choice" was often an obscure link in a lengthy privacy policy.

E. Compliance Dates

35. Have entities encountered unexpected difficulties or costs in implementing the PFDR Rule to date?

Implementing the PFDR Rule has indeed presented entities with unexpected difficulties and costs. Key challenges include regulatory uncertainty and the absence of ready-made solutions from core providers at the time of the final rule, which necessitated custom approaches. There is a significant slow down and lack of participation due to uncertainty regarding the ultimate content of the PFDR Rule. It has also created space for significant misinformation, much of it spread by larger institutions, which has led small and mid-sized players to misunderstand the opportunities that Open Banking could provide in enabling them to deliver services to consumers and small businesses on par with large institutions.

36. If the Bureau were to make substantial revisions to the PFDR Rule, how long would entities need to comply with a revised rule? How would the necessary implementation time vary based on the size of the entity covered by the rule?

The staggered deadline for smaller institutions is unnecessary and potentially damaging to small and mid-sized institutions. These organizations rely on their core providers to deliver solutions. However, these core providers are not required to provide compliance solutions under the current rule. These core providers are certainly capable of delivering compliance with Rule 1033 at scale, but they are more likely to deprioritize smaller institutions if given the opportunity, reinforcing an existing competitive disadvantage. As a result, the largest institutions continue to widen the gap as compliance deadlines are delayed and further staggered, while also being incentivized to add friction and arbitrary obstacles.