JPMorganChase

October 21, 2025

The Honorable Russell Vought
Acting Director
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552
Via Electronic Delivery

Re: Advanced Notice of Proposed Rulemaking regarding "Personal Financial Data Rights Reconsideration" Docket No. CFPB-2025-0037

Acting Director Vought,

JPMorgan Chase ("JPMC") appreciates the opportunity to comment on the Consumer Financial Protection Bureau's ("CFPB") Advanced Notice of Proposed Rulemaking ("ANPR") regarding "Personal Financial Data Rights Reconsideration" under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd Frank").

At JPMC, **customers are the center of everything we do**, from the products and services we offer to help them manage and improve their financial lives, to the extensive measures we undertake to keep their personal financial data safe and secure. Consumer-permissioned data sharing is no different: **we support data sharing and open banking,** and we have been at the forefront of building and maintaining a safe and secure ecosystem, where customers can seamlessly connect their accounts to fintech apps, all while keeping their personal data private and secure.

I. The Free Market Is Working

JPMC helped pioneer bilateral data-sharing agreements, starting in 2017, and now maintains agreements with major aggregators, fintechs, payment processors, and a prominent cryptocurrency exchange. Each of these agreements was reached through arms-length negotiations, and several of these parties reaffirmed their commitment to our data-sharing principles by negotiating amendments that updated the terms of access. JPMC provided meaningful consideration in these negotiations, including streamlining processes that were identified by our counterparties.

Our innovation and leadership have driven significant growth: data sharing has flourished across the United States. For example, the number of apps linked to JPMC accounts has more than doubled from 5,000 to 11,000 over the last two years, and these apps serve over 24 million of our customers. During that same time period, monthly data calls have doubled from 1 billion to 2 billion. Despite holding only 11% of U.S. deposits, JPMC's data channel supports Application Programming Interface ("API") call volumes equivalent to the *entire* UK open banking system.[1] This growth happened because of free market participants—not government mandates.

[1] *See* https://www.openbanking.org.uk/.

Long before the CFPB published the 2024 Personal Financial Data Rights rule ("PFDR"), JPMC contributed to making the ecosystem more secure by introducing its own APIs for customer data sharing. This innovation eliminated the need for the continued use of screen scraping—where data middlemen asked consumers for their login credentials, used that confidential information to gain direct access to a bank account, and accessed the account multiple times each day to harvest data. Through JPMC's innovation, consumers could keep their login credentials private, select specific accounts for data sharing with aggregators, and transmit their data through safe and secure data channels. Our investment in consumer protection through our infrastructure is significant. Since launching our APIs, we estimate we have spent hundreds of millions specifically to build and harden our data-sharing environment, ensuring a secure way for aggregators, payments processors, and fintechs to access our customers' data. Over the same period, we estimate we have spent billions on the infrastructure needed to collect, organize, host and secure the data—an investment that is the foundation of our entire network. Not to mention the material investment to provide the best-in-class, underlying financial products and services that generate the data.

In addition to these technological innovations, the agreements between JPMC and aggregators have helped to make the ecosystem more secure, innovative, competitive, and pro-consumer by: (1) having aggregators agree to access only accounts specifically permissioned by consumers; (2) aggregators agreeing only to use consumer data for improving products and services/creating new services related to the service that the consumer is requesting; (3) identifying the specific data elements that will be shared; (4) providing clear allocation of liability; (5) providing for risk management and termination rights; and (6) committing to performance standards far stronger than anything required by the PFDR and on aspects that market participants truly value.

While we have made progress, there is still more to do. Data-sharing risks are not hypothetical. Financial data is some of the most private, valuable, and sensitive information in our customers' lives, and there are real risks when their data is misused or otherwise compromised. Indeed, over the last five years, reportedly millions of consumers' data have been exposed in fintech data breaches, including (1) in 2021, a major fintech trading platform announced a data breach affecting 7 million customers; (2) in March 2025, a major fintech app announced a class action settlement for a data breach involving potentially 158 million consumer accounts; and (3) in May 2025, a federal court granted preliminary approval of a class action settlement for a data breach involving a bank-service partner for fintechs. Data misuse also has been a problem in the industry—consumer class actions also have been filed against several prominent aggregators, challenging their approach to obtaining consent and their use of data to develop other products and services, including: (1) a $58 million class action settlement with one major aggregator in 2022; (2) a 2020 putative class action against another; (3) a 2023 putative class action lawsuit against yet another and (4) a 2024 putative class action lawsuit against a fourth aggregator.

Further, as consumer data has been increasingly used for payments, fintech apps' payments initiation have been plagued by comparatively high rates of fraud, resulting in customer claims and disputes that banks must process and investigate.[2] It is critical to note that Section 1033 is aptly named "Consumer

[2] We have seen before what happens when intermediaries aren't accountable for consumer protection: spikes in fraud, elder abuse, and other real harms. Today, for example, foreign middlemen can host fraudulent sites on cloud or web platforms, profit

Rights to Access *Information*" (ital. added). Section 1033 was never intended for payments initiation, money movement or open banking and, in fact, the statute is silent on payments. We trust that the new leadership at the CFPB will narrowly construe any final rule, instead of creating a massive open banking regime that was not contemplated by Congress.

II. The PFDR Would Undermine Progress

The PFDR's attempt to replace market-driven solutions with prescriptive rules would stifle innovation and make the ecosystem less secure. Our experience illustrates that voluntary, commercial agreements can accomplish more than government regulation. Indeed, in areas ranging from performance and security standards to prohibiting unsafe market behavior such as screen scraping, JPMC's agreements produced better results for the consumer and the ecosystem than the PFDR.[3]

The PFDR would have disrupted this well-functioning market without any authority from Congress. The CFPB got it exactly right when it said in its motion for summary judgment earlier this year: "nothing in the language of Section 1033 or its legislative history suggests that Congress intended to delegate to the Bureau free-ranging authority to regulate the entire open banking system—that is, the intricate network of commercial entities sharing a consumer's personal financial data well beyond sharing it with the consumer directly."[4]

III. All Participants Should Share Responsibilities and Invest in Maturing the Ecosystem

A healthy data-sharing ecosystem requires investment and accountability from all stakeholders, including those who build and maintain APIs and others who pay market rates for the value they receive. Allowing fees to be charged lets the market decide the value of services, supports ongoing maintenance and improvements in essential infrastructure, discourages unnecessary data collection, and motivates aggregators to prioritize secure practices over quick profits. When aggregators pay market-based rates, they are more likely to take only the data they need, and data providers are more likely to continue to invest in and improve the infrastructure on which the entire ecosystem depends. Banning or regulating fees is not lawful; leads to over-collection of sensitive consumer data; forces banks to subsidize aggregators, payments processors, and crypto companies—many of whom are very large, multi-billion dollar companies that are creating high-margin products that directly compete with core banking; and slows down investment and innovation—ultimately harming consumers. While some data middlemen and well-funded fintechs have publicly and misleadingly criticized JPMC's fee structure, JPMC's pricing represents a *small fraction* of the fees listed and negotiated by those same aggregators and fintechs for the very same data and services. We know this because some aggregators publicly list their fees and JPMC itself pays these fees to import data for our customers.

---

from exploitation, and face no liability, while the platform itself gets paid and also bears no responsibility for consumer harm. We should not repeat those mistakes in open banking, unleashing fintech apps and their service providers without accountability for the full range of harm they cause.

[3] The PFDR's rigid rules likely would have resulted in a "race to the bottom" for security standards, with companies checking the minimum requirements box instead of innovating for better solutions.

[4] See CFPB Motion for Summary Judgment at 6.

Our ability to charge fees was a component of every agreement we signed since our first bilateral agreement in 2017. JPMC did not charge fees for many years as the industry was maturing, despite our data access agreements expressly allowing us to do so. With a business model based on free inputs, aggregators were emboldened to take much more data than necessary, which exposed customer data to greater risks and overly taxed our system. Now that the ecosystem has matured, and data over-consumption has proliferated, our costs have risen.

We now have successfully negotiated fees on terms that will support ongoing maintenance of, and improvements to, our data-sharing infrastructure and disincentivize unnecessary data access from customer accounts. As of the date of this letter, **JPMC has reached agreements representing 80% of the aggregator-volume on JPMC's APIs.** Those negotiated arrangements have already yielded benefits to all parties in the ecosystem, including decreases in the volume of unnecessary data calls; deregistration of unnecessary payment credentials; increased performance standards; and other innovation commitments.

The engine of free exchange that powers our nation's economy is fully capable of driving an innovative, customer-centric marketplace for data access and sharing. Any new rulemaking should preserve and promote this competitive market, especially given Section 1033's limited scope. The statute is a sparse, four-paragraph provision meant to let consumers access their own data, not a vehicle to reshape the already thriving financial services sector. It sets a statutory minimum for consumer data access by guaranteeing access to a limited set of data elements by a limited set of parties – which banks are already providing through online banking and downloadable materials. We hope that any final rule will support, not hinder, innovation and investment in this fast-growing and dynamic market. We should avoid following Europe's highly prescriptive approach which has resulted in a far less vibrant and robust data-sharing ecosystem with sluggish consumer adoption. Only by working together—banks, payment processors, fintechs, and data aggregators with limited government intervention—will we be able to maintain, protect, and improve this innovative system and truly serve those who matter most: consumers.

* * *

As part of our response to the CFPB's ANPR, JPMC offers below a detailed description of our consumer-centric data-sharing principles, its overarching perspectives on the CFPB's questions, and detailed answers to each of the questions in the appendix.

I. Data-Sharing Principles the Private Sector Should Be Allowed to Address

Our data-sharing principles are simple and foundational to the bilateral agreements we have already signed: consumers should have control of their data and its use from beginning to end; the data-sharing ecosystem must be safe, secure, and private; and all stakeholders should support the ecosystem to promote security and innovation. To accomplish this, we have provided further details below:

- Consumers must control their data, with clear consent, transparency of use, and easy revocation.

- Third parties may use account data solely for the direct benefit of the consumer and specifically for the product or services they authorized. Third parties must regularly seek reauthorization and remove unauthorized data from the ecosystem.
- Third parties may not sell the data beyond the services the consumer signed up for, even in anonymized/aggregated form.
- Screen scraping should be prohibited, and secure APIs and tokenization should be standard.
- All ecosystem participants must meet robust security and liability standards, and banks and other data providers must be able to conduct third party risk management oversight with an ability to decline participants who do not meet the standards.
- Consumers should be able to access their data across industries, banks, and nonbanks, just as banks provide access to their financial data. If providers are accessing data through Section 1033 mechanisms, they should provide access to account data in their ecosystem on reciprocal terms.
- Data providers must be able to charge market-based rates.
- A clear liability framework must exist.

II. JPMC's Perspective on the ANPR Questions

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

Section 1033(a) is a brief provision designed to ensure that consumers have access to their financial information. Specifically, the statute states that access to "information relating to any transaction, series of transactions, or to the account including costs, charges and usage data. The information shall be made available in an electronic form usable by consumers."[5] Section 1033's plain language addresses a consumer's ability to manage their finances – it does not create a cottage industry of data middlemen or payments processors pulling data for free, without accountability and without commercial restrictions.

Congress did not intend for technology companies, data aggregators, payments processors, or fintech apps to have statutory rights to consumer data. The narrow language of Section 1033 grants this statutory right to data to consumers and those acting in a fiduciary-like capacity. As Barney Frank, a Dodd-Frank author, recently stated: "When we passed Dodd-Frank, the aim was to build trust between consumers and financial institutions; the intent was not to create a new class of middlemen who undercut the work of institutions and warehouse customer data."

Interpreting the law this way does not mean popular apps and their data-middlemen providers will lose access to consumer-permissioned data. Consumers still control their data, and market participants can receive access through commercial agreements and conspicuous, informed consent. The past decade shows that consumer demand, conspicuous disclosures and informed consent, commercial agreements, and responsible business practices drive access to data. When granted access to sensitive financial information, data middlemen must act responsibly, using this data exclusively for the benefit of the specific customer and the products or services they utilize. They should not leverage consumer financial data to develop or support unrelated products or services, nor can they disclaim their responsibilities

[5] DFA Sec. 1033(a).

through disclosures. JPMC has helped lead the development of responsible, consumer-permissioned access and use of data, and we expect to continue to do so.

B. Fees Under Section 1033

There Is No Lawful Basis to Regulate Fees

JPMC supports the growing market for services that rely on shared consumer financial data and has invested heavily in this area. However, it is essential that all participants invest in the ecosystem to keep it secure and effective for consumers.

Congress did not address fees in Section 1033, so the CFPB does not have the authority to regulate them.[6] As the Trump Administration's CFPB rightly stated in its Motion for Summary Judgment ("MSJ"): "Congress's silence on fees is a particularly shaky foundation for the Rule's absolute fee prohibitions. The statute itself simply dictates that data providers 'make available to a consumer' their consumer's financial data, yet the Rule regulates beyond the scope of the statute by mandating that data providers make consumer data available to other commercial actors in a costly and complicated data-sharing system. The Rule then adds insult to injury by forcing data providers to bear the costs of this new regime, giving a windfall to third parties that directly benefit from that access requirement. Indeed, the Rule itself acknowledges the significant costs for data providers to establish and maintain a developer interface."[7] We agree that the PFDR's fee prohibition targeting banks and other data providers was unlawful.[8]

As to the ANPR questions that implicate cost-based limitations or fee caps, regulating fees in that manner also is unlawful. As the CFPB acknowledged in its MSJ, "[a]gencies have only those powers given to them by Congress."[9] Here, Section 1033 is silent on fees—something the PFDR itself already acknowledges.[10] This silence means there is no lawful basis for the CFPB to regulate fees. Nor does silence provide a lawful basis for the CFPB to decide how much the private sector should be allowed to

---

[6] CFPB Motion for Summary Judgment at 11 ("The [PFDR] separately exceeds the Bureau's authority and is contrary to law because Section 1033 does not authorize the Bureau to prohibit banks from charging any fees for maintaining and providing access through the required developer interfaces.").

[7] *See* CFPB Motion for Summary Judgment at 12.

[8] To be clear, the PFDR did not prohibit fees across the ecosystem. Instead, the PFDR targeted one market participant – the most important one – and prohibited data providers alone from charging fees. Other members of the of the private sector were allowed to continue their existing practices of market prices for consumer data. Whether banks alone must bear the costs of funding a massive data-sharing regime under Section 1033 is a "fundamental detail[]" of the regulatory scheme that Congress did not authorize the CFPB to address through "vague terms or ancillary provisions." *See Whitman v. Am. Trucking Ass'ns*, 531 U.S. 457, 468 (2001).

[9] CFPB Motion for Summary Judgment at 5.

[10] See 89 Fed. Reg. at 90884. Courts should require clear indications that Congress authorized such burdens on businesses and ordinary free-enterprise principles. *Whitman*, 531 U.S. at 468; *see also* Sanofi Aventis U.S. LLC v. HHS, 58 F.4th 696, 707 (3d Cir. 2023) ("Legal duties do not spring from silence."); Christensen v. Harris Cnty., 529 U.S. 576, 588 (2000) (treating absence of authorization for action as authority to issue prohibition on that action is "exactly backwards")

charge for services.[11] Any such rule would violate Section 1033 and the Administrative Procedures Act ("APA") and be entitled to no deference under *Loper Bright Enterprises v. Raimondo*, 603 U.S. 369 (2024).[12]

Finally, the PFDR took the position that allowing data providers to negotiate fee arrangements with third parties "would obstruct the data access right that Congress contemplated" in Section 1033.[13] Nothing in the text of the statute supports that position, and the recent free-market actions of market participants have shown that position to be demonstrably false. Nor is the PFDR's version of free and unlimited data access for third-party commercial actors what Congress "contemplated" when it enacted Section 1033. As the CFPB noted in its recent court filing in the 1033 litigation: "There is no indication in Section 1033 that Congress authorized the Bureau to force data providers to establish a separate complex and costly system to make information about consumers available to separate commercial actors, free of charge."[14]

Market-Based Rates Drive Proper Data Use, Data Security, and Innovation

Charging fees related to data sharing is not a new or novel concept. It is standard practice across industries, including pharmaceuticals, telecommunications, social media, healthcare, and financial services. Market-based rates are permitted to be charged in all those industries. In fact, JPMC's consumer businesses pay approximately $350 million for data to run its businesses, the majority – approximately $260 million per year in 2024 – for data-sharing services.[15] This data we pay for enables products to support our consumers and small businesses with services like budgeting, financial planning, fraud management, credit access, and identity monitoring.[16]

---

[11] *See also West Virginia v. EPA*, 597 U.S. 697, 723 (2022) ("Extraordinary grants of regulatory authority are rarely accomplished through 'modest words,' 'vague terms,' or 'subtle devices.'") (citation omitted); *Ala. Ass'n of Realtors v. Dep't of Health & Human Servs.*, 594 U.S. 758, 764 (2021) (requiring "exceedingly clear language" when Congress "wishes to significantly alter the . . . power of the Government over private property") (citation omitted); *Ams.for Beneficiary Choice v. U.S. Dep't of Health and Human Servs.*, No. 24-cv-00439-O, 24-cv-00446-O, 2025 WL 2390849, at *6 (N.D Tex. Aug. 18, 2025) (holding that the Centers for Medicare and Medicaid Services lacked authority to establish a rate cap because the statutory language at issue contained no language expressly delegating ratemaking authority).

[12] Any regulation or prohibition on fees also would raise questions under the major questions doctrine or other legal doctrines prioritized by President Trump in his statements regarding regulatory policy. See https://www.whitehouse.gov/presidential-actions/2025/04/directing-the-repeal-of-unlawful-regulations/; *see Biden v. Nebraska*, 600 U.S. 477, 502, 506 (2023) (holding that the "economic impact" of the Biden administration's student debt cancellation program raised a major question of "deep economic and political significance" that required the administration to point to "clear congressional authorization to justify the challenged program").

[13] 89 Fed. Reg. at 90884; see also id. at 90886 (asserting that "allowing data providers to charge what they see as commercially reasonable fees is likely to obstruct consumers' ability to use their data").

[14] CFPB Motion for Summary Judgment at 12.

[15] These figures do not include fees for data-sharing that JPMC pays across other areas of its businesses, including, for example, institutional research.

[16] Approximately half of the fees paid by JPMC's consumer businesses support services related to credit access and account underwriting for consumer and small business accounts. The other half of the fees we pay support our third-party identity and verifications services and data aggregator and enrichment services.

Open banking also is no longer new in the market, and it is operating at a scale and momentum that is mature. Market rates have existed in open banking for nearly a decade—aggregators and payments processors publicly advertise their rates, and their fees have been commercially negotiated in thousands of bilateral agreements. JPMC is among those who have reached commercial agreements with aggregators, and we pay their fees to import data for our customers. JPMC charging fees may be a new development, but this market should not be exempt from free-market principles and the right to charge market rates should be reciprocal. Aggregators, payments processors, and fintechs access our APIs two billion times per month to support their businesses, and they should pay market rates.

Without fees, aggregators are incentivized to access data excessively, distorting the market, and shirking accountability for consumer protection. In the process of negotiating fee agreements, we have found that free access leads to unnecessary over-collection of data. **Recent feedback shows that some aggregators plan to reduce their API call volumes by 30-50%,** while still providing the exact same services to customers, and fintech apps have started to deregister unused account tokens that could be used to withdraw funds from consumer account because they did not need the information to begin with. When companies pay for data, they are more careful about what they collect.

Likewise, when banks charge market rates, they are motivated to improve their services.[17] This creates a healthier, more efficient market. Regulating or banning fees would distort the market, discourage investment, and force data providers to bear costs without fair compensation. Ultimately, this would harm consumers and slow innovation.

The CFPB Should Not Set Cost-Based Limitations or Fee Caps

The CFPB does not have the legal authority to impose cost-based limitations or fee caps. Any such provision in a final rule would exceed the authority provided by Section 1033 and, therefore, violate the APA. Further, it is inappropriate to regulate business-to-business fees based on a narrow range of limited costs. The costs associated with data sharing are expansive, including the investments for the API that shares data, the underlying infrastructure and systems needed to collect, host, and secure it, and the products and services that generate the data. For all the reasons described in the preceding paragraph, the CFPB should allow market-based pricing.

Based on publicly available pricing, the fees that JPMC charges represent a small fraction of the overall fees fintechs are already charging today. For example, one major market participant advertises fees of $0.10 for every balance call, at least 50 times more than what JPMC charges for a non-payments balance call. That participant posts substantially higher fees for certain payments – 2.6% + 30 cents for "instant bank payments," which translates into a $2.90 fee for a $100 transaction. JPMC's fee to support that payment would be less than 1% of that processor's fee. While we have chosen one market participant to convey the point, they are not an outlier.

[17] The PFDR's rigid rules likely would have resulted in a "race to the bottom" for security standards, with companies checking the minimum requirements box instead of innovating for better solutions.

C. Privacy Concerns in the Exercise of Section 1033 Rights

Through bilateral agreements, we negotiated responsible restrictions on the secondary use and sale of data by aggregators, payments processors, and fintechs. We strongly support the CFPB's view in the PFDR that targeted advertising, cross-selling, and data sales are not allowable uses of consumer-permissioned data. Data middlemen are increasingly using consumer data to develop new products and services that are unrelated to the service for which that data was shared. For example, data middlemen are using data connections to develop commercial fraud models, cash underwriting services, and other unrelated businesses. This is why informed, transparent consumer consent is so critical. We believe data sharing is a lifecycle: it begins with informed consent, progresses with usage specifically limited to the product or service utilized by the consumer for their benefit, and concludes when the customer withdraws permission. Consumers must be clearly informed about data sharing, retain control throughout the process, and have the ability to revoke access and delete their data upon discontinuing a service.

If the CFPB limits Section 1033 to fiduciary-like representatives, most privacy concerns will be addressed by the obligations those parties owe to consumers. JPMC remains committed to letting customers share their financial information without losing control.

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

The risks to consumer financial data are the same whether the data is held by a bank, aggregator, or fintech. **Protections should be consistent across all parties.** JPMC's agreements help safeguard customer information, but the PFDR would limit banks' ability to control third-party access and ensure security.

Once data leaves the bank, it faces real risks like breaches, privacy violations, and fraud. Fraud claims for aggregator-initiated payments are nearly *two times higher* than the same payments not initiated through aggregators. Additionally, consumers may not realize they have relationships with both fintech apps and data aggregators, and they turn to their bank when problems arise. JPMC spends millions each year handling claims and investigating issues, even when not directly involved with the transaction. Responding to breaches can require closing accounts, recovering losses, and providing extensive customer support.

Tokenized Account and Routing Numbers Offer Additional Protection

To protect customers from harm, banks should be able to share tokenized account and routing numbers ("TANs") instead of actual account numbers. TANs limit exposure in the event of a breach and allow consumers to easily manage and revoke access. This is possible because JPMC issues a unique token to each fintech app for each consumer account. In the event of a breach, JPMC can suspend or delete that individual TAN without the disruption of closing the customer account and needing to open a new one. These risks are not hypothetical: following announcements of cyber breaches involving fintech apps, JPMC has reissued TANs for consumers linked to those apps, protecting them from unauthorized transactions to their account. Beyond these important security protections, TANs also allow our

customers to use a dashboard on our banking website or app to see which third parties have stored TANs and easily manage access.

Bank Risk Management Oversight is Critical to Secure the Ecosystem

The PFDR constrained banks' ability to apply prudent risk management standards, which is contrary to the principles of safety and soundness. Banks must be able to deny third-party access for risk-based reasons, as required by safety and soundness rules, anti-money laundering laws, and other detailed guidance on third-party risk management issued by the Office of the Comptroller of the Currency and other federal regulatory agencies. This is how JPMC's negotiated agreements have long operated, and we expect to continue to operate under a new rule.

The PFDR significantly restricted this ability in a way that puts the customers and the financial system at risk. While the PFDR permitted "reasonable" denials, its narrow definition of "reasonable" denials creates confusion and risk. Banks may be forced to choose between satisfying risk management guidance or complying with the PFDR. The CFPB should remove these restrictions that create conflicting legal requirements in order to protect banks and consumers.

All entities accessing data pursuant to Section 1033 should follow the security standards defined in the Federal Financial Institutions Examination Council ("FFIEC") IT Examination Handbook and the requirements of GLBA. These standards should apply to all participants, not just banks, and should be inspected by regulators.

The CFPB should ensure that any final rule does not impair banks' ability to use other important risk-management tools. Banks should retain the ability to require information security standards through bilateral agreements with data aggregators and third-party data recipients to be met as a condition of accessing their APIs. Bilateral contracts remain essential for addressing liability, risk management, and data security.

E. Data Manipulation

On the topic of data use standards set by the Financial Data Exchange, the CFPB should be aware that aggregators often ingest standardized data and subsequently transform it into proprietary formats. This practice creates barriers for consumers seeking to access or transfer their data, thereby increasing switching costs and limiting consumer choice.

No matter how much data these middlemen manipulate to claim proprietary ownership, it does not make it true. The data should always remain the property of the consumer. If the CFPB considers standardization, aggregators should adhere to the same standards as banks for data sharing.

F. Compliance Dates

It is incomprehensible that the industry – including banks of all sizes – is marching towards complying with a rule that the CFPB itself says is unlawful. The CFPB should immediately suspend current PFDR compliance deadlines.

Any changes to the rule through this rulemaking will require new compliance work, making it impractical to continue working towards complying with the suspended rule. JPMC estimates it could take 24 months to comply with a revised rule, given the complexity and scale of changes involved. This rule is unique because it requires cooperation throughout the entire ecosystem, including banks, data recipients, and aggregators. Compliance timelines should allow all parties enough time to adapt, ensuring interoperability and standardization for safe, reliable data sharing.

In terms of procedure, we do not believe the CFPB has to conduct an *additional* process under the Small Business Regulatory Enforcement Fairness Act ("SBREFA")[18] because they already fulfilled these requirements when it conducted the small entity representative ("SER") panel on October 27, 2022 and released the SBREFA report[19] on March 30, 2023. During this process, the main issues, including charging, were already discussed by the SERs.

III. Conclusion

This is a complex, evolving, and growing data ecosystem that has thrived through bilateral agreements which reflect market forces and, ultimately, consumer preferences. The current ecosystem has fostered innovation, competition, and robust consumer protections without the need for expansive regulation. We hope the CFPB will promote the market-driven approach that has led to this progress, and – most importantly – put consumer protection and preferences above all else.

JPMC appreciates the opportunity to set forth our consumer-centric principles and additional recommendations as the CFPB endeavors on a revised 1033 rulemaking. In the appendix, please find our answers to each of the specific ANPR questions. We stand ready to be a resource as the process evolves and welcome the opportunity to discuss these important issues.

Sincerely,

Melissa Feldsher
Head of Consumer Payments

[18] 5 U.S. Code § 609.

[19] 1033 Data Rights Rule SBREFA Panel Report, March 30, 2023
https://files.consumerfinance.gov/f/documents/cfpb_1033-data-rights-rule-sbrefa-panel-report_2023-03.pdf

APPENDIX

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?

Answer: The PFDR stretches the definition of "representative" far beyond what Congress intended. The statute is clear: data rights belong to consumers and their fiduciaries, not tech companies, payments processors, or aggregators.

In their recent court filing, the CFPB aptly cited the *Merriam-Webster Dictionary* for the "plain meaning" of representative, saying: "Thus, the best reading of 'representative' is 'someone who represents another as agent, deputy, substitute, or delegate usually being invested with the authority of the principal.'" *See* CFPB Motion for Summary Judgment ("MSJ") at 9. We agree with this reading.

The CFPB then devoted three pages of its motion for summary judgment to explaining how the PFDR's interpretation of "representative" exceeded Section 1033's authority and was inconsistent with legal precedent. JPMC endorses the CFPB's analysis on pages 8-11 of its motion, including this notable observation: "The Bureau exceeded its statutory authority when it used the term 'representative' as a hook to establish a comprehensive open-banking regulation, instead of adhering to statutory authority to only make a consumer's information available to that individual or those who are actually acting as agents, trustees, or representatives on that individual's behalf." *See* CFPB MSJ at 9.

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?

Answer: The plain text of Section 1033 is the starting point – and the endpoint – for interpretation. As the CFPB acknowledged in its motion for summary judgment, "[a]gencies have only those powers given to them by Congress." Further, "[w]hen 'a statute gives an agency no room at all to maneuver,'" that statute must be given "its 'single, best meaning,' 'fixed at the time of enactment.'" *See* CFPB MSJ at 5.

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?

Answer: Yes. All three terms imply fiduciary duties. The statute groups them together for a reason.

As the CFPB stated in its motion for summary judgment: "The terms 'agent' and 'trustee' both involve a fiduciary relationship and a duty of loyalty to act for the principal's benefit. And the term 'representative' in the statute 'should be read in a similar manner to its companions'--that is, it should take on a meaning similar to the words 'agent' and 'trustee' listed alongside it." *See* CFPB MSJ at 8.

Regarding the question about distinctions between "agent" and "representative," the CFPB correctly answered this question in its motion for summary judgment. An agent involves "a fiduciary relationship and a duty of loyalty to act for the principal's benefit." CFPB MSJ at 8. A representative involves "a special relationship and a fiduciary or similar obligation to those they represent – such as, for instance, an executor of an estate, a parent or guardian, or other designed persons." CFPB MSJ at 8; *see also e.g., In re Imerys Talc Am., Inc., 38 F.4th 361, 376 (3d Cir. 2022)* ("'Legal representative' is a term of art, referring to one who owes fiduciary duties to his absent, represented constituents.")

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"?

Answer: The CFPB's analysis should adhere closely to the statutory text as enacted. As the CFPB noted in its court filing: "[a]gencies have only those powers given to them by Congress" and "[w]hen a 'statute gives an agency no room at all to maneuver,'" that statute must be given its "'single, best meaning,' 'fixed at the time of enactment.'" Finally, when interpreting a statute, the agency must "[f]irst and foremost ... analyze the statutory text," and "when the text standing alone does not supply an answer, courts must consider canons of interpretation" that can "make[] the statute's meaning clear." *See* CFPB MSJ at 8.

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?

Answer: Consumers still control their data, and data middlemen still can receive access to that data through commercial agreements and conspicuous, informed consent. Market participants compete by earning consumer trust—not by statutory entitlement. Further, when granted access to highly-sensitive financial information, data middlemen must act responsibly, using this data exclusively for the benefit of the specific customer and the products or services they utilize. They should not leverage consumer financial data to develop or support unrelated products or services, nor can they disclaim their responsibilities through disclosures.

Congress did not intend technology companies, data aggregators, or payment processors to have statutory rights to consumer data. As Barney Frank, a Dodd-Frank author, recently stated: "When we passed Dodd-Frank, the aim was to build trust between consumers and financial institutions;

the intent was not to create a new class of middlemen who undercut the work of institutions and warehouse customer data."

Interpreting the law this way does not mean popular apps and their providers will lose access to consumer-permissioned data. The past decade shows that consumer demand, conspicuous disclosures and informed consent, commercial agreements, and responsible business practices drive access to data. For nearly a decade, JPMC has helped lead the development of consumer-permissioned access to data, and we expect to continue to do so.

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?

Answer: No, standardization is about data formats "usable by consumers," not access rights. Section 1033(d) does not the expand the definition of "consumer" or "representative" to include data middlemen or aggregators.

Instead, the CFPB got it exactly right when it said in its court pleading: "the term 'representative' in the statute 'should be read in a similar manner to its companions'--that is, it should take on a meaning similar to the words 'agent' and trustee' listed alongside it." CFPB MSJ at 8.

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?

Answer: The law is clear—the CFPB has no authority to expand the definition of "representative" beyond the statute's plain meaning. Only those with fiduciary duties—loyalty, care, no self-dealing—qualify as having statutory rights under Section 1033.

If a new rule found that data middlemen, payments processors, and fintech apps have *statutory rights* to consumers' data, that rule would exceed the CFPB's authority under Section 1033 and, therefore, violate the Administrative Procedures Act ("APA"). If the CFPB abandoned positions that it took in its motion for summary judgment, the new rule also would be arbitrary and capricious. Any party who claims a statutory right to consumer data pursuant to Section 1033 must have fiduciary obligations to their principal, which means they have a duty of loyalty and care to their principal, cannot act in their own interest, cannot sell data, and cannot disclaim their fiduciary duties through disclosures.

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?

Answer: The term "consumer" as used elsewhere in Dodd-Frank is intended to reflect its ordinary meaning—specifically, an individual. Section 1032 mandates that disclosures be provided in a manner that "permits consumers to understand the costs, benefits, and risks

associated with the product" (12 U.S.C. § 5532(a)). Furthermore, when assessing whether an act may be deemed abusive under Section 1031, the CFPB considers whether the consumer possesses "a lack of understanding of the material risks, costs, or conditions" (12 U.S.C. § 5531(d)(2)(A)). These provisions are clearly designed to apply exclusively to individual consumers. Interpreting them to include a data middleman, payments processor, or fintech entity would not align with the legislative intent or other portions of the statute.

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?

Answer: No. Congress did not give the CFPB legal authority to regulate fees. To be clear, the PFDR did not prohibit fees across the ecosystem. Instead, the PFDR targeted one market participant – the most important one – and prohibited data providers alone from charging fees. Other members of the of the private sector were allowed to continue their practices of charging market rates for consumer data. Forcing banks to subsidize third parties is unlawful, arbitrary, and ignores the real value, and risks, of data sharing and broader investment to produce, collect, organize, host, and secure the data.

As the CFPB said in its motion for summary judgment, "Congress's silence on fees is a particularly shaky foundation for the Rule's absolute fee prohibitions. The statute itself simply dictates that data providers 'make available to a consumer' their consumer's financial data, yet the Rule regulates beyond the scope of the statute by mandating that data providers make consumer data available to other commercial actors in a costly and complicated data-sharing system. The Rule then adds insult to injury by forcing data providers to bear the costs of this new regime, giving a windfall to third parties that directly benefit from that access requirement. Indeed, the Rule itself acknowledges the significant costs for data providers to establish and maintain a developer interface." *See* CFPB Motion for Summary Judgment at 12. JPMC agrees with the CFPB that the fee prohibition targeting banks is unlawful because the PFDR exceeded its statutory authority.

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

Answer: No. Consumers already get free access to their data. The fee prohibition that targeted data providers only benefits commercial actors who already were monetizing the data – directly and indirectly. It does not benefit consumers and ignores the reality of how the market works.

Congress contemplated that consumers and their fiduciaries have statutory rights to data. Those rights exist at JPMC—our customers and their fiduciaries have free and unlimited access to their financial data through JPMC's website, mobile app, branches, and call centers.

The CFPB's own motion for summary judgment also answers this question: "The Rule's contrary logic proves too much. According to the Rule, '[i]f data providers could decide what fee to charge, they could limit or eliminate the right that CFPA section 1033 confers.' But the Rule goes

far beyond ensuring that fees do not get in the way of information being made available to consumers and instead forces data providers to bear significant costs in making data available for the open banking system to function." *See* CFPB MSJ at 12.

Finally, the PFDR's flawed data-obstruction assertion has been shown to be false: JPMC has reached agreements representing 80% of the aggregator traffic on JPMC's APIs, and JPMC customers continue to enjoy access to the apps they choose.

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?

Answer: Regulating fees through cost-based limitations, fee caps, or fee prohibitions is unlawful. Any such provision in a final rule would exceed the CFPB's authority under Section 1033 and, therefore, violate the APA.

Further, it is inappropriate to regulate business-to-business fees based on a narrow range of costs. That's because the costs associated with data sharing are expansive, including the investments for the API that shares data, the underlying infrastructure and systems needed to collect, host, and secure the data, and the products that generate the data. To illustrate, since launching our APIs, JPMC estimates it has spent hundreds of millions specifically to build and harden our data-sharing environment, ensuring a secure way for aggregators, payments processors, and fintechs to access our customer's data. Over the same period, we estimate we also have spent billions on the infrastructure needed to collect, organize, host and secure the data—an investment that is the foundation of our entire network. Not to mention the material investment to provide the best-in-class, underlying financial products and services that generate the data.

12. What is a reasonable range of estimates regarding the marginal cost to covered financial institutions of responding to requests made under the auspices of section 1033? How do these estimates vary by the size of the covered financial institution?

Answer: See answer to Question 11.

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?

Answer: Banks should hear directly from their customers about whether third parties are authorized to receive sensitive financial data. As to costs, see answer to Question 11.

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?

Answer: Section 1033 is the starting point – and the endpoint – for interpretation on this issue. As the CFPB acknowledged in its motion for summary judgment, "[a]gencies have only those powers given to them by Congress." *See* CFPB MSJ at 5. Here, regulating fees through cost-based limitations, fee caps, or fee prohibitions is unlawful. Any such rule would exceed the CFPB authority under Section 1033 and, therefore, violate the APA.

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?

Answer: Yes, but a reasonable rate should be determined by free-market negotiations and should not be limited to offsetting costs. Instead, market rates, which data providers should be allowed to charge, should reflect the value derived from accessing the data and the risks of sharing it.

Charging fees for data is not a new or novel concept. It is standard practice across industries, including pharmaceuticals, telecommunications, social media, healthcare and financial services. In fact, JPMC's consumer businesses pay approximately $350 million for data, the majority – approximately $260 million per year in 2024 – for data-sharing services, commensurate with the ones it enables for open banking. This data we pay for enables products to support our consumers and small businesses with services like budgeting, financial planning, fraud management, credit access, and identity monitoring.

Open banking is no longer new in the market—it is operating at a scale and momentum that is mature. Market prices have existed in open banking for nearly a decade—aggregators and payments processors publicly advertise their rates and their fees have been commercially negotiated in thousands of bilateral agreements. JPMC is among those who have reached commercial agreements with aggregators, and we pay their fees to import data for our customers. JPMC charging fees may be a recent development, but this market should <u>not</u> be exempt from free-market principles and the right to charge market rates should be reciprocal. Data middlemen access our APIs two billion times per month to support their businesses; they should pay market rates.

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?

Answer: No. Fee caps are unlawful and anti-competitive. The market—not regulators—should set prices.

Regulating fees through fee prohibitions, fee caps, or cost-based limitations exceeds the CFPB's authority under Section 1033 and, therefore, violates the APA. See answer to Question 15.

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?

Answer: No, hidden account fees are unfair and distort the true cost of open banking products and services. Costs should be communicated clearly and transparently—so that users understand the true and full costs—when they decide to use the open banking product or service. Consumers who are using open banking services—not all customers—should pay the direct cost of the specific service they are using.

We firmly believe that consumers should not pay bank account fees to support the open banking ecosystem. Bank account fees should be limited to the products and services that banks offer directly to consumers. Here, JPMC provides its customers with free access to data about their accounts through its website, mobile app, branches, and call centers.

Information Security Concerns in the Exercise of Section 1033 Rights

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

Answer: If the CFPB limits Section 1033 to fiduciary-like representatives, most privacy concerns will be addressed by the obligations those parties owe to consumers.

We strongly support the CFPB's view in the PFDR, in § 1033.421(a)(2), that targeted advertising, cross-selling, and data sales are not allowable uses of consumer-permissioned data. Data middlemen increasingly appear to be using consumer data to develop new products and services that are unrelated to the service for which that data was shared, such as developing fraud models, cash underwriting services, and other unrelated activities. We believe data sharing is a lifecycle: it begins with informed consent, progresses with usage specifically limited to the product or service utilized by the consumer for their benefit, and concludes when the customer withdraws permission. Consumers must be clearly informed about data sharing, retain control throughout the process, and have the ability to revoke access and delete their data upon discontinuing a service.

Additional and important controls can be managed through voluntary agreements, as they have been for years. There should be clarity that banks and data providers can continue to pursue market-driven strategies so that data middlemen, fintechs, payments processor are accountable for the full range of harm they cause.

19. What are the fixed costs of establishing an information security architecture that is capable of ensuring, in the absence of compromise of operational protocols, that customer financial information can

be securely acquired, stored, and transmitted, by the consumer, from a "covered person" to the consumer?

Answer: As noted, regulating fees through cost-based limitations, fee caps, or fee prohibitions is unlawful.

Further, it is inappropriate to regulate business-to-business fees based on a narrow range of costs. That's because the costs associated with data sharing are expansive. Our investment to protect consumer data through our infrastructure is significant. Since launching our APIs, we estimate we have spent hundreds of millions specifically to build and harden our data-sharing environment, ensuring a secure way for aggregators, payments processors, and fintechs to access our customers' data. Over the same period, we have spent billions on the underlying infrastructure and systems needed to collect, organize, host and secure the data—an investment that is the foundation of our entire network. Not to mention the material investment to provide the best-in-class, financial products and services that generate the data

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?

Answer: The market can develop solutions for safe and secure data sharing for covered persons of varying sizes. The cost of those solutions can be accounted for in market-based pricing.

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?

Answer: As noted, security is very expensive, and data security and misuse in open banking have been a problem for fintechs and data aggregators (who are not fiduciaries).

Over the last five years, reportedly millions of consumers' data have been exposed in fintech data breaches. For example, in 2021, a major fintech trading platform announced a data breach affecting 7 million customers. In March 2025, one major fintech app announced a class action settlement for a data breach involving potentially 158 million consumer accounts. Finally, in May 2025, a federal court granted preliminary approval of a class action settlement for a data breach involving a bank-service partner for fintechs.

In addition, data misuse has been a problem in the industry—consumer class actions also have been filed against several prominent aggregators, challenging their approach to obtaining consent and their use of data to develop other products and services, including: (1) a $58 million class action settlement with one major aggregator in 2022; (2) a 2020 a putative class action against another; (3) a 2023 putative class action lawsuit against yet another; and (4) a 2024 putative class action lawsuit against a fourth aggregator.

22. Are there any peer-reviewed studies discussing whether levels of information security materially vary between those businesses that have fiduciary duties to their clients and those that do not?

Answer: See answer to Question 21 for recent litigation for data breaches and business practices for parties who do not have fiduciary duties.

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?

Answer: As noted above, cyber security is very expensive, and fintechs have had repeated data breaches that impact hundreds of millions of customers. These breaches have resulted in data loss and major settlements.

For data breaches involving third parties, JPMC also incurs real costs. Depending on the scenario, such data loss events require JPMC to reissue deposit accounts or reissue tokenized account numbers ("TANs"), reissue credit and debit cards, monitor for fraud, prepare for and handle incoming customer complaints, and absorb operating losses.

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?

Answer: Banks invest heavily in security, while non-bank actors often fall short. See JPMC's answer to Question 21.

25. Covered persons are subject to several legal obligations regarding risk management, such as safety and soundness standards, Bank Secrecy Act (BSA) requirements, and Anti-Money Laundering (AML) regulations. What should covered persons consider under these legal obligations when making information available to consumers? How could the PFDR Rule's interface access provision better allow covered persons to satisfy these legal obligations?

Answer: The PFDR undermines risk management. Banks must retain the right to deny risky access and set security standards through bilateral agreements.

The PFDR constrained banks' ability to apply prudent risk management standards, which is contrary to the principles of safety and soundness. Banks must be able to deny third-party access for risk-based reasons, as required by safety and soundness rules, anti-money laundering laws, and other detailed guidance on third-party risk management issued by the Office of the Comptroller of the Currency and other federal regulatory agencies. This is how JPMC's negotiated agreements have long operated, and we expect to continue to operate under a new rule.

The PFDR significantly restricted this ability in a way that puts consumers and the financial system at risk. While the PFDR permits "reasonable" denials, the PFDR's narrow definition of "reasonable" creates confusion and risk. Banks may be forced to choose between satisfying risk

management guidance or complying with the PFDR. CFPB should remove these restrictions that create conflicting standards in order to protect banks and consumers.

The CFPB should ensure that it does not impair banks' ability to use other important risk-management tools. Banks should retain the ability to require information security standards through bilateral agreements with data aggregators and third-party data recipients to be met as a condition of accessing their APIs. Bilateral contracts remain essential for addressing liability, risk management, and data security.

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

Answer: The PFDR's reliance on GLBA and the FTC Safeguard Rule for third-party data security created inconsistent oversight and standards. Mandating compliance with the FFIEC IT Security Handbook, and the requirements of the GLBA, would provide the most comprehensive and relevant protection for financial data. These standards should apply to all participants, not just banks, and should be inspected by regulators.

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?

Answer: Recognizing there are real risks to consumers, please see our answer to Question 26 for *minimum* security and privacy standards that should apply in the marketplace. We firmly believe the private sector also can help shape additional security and privacy standards. Indeed, we believe JPMC's commercial agreements have produced better results than the PFDR.

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?

Answer: Screen scraping is an unsafe practice, and aggregators have entered into commercial agreements with JPMC to not engage in the practice. In addition, to protect customers from harm, banks should be able to share TANs instead of actual account numbers. TANs limit exposure in the event of a breach and allow customers to easily manage and revoke access. This is possible because JPMC issues a unique token to each fintech app for each consumer account. In the event of a breach, JPMC can suspend or delete that individual TAN without the disruption of closing the customer account and opening a new one.

These risks are not hypothetical: following announcements of cyber breaches involving fintech apps, JPMC has reissued TANs for consumers linked to those apps, protecting our customers from unauthorized transactions to their account. Beyond these important security protections, TANs also allow our customers to use a dashboard on our banking website or app to see which third parties have stored TANs and easily manage access.

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?

Answer: No. Most API calls on our system are not tied to actual consumer requests—these calls are mass, automated data extractions by aggregators or fintechs and there is no consumer on the other end waiting for their data. A study by The Clearing House ("TCH") indicates that most consumers do not know the extent to which aggregators are accessing their account. *See* The Clearing House, Consumer Survey: Data Privacy and Financial App Usage, December 2021, *available at* 2021-tch-consumersurveyreport_final.pdf (finding 80% of financial app users are not aware that apps may use third parties to access consumers' personal and financial information, 78% didn't know aggregators regularly access personal data even when the app is closed or deleted, and 73% of financial app users are not fully aware that apps or third parties may store their bank account username and password).

Privacy Concerns in the Exercise of Section 1033 Rights

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

Answer: We strongly support the CFPB's view in the PFDR, in § 1033.421(a)(2), that targeted advertising, cross-selling, and data sales are not allowable uses of consumer-permissioned data. Data middlemen are increasingly using consumer data to develop new products and services that are unrelated to the service for which that data was shared. For example, data middlemen are using data connections to develop commercial fraud models, cash underwriting services, and other unrelated business.

This is why informed, transparent consumer consent is so critical. We believe data sharing is a lifecycle: it begins with informed consent, progresses with usage specifically limited to the product or service utilized by the consumer for their benefit, and concludes when the customer withdraws permission. Consumers must be clearly informed about data sharing, retain control throughout the process, and have the ability to revoke access and delete their data.

If the CFPB limits Section 1033 to fiduciary-like representatives, most privacy concerns will be addressed by the obligations those parties owe to consumers.

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?

Answer: JPMC is unable to confidently assess the practices of other entities. However, we do understand that data middlemen, payments processors, and fintech apps are using consumer financial data for purposes that are unrelated to the specific customer and the services used by that consumer. Indeed, they are using consumer financial data to build unrelated, for-profit products or services. We strongly support the CFPB's view in the PFDR that these are not allowable uses of consumer-permissioned data.

32. How prevalent is the licensure or sale of consumer financial data by bank and non-bank financial institutions where consent to license or sale is part of a standard user agreement or privacy notice?

Answer: See answer to Question 31.

33. What is the prevalence of licensure or sale of consumer data by companies with a fiduciary duty to their clients?

Answer: See answer to Question 31.

34. What estimates exist on the percentage of financial service platform users who actually read and/or understand user agreements and privacy notices in their entirety?

Answer: While JPMC operates under rigorous federal laws, regulations, and supervisory guidance governing disclosure requirements for financial services products, the same cannot be said for fintechs and their data middlemen service providers.

We are concerned about the disclosures by such market participants and whether their customers are reading them. The TCH study supports our concern—80% of users were not aware that data middlemen access their financial data and 78% didn't know that this access continues after the app is closed. *See* The Clearing House, Consumer Survey: Data Privacy and Financial App Usage, December 2021, *available at* *2021-tch-consumersurveyreport_final.pdf*. We believe that privacy disclosures and data use practices should be conspicuous, clear and transparent, and consumer consent for data use should be informed, specifically provided, and revocable.

Compliance Dates

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

Answer: Yes. It is incomprehensible that the industry—including banks of varying sizes—is marching towards complying with a rule that the CFPB itself says is unlawful. The CFPB should immediately suspend current PFDR compliance guidelines.

Any changes to the rule will require new compliance work. This rule is unique because it requires cooperation among banks, data recipients, and aggregators. Compliance timelines should allow all parties enough time to adapt, ensuring interoperability and standardization for safe, reliable data sharing. At least 24 months will be needed to comply with a revised rule.

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?

Answer: See answer to Question 35.