

Rohan M. Amin
Chief Product Officer

December 28, 2023

Comment Intake – Financial Data Rights
c/o Legal Division Docket Manager
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

Filed electronically at <https://www.regulation.gov> and by email at 2023-NPRM-Data-Rights@CFPB.gov

Personal Financial Data Rights Rulemaking, Docket No. CFPB-2023-0052; RIN 3170-AA78

Ladies and Gentlemen:

JPMorgan Chase & Co. (“JPMC”) appreciates the opportunity to comment on the Consumer Financial Protection Bureau’s (the “Bureau” or “CFPB”) Notice of Proposed Rulemaking on Personal Financial Data Rights.¹ Enabling customers to share their financial data offers them a powerful tool that facilitates innovation and competition.

JPMC commends the CFPB on the proposed rule to facilitate the adoption of standards that ensure safe, permissioned access to financial data. Unsafe data access practices, such as screen scraping, pose substantial risks to consumers and data providers,² including potential liability for unauthorized transactions in the event of a breach or misuse of data. At the same time, mis-calibrated regulation would impede data providers’ ability to protect their customers by adopting reasonable time, place, and manner risk management controls on third party access.

As both a leading data provider and recipient of permissioned data, we have extensive experience with the practical realities of enabling safe data sharing. We have made substantial investments to build a strong infrastructure that gives consumers convenience, privacy and security when they share their data. Today, we support secure data sharing for millions of JPMC customers, whether for budgeting, loan applications, or other use cases that improve our customers’ access to insights and diverse competitive offerings. We support over one billion third party API calls each month. And every month, thousands of JPMC customers engage with

¹ Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796 (proposed Oct. 31, 2023) (hereafter, “NPRM”).

the Security Center dashboard on our consumer portal to easily view, modify, or remove a permissioned third party's access (see Appendix 1).

Our goal with this letter is to share our learnings with the CFPB to guide the refinement of this regulation, for the benefit of consumers and the broader ecosystem.

This letter is organized as follows:

- **Part 1:** Comments on nine key regulatory issues [pages 3-27]
- **Part 2:** Additional detailed feedback on the NPRM [pages 28-58]

Part 1 | Comments on nine key regulatory issues

- I. Screen scraping**
 - II. Prohibition on fees**
 - III. “Information to initiate a payment to or from a Regulation E account”**
 - IV. Risk management and third party oversight**
 - V. Industry standards body**
 - VI. The important, distinct role of data aggregators**
 - VII. Consumer authentication and authorization**
 - VIII. Scope of data that must be shared**
 - IX. Secondary data use**
-

I. Screen scraping

➡ Credential-based data access and screen scraping are dangerous practices.³ Once a data provider has an API available, the Bureau should prohibit third parties from screen scraping and allow the data provider to block all screen scraping. Otherwise, third parties have the incentive and means to continue screen scraping, which harms data providers and puts consumers at risk.

The Bureau's proposed rule falls short of fully addressing the inherent risks of credential-based access and screen scraping. Data providers cannot end screen scraping on their own through blocking. Sharing data should not come at the risk of exposing consumers' log-in credentials or third parties gathering more consumer data than what is necessary to provide the customer's desired product or service. The Bureau should therefore:

1. Prohibit credential-based access and screen scraping by third parties once a data provider has enabled API access;
2. Explicitly acknowledge a data provider's right to block credential-based access and screen scraping traffic once they have a developer interface; and
3. Prohibit screen scraping by third parties for access to information not defined as covered data in the final rule.

Based on our experience, many data recipients will not voluntarily become authorized third parties and access data solely through APIs. Absent an explicit ban, we expect that some third parties will continue to attempt to access consumer data through screen scraping. Some third parties may believe consumer authorization entitles them to use credential-based access, or they may be unwilling to agree to reasonable risk management conditions a data provider establishes. Others may seek to access consumer portal functionality beyond the scope of section 1033 and intended solely for the customer (e.g., to send a Zelle payment). Third parties also may avoid using an API to evade regulatory requirements, such as those related to data use or data security.

In our experience, blocking screen scraping by evading third parties is costly, difficult, and imperfect. To avoid being blocked, evaders use sophisticated techniques commonly employed by fraudsters and hackers to deliberately evade our security controls. Some third parties deliberately manipulate their scripts to make scraping logins appear "human." Tactics include sending traffic from mobile device farms, sending traffic through rotating residential or mobile IPs, emulating biometric logins, manipulating web headers, and modifying scripts within hours when traffic is blocked. These behaviors are unsafe, unsound and completely unacceptable uses of technology and make it harder for us to protect our systems and safeguard customer data.

Attempting to distinguish and block screen scraping traffic from consumer traffic requires significant financial investment and sophisticated techniques. JPMC has spent millions of dollars on techniques and technologies to block evasive screen scraping. It is not practical or possible for

³ As the Bureau notes, screen scraping "may pose risks to consumers' data privacy and security" and "also presents risks to data providers" by straining information systems and exacerbating "concerns with respect to liability." NPRM, 88 Fed. Reg at 74799.

all data providers, particularly smaller entities with less technological sophistication, to block determined evaders. Even when a data provider is able to block screen scraping traffic, consumers are still at risk as log-in credentials still can be shared with a third party.

Evasive screen scraping traffic also has impacted the uptime and availability of our consumer-facing website. Our consumer portal has suffered from incidents where screen scraping traffic overloaded services on our consumer portal, triggered alerts, or caused some customers' digital profiles to be locked, creating real inconvenience and access delays for customers.

Finally, screen scraping should be banned completely and not simply with respect to *covered data* made available in the API.⁴ To do otherwise would severely undermine the stated goals of the CFPB as *all* consumer data could still be screen scraped and the underlying consumer risks associated with screen scraping would remain.⁵ Permitting screen-scraping in *any form* undermines the protections, privacy, accountability, and consumer control envisioned by this rule.

II. Prohibition on fees

➡ The CFPB should allow data providers to charge reasonable fees to third parties for enabling data access, just as many data aggregators charge fees today. Prohibiting data providers from charging fees lacks any basis in section 1033 and would unfairly conscript data providers into subsidizing the business models of for-profit entities that monetize the data they receive.

-
- A. Data providers will incur substantial ongoing expenses to comply with the rule and should be permitted to charge a reasonable fee to the commercial entities that will benefit from those investments.

The proposed rule takes an overly simplistic and narrow view of the underlying economics required to support a channel for customer permissioned data sharing and forces data providers to subsidize the business model for data aggregators and third parties. First, the CFPB erroneously focuses solely on the marginal costs of the developer interface, rather than reasonable fees that a data provider should charge that are benchmarked to the market. Second, there are significant upfront and ongoing costs that will be incurred to build and maintain a developer interface and ensure customers cash safely share their data. Third, by myopically

⁴ The CFPB should note that unfettered access through screen scraping could expose to authorized third parties information that is explicitly excluded from sharing under section 1033.221.

⁵ For example, if a third party accessed a customer's checking account data via a secure API and also screen scraped the same data provider to obtain additional data (which, in actuality, means getting unconstrained access to all the consumer's data), all of the underlying consumer risks associated with screen scraping will remain without the protections that arise from being an authorized third party.

focusing on the interface costs, the CFPB ignores the broader foundational business and infrastructure investments data providers must make on an ongoing basis, without which the data would not exist. A data provider cannot be expected to build and maintain services to enable third party access to customer data without accounting for the foundational investments upon which those services rely or the cumulative impact on the overall economics of providing banking services.

The upfront and ongoing costs⁶ that data providers will incur to enable third party data sharing under this rule are substantial and include:

1. *Technology costs*: software development, product management, production management, infrastructure costs⁷, analytics, and other personnel to support the developer interface;
2. *Cyber and security costs*: to protect customer data and secure interfaces;
3. *Third party risk management costs*: adapting to a (potentially large) number⁸ of third parties connecting directly and a potential increase in the scope of activities for third party oversight; and
4. *Operational, customer support, and third-party support costs*: enabling direct integrations, legal and compliance activities, addressing and resolving issues raised by customers and third parties, managing any data breach or fraud events, and complying with numerous operational requirements in the rule⁹

The prohibition on fees is contrary to the CFPB's stated objective to "ensure data providers make data available reliably, securely, and in a way that promotes competition"¹⁰ and instead creates market distortion, inhibits innovation, and forces data providers to transfer economic value to third parties and data aggregators without fair compensation. Accordingly, we urge the CFPB to eliminate the prohibition against charging fees in section 1033.301 and expressly provide that data providers can charge reasonable fees¹¹ to an authorized third party, or a data aggregator acting on behalf of an authorized third party, in connection with establishing or maintaining the

⁶ A large share of these costs are fixed and will need to be incurred by any size data provider. For example: conducting risk management, building API functionality, enabling and managing direct integrations, and protecting systems.

⁷ We disagree with the CFPB's assertion in the NPRM that the incremental costs from increased data requests are likely to be minimal on a per-account basis. Third party traffic cumulatively will account for a large share of a data provider's overall infrastructure costs and burden under this rule.

⁸ In the NPRM, the CFPB states that "the CFPB expects that, on average, large data providers will need to negotiate 10 or fewer additional data access agreements in the years immediately following implementation of the proposed rule, at a maximum cost of \$68,000 per large data provider." We strongly disagree with both the estimate on the incremental number of potential new direct connections and the total cost. This rule as drafted could lead to a large number of third parties seeking direct connectivity, and the costs for data providers to process these inquiries, establish contracts, and conduct appropriate third party risk management would be substantial.

⁹ Because of how the CFPB has structured the rule—namely, to leverage SSO standards that do not yet exist as "indicia" of compliance—it is unclear what the rule itself will require and thus what costs compliance will entail. Accordingly, the cost figures advanced by the CFPB could be even less accurate.

¹⁰ 88 Fed. Reg. at 74800.

¹¹ The underlying justification for the proposed fee prohibition is flawed. While the NPRM discusses the harms associated with unfettered discretion to set fees, it fails to adequately consider reasonably available alternative approaches to the fee prohibition, such as reasonable fees. The CFPB offers no explanation as to why it has not considered alternative approaches.

developer interface and receiving requests or making available covered data in response to requests.¹²

Data aggregators charge fees to third parties for enabling data access and for products derived from that data access, profiting from data providers' infrastructure and security investments. If data aggregators are permitted to charge fees to authorized third parties, there is no reason data providers should not likewise be permitted to charge reasonable fees.

The requirement that fees be "reasonable" should relieve the CFPB's concerns with excessive fees that effectively deny consumer access to information, create anti-competitive price discrimination, and delay access and compliance. Further, allowing data providers to assess reasonable fees ensures they can invest in data security, risk management and customer servicing. Otherwise, many data providers—especially those with fewer resources—will be unable to invest sufficiently in innovation and security, hampering progress and the customer experience.

While the CFPB acknowledges that the proposal does not prohibit generally applicable fees (like account maintenance fees¹³) charged to consumers, an increase in account maintenance fees is not the optimal way for data providers to adapt to the impacts of this rule. As a general principle, it's better when consumers are aware of, and can make choices about, the services they are paying for. An increase in account maintenance fees for all customers, regardless of their use of data-sharing services, does not accomplish this.

Notably, the principle of fair compensation for data providers is consistent with the Data Act proposed recently (in November 2023) by the European Parliament, which states that "[i]n order to promote continued investment in generating and making available valuable data, including investments in relevant technical tools, while at the same time avoiding excessive burdens on access to and the use of data which make data sharing no longer commercially viable, this Regulation contains the principle that in business-to-business relations data holders may request reasonable compensation when obliged... to make data available to a data recipient."

B. Section 1033 does not authorize the CFPB to prohibit data providers charging fees to third parties.

Nothing in Section 1033 supports the proposed rule's forced subsidization without fair compensation. Section 1033 provides that, "[s]ubject to rules prescribed by the Bureau," covered persons must make certain information "available to a consumer, upon request."¹⁴ The provision nowhere mentions fees, much less authorizes the CFPB to prohibit them. And while section 1022(b)(1) of the Dodd Frank Act provides that the CFPB "may prescribe rules ... as may be necessary or appropriate to enable the Bureau to administer and carry out the purposes and

¹² The CFPB and other regulatory agencies have recognized the need for financial institutions to charge reasonable and proportional fees for services that are rendered. See, e.g., Credit Card Penalty Fees, 88 Fed. Reg. 18906 (proposed March 29, 2023) (amending 12 C.F.R. pt. 1026); Regulation II, 12 C.F.R. pt. 235.3.

¹³ 88 Fed. Reg. at 74814 ("[T]he proposed rule would not address account maintenance fees that a data provider might charge to consumers regardless of whether they use the interface").

¹⁴ 12 U.S.C. § 5533(a)

objectives of the Federal consumer financial laws, and to prevent evasions thereof,”¹⁵ that general authorization to engage in rulemaking does not authorize the CFPB to promulgate an outright prohibition on fees. Had Congress intended these provisions to address fees, it would have done so, and the absence of any such language in section 1033 forecloses the agency from prohibiting fees in the final rule.¹⁶

In addition, compelling data providers to subsidize a third party’s business without fair and reasonable compensation raises serious constitutional concerns. By mandating the provision of free services or effecting a forced sale, the rule’s fee prohibition could amount to an uncompensated taking or a regulatory taking in violation of the Fifth Amendment.

III. “Information to initiate a payment to or from a Regulation E account”

➡ By mandating that data providers share “[i]nformation to initiate payment to or from a Regulation E account,” the CFPB is inappropriately leveraging section 1033 to require account providers to enable payments by third parties. This exceeds the agency’s statutory mandate and creates a host of significant risks and costs that the agency’s proposal fails to even address, much less adequately resolve. The CFPB should not unleash these risks into the payments ecosystem without undertaking a comprehensive review and update to the existing payments regulatory framework in coordination with prudential regulators.

-
- A. The initiation of payments moves the scope of the rule from data sharing to money movement, which presents a number of new risks and costs.

The payments ecosystem is complex with significant nuances across networks, types of transactions and constituents. The CFPB’s proposal ventures into regulating the payments ecosystem without proper consideration of the costs, interactions among participants, and significant risks this proposal would create.¹⁷ Requiring the sharing of payment initiation information will be a catalyst for significant growth of “pay-by-bank” models, a payment method that is ill suited, yet is increasingly being adopted, for many types of transactions like eCommerce purchases. The CFPB should drop the requirement to enable payments from the

¹⁵ id. § 5512(b)(1)

¹⁶ The Fair Credit Reporting Act, for example, requires consumer reporting agencies to disclose consumers’ credit information to the consumer upon request and “without charge.” Similarly, another provision of the Dodd-Frank Act requires creditors to provide copies of appraisals and valuations to loan applicants at “no additional cost.” The absence of any such language in section 1033 forecloses the agency from prohibiting fees in the final rule.

¹⁷ See, 12 U.S. Code § 5512(b)(2)(A) & (B) (requiring that the Bureau in its rulemaking consider the potential benefits and costs to consumers and the impact of the proposed rule on covered persons as well as consult with the appropriate prudential regulators regarding consistency with prudential, market, or systemic objectives administered by such agencies).

final rule and take steps to separately consider these complexities and nuances before embarking on regulating the payments space through its section 1033 rulemaking.

The regulatory framework surrounding money movement (including Regulation E) never contemplated, and does not fully account for, the new realities and multiple entities involved in payment transactions. Specifically, it does not fully account for data aggregators and third parties that directly engage with consumers to enable payments but may not have the same liability or responsibilities under Regulation E (and other relevant laws and regulations) to consumers as the account holding financial institution even where they are at fault. These parties also do not bear or assume the cumulative costs associated with engaging in dispute investigation, resolution, and customer reimbursements.

The proposed rule will lead to an increase in pay-by-bank transactions that will impose additional costs on covered persons relating to unauthorized or disputed transactions, a cost that is not justified by any potential benefits of the proposal. Even when data aggregators or third parties may bear responsibility for an unauthorized transaction, under current rules and regulations the consumer's financial institution must play the leading role in managing a consumer's expectations and inquiries and making the customer whole. Customers expect their financial institution to address unauthorized transactions and resolve transaction errors, even if a third party is at fault and regardless of whether those transactions are initiated through the financial institution or through a third party. Failure to engage consumers and cover those costs in advance exposes the financial institution to reputational and regulatory risk it cannot reasonably or fairly be expected to manage or control.

An increase in pay-by-bank transactions will impose other costs on covered persons and consumers. Data aggregators and third parties provide payment services without having to sufficiently invest in resources, staff and technology necessary to mitigate fraud risk, manage customer complaints, conduct investigations or resolve disputes. Nor do they have to make customers whole. For example, currently in situations where a customer reports an unauthorized transaction, the financial institution will undertake an investigation and, where it determines the cause is due to the third party, the financial institution will first make the customer whole (before trying to be reimbursed by the third party). Even if the financial institution is able to get the third party to reimburse it for the amount paid to the customer, this does not fully cover the totality of the costs associated with servicing the customer. This is a form of regulatory arbitrage that does not incentivize data aggregators or third parties to invest in necessary resources or tools that are required when engaging in money movement activities.

The CFPB errs in assuming that these novel risks can be addressed through rules outlined by private networks. Private network rules are limited in terms of the recoupment of losses caused by a third party or the allocation of liability among multiple parties, nor do they fully address customer servicing obligations and costs. To mitigate some of these risks, material improvements to consumer disclosures will be necessary to ensure consumers understand the heightened risks of sharing payment initiation information with data aggregators and third parties. The CFPB should require third parties to have appropriate resourcing and operations in place to manage consumer complaints, service customers, and investigate disputes, and the necessary capital and insurance to make the consumer whole. This underscores why section 1033 and the current

rulemaking are not appropriate vehicles for mandating the disclosure of information to initiate payments in section 1033.211(c). At the very least, if the CFPB retains this provision, given the increased consumer risks inherent in data aggregators and third parties providing payment services, the CFPB should also require these entities to compile, maintain and submit to the Bureau instances of unauthorized transactions and customer loss due to these activities. Additionally, anti-money laundering risk must be addressed by the appropriate regulators.

- B. Updating the existing payments regulatory framework is complex and will require a comprehensive assessment by the CFPB and coordination with the prudential regulators to ensure consumers are protected and risks are fairly allocated among participants.

The proposed rule under section 1033 is not the appropriate vehicle for the CFPB to go forward and mandate the sharing of information that enables money movement. Before regulating on this topic, the CFPB would need to fully address the risks and costs that would be imposed on financial institutions to ensure that liability follows the movement of the data. Data aggregators and third parties should be fully liable for the risks they create. The CFPB must involve the prudential regulators to address unsafe or unsound practices and directly supervise data aggregators and third parties that enable money movement.

The CFPB's rulemaking would need to clarify liability across participants under section 1033 and Regulation E by:

1. *Providing clarity with respect to the types of "means of access" that fall under the definition of an "access device" in 12 C.F.R. § 1005.2(a)(1) where such information is authorized by a consumer to be shared with a data aggregator or third party.* Since the CFPB specifically is directing data providers to share information that can be used to initiate payments, where such information is provided pursuant to that directive, payments should be considered authorized until such time as the consumer notifies the financial institution that the authorization is revoked.
2. *Requiring data aggregators and third parties to specifically disclose the nature of the authorized use of payment initiation information and whether such use includes acting as a service provider.* Regulation E apportions liability differently to the account holding institution depending on whether the transaction at issue involves a service provider. However, the liability apportionment regime in Regulation E is often difficult for account holding financial institutions to address; the account holding institution can be hampered in conducting a reasonable investigation as they may not have sufficient information to determine the role that a particular third party was playing in the transaction. To the extent the CFPB refuses to remove proposed section 1033.211(c) in the final rule, the CFPB should address this lack of clarity by adding a provision to the proposal pursuant to section 1033, requiring third parties to disclose in connection with the data request whether or not the third party will be acting as a service provider. The CFPB also should require clear, conspicuous and appropriate consumer disclosures by the financial institution and/or third party about their status and responsibilities.

3. *Provide that Data Aggregators should be considered “service providers” as defined in 12 C.F.R. § 1005.14(a) if they otherwise meet the definition of service provider even where the Data Aggregator may have an agreement with the account holding institution.* Presently, the definition of “service provider” under Regulation E is limited to entities that (i) do not hold the consumer’s account, (ii) issue a debit card or other access device that the consumer can use to access the consumer’s account held by a financial institution, and (iii) have no agreement with the account holding institution regarding such access.¹⁸ Data aggregators increasingly are entering into the provision of services beyond mere aggregation, including the provision of payments services. Accordingly, if the CFPB proceeds with proposed section 1033.211(c), it should ensure that data aggregators are held responsible for all Regulation E obligations and that they are not able to escape liability for unauthorized consumer payment transactions merely because they have a data access agreement with the data providing financial institution. Further, while it may be possible for financial institutions to address liability in their data access agreements, not all institutions will have that level of bargaining power and the ecosystem and consumers would benefit from a uniform liability standard.
4. *Provide, in the proposal, an indemnification mechanism.* If section 1033.211(c) is retained in the final rule, the CFPB should include a provision in any final rule noting that where (i) a financial institution/data provider is obligated to provide payment initiation information to a data aggregator or third party, and (ii) that information is used to initiate a payment, the financial institution will be indemnified for any claims brought by the consumer due to that transaction. Such a rule would allow the financial institution to seek recourse from the data aggregator or third party for any resulting unauthorized transactions due to their payment initiation.

C. The mandate to share information “to initiate payment” exceeds the scope of Section 1033.

Requiring data providers to make information available to facilitate payments from *any* account clearly exceeds the scope of the CFPB’s statutory authority. While Section 1033 requires data providers to provide information relating to “transactions” and “account[s],”¹⁹ it does not speak to payments, much less enabling third parties to initiate payments. The CFPB does not have authority to require a data provider to make available information that *must be usable by* third parties to leverage *services* provided by the data provider, including enabling payments.

Additionally, the CFPB should not require data providers to make available information to initiate payments from a Regulation Z credit card.²⁰ The CFPB has not fully considered the costs, risks, and benefits regarding making information available to initiate payments from any account types, including card accounts.²¹ These would include the appropriate designation of third parties as payment facilitators, the application of PCI obligations, the clear assignment of

¹⁸ 12 C.F.R. § 1005.14(a).

¹⁹ 12 U.S.C. § 5533(a)

²⁰ 88 Fed. Reg. at 74811.

²¹ 12 U.S. Code § 5512.

liability and consumer servicing responsibilities, and also would require reconciliation with the card network rules.

IV. Risk management and third party oversight

➡ The CFPB—not data providers—must be responsible for directly regulating and overseeing third parties and mitigating the risks that it is introducing through this rulemaking. At the same time, the CFPB should not constrain data providers’ ability to conduct appropriate third party risk management.

Through this rule, the CFPB is introducing substantial new risks by allowing thousands of unregulated third parties to gain access to vast amounts of sensitive financial data. The CFPB must take responsibility for directly regulating, supervising, and enforcing regulatory obligations that apply to third parties and data aggregators that receive data under this rule and for ensuring that third parties are held fully liable for any harm they cause across the data sharing ecosystem.

It exceeds the CFPB’s authority under section 1033 to shoulder data providers with an obligation to enforce third parties’ compliance with the regulation. It also poses significant practical challenges²² and Constitutional issues to make data providers or an industry body responsible for oversight and supervision. Such a delegation would be unsafe, unsound, and stifling to innovation and healthy competition. Data providers should never be in a position where a third party’s regulatory non-compliance raises regulatory scrutiny on the data provider.

The CFPB should: (1) place regulatory obligations directly on third parties; (2) ensure appropriate adherence to all regulatory requirements through regular examination and enforcement of data aggregators and third parties, (3) establish a level playing field of information security requirements for all parties that are not already supervised by federal prudential regulators, and (4) ensure third parties are appropriately liable, including for scams and fraud.

The CFPB must have an oversight and supervisory framework on third parties in place before any compliance date timeline begins to toll.²³ The CFPB has not made clear how it intends to achieve these ends, including supervision of data aggregators and authorized third parties.

1. The CFPB’s recently proposed “larger participant rulemaking” does not adequately address this issue. As proposed, that rule would expand the CFPB’s supervisory authority to cover roughly 17 large nonbank companies that offer general-use payment applications. According to the Bureau, this will allow them to enforce protections in the payments space “against unfair, deceptive, and abusive acts and practices, rights of

²² Beyond this being the CFPB’s responsibility, this would bring immense practical challenges. Even for a bank of JPMC’s size, assessing the compliance of thousands of third parties against each of their many obligations under this rule would be extremely difficult to implement.

²³ 88 Fed. Reg. at 74869 (proposed § 1033.121).

consumers transferring money, and privacy rights.” However, this proposal would not cover thousands of companies that receive and process data under section 1033, including large and small data aggregators or authorized third parties that do not offer payment services. Nor does it cover the full set of obligations on third parties under this proposed rule.

2. The NPRM explains the CFPB’s supervisory authority over third parties by adding section 1001.2(b), clarifying the definition of financial product or service to include “providing data processing product or services”. In doing so, the CFPB seeks to “ensure that activities involving consumers’ potentially sensitive personal financial information are subject to the CFPA and its prohibition on unfair, deceptive, or abusive acts or practices.” However, this is not sufficient to ensure that data aggregators and authorized third parties will be held responsible for the full extent of their obligations under this rule. Reliance on UDAAP enforcement alone is not sufficient in the absence of clear, affirmative compliance obligations and a comprehensive CFPB supervisory and enforcement program sufficient to cover all parties under this rule.
3. If the CFPB has another mechanism by which it intends to exercise direct supervisory authority and oversight on data aggregators and other third parties (as we feel is necessary), it should clarify in the final rule what that mechanism is.

At the same time, the CFPB must acknowledge that financial institutions have prudential safety and soundness requirements as data providers. Additionally, consumer data sharing creates real risks for data providers and their customers, which data providers must be able to manage.

As the CFPB is aware, the Office of the Comptroller of the Currency (“OCC”) and other federal financial services regulatory agencies have issued detailed guidance on third-party risk management.²⁴ The final rule should clearly state that nothing in the rule shall be interpreted to limit a data provider's obligation and discretion to comply with prudential safety and soundness requirements. Communicating this broadly to the market will ensure consistent understanding of the interplay between the final rule and prudential obligations, particularly for non-bank market participants less familiar with prudential regulatory obligations.²⁵

²⁴ See generally Fed. Rsr. Sys., FDIC, OCC, *Interagency Guidance on Third-Party Relationships: Risk Management*, 88 Fed. Reg. 37920 (June 9, 2023) (hereafter, “Interagency Guidance”).

²⁵ Advancing the benefits of open banking may impose significant risks to safe and sound banking, as OCC Deputy Comptroller Donna Murphy recently stated in Congressional testimony. Statement of Donna Murphy, Deputy Comptroller, Before the Subcommittee on Digital Assets, Financial Technology and Inclusion Committee on Financial Services, U.S. House of Representatives (December 5, 2023) at p. 7. Referencing the recently updated Interagency Guidance on Third Party Relationships: Risk Management Deputy Comptroller Murphy acknowledged that the OCC is “aware that advances in open banking will have implications for institutions of all sizes as well as for [the OCC’s] supervision of them. These implications may include liquidity risk from increased account portability; compliance risk; and operational risk, including cybersecurity risk and third party risk.” The testimony clearly and unambiguously underscored that banks are responsible to operate in a safe and sound manner and in compliance with applicable laws when engaging with third parties: “[t]he use of third parties has significant potential benefits, *but strong third party risk management is essential to avoid harm to consumers or weakening of bank safety and soundness.*” *Id.* (emphasis added).

While JPMC supports the CFPB’s recognition that a data provider can deny a third party’s access based on risk management concerns, it is important that the final rule not define eligible risk management concerns too narrowly and constrain a data provider’s discretion.

- The CFPB should remove the current requirement that to be reasonable, a data provider’s denial of a third party’s access must, at a minimum, be directly related to “a *specific risk of which the data provider is aware*, such as a failure of a third party to maintain adequate data security.”
- Data providers must be permitted to implement comprehensive and scalable risk management programs that anticipate and manage numerous potential risks that could materialize.
- Since financial institutions must manage all manner of risks, not just those related to data security, a data provider must have the ability to require data aggregators and authorized third parties to agree to certain, reasonably designed obligations related to risk management as a condition for access.²⁶ Agreement on such obligations can prevent harm to consumers, promote faster resolution for consumers when things do go wrong, and provide a mechanism for ensuring third parties take their obligations seriously. This is consistent with the prudential risk management obligations to ensure consumer protection applicable to financial institutions.
- As we discuss in the next section, this rulemaking must not impose constraints on how a data provider reasonably carries out third party risk management by obligating data providers to grant access to consumer data solely in reliance on standards or accreditation from an outside body that issues qualified industry standards.
- The CFPB also should not constrain an account provider’s right to deny access for reasonable risk management concerns on the basis that the third party itself is subject to direct supervision or enforcement by the CFPB or prudential regulators.

V. Industry standards body.

➡ An industry-led standards body can play an important role in the data sharing ecosystem. The final rule should allow flexibility for appropriate governance and narrow the role of industry standards body(s).

JPMC agrees with the principle that an industry-led body should play an important role in promoting interoperability and addressing technical details on how data sharing works. JPMC is a founding member of the Financial Data Exchange (FDX) and has worked closely with data aggregators, fintechs, other financial institutions, and consumer groups for the past several years

²⁶ These could include obligations related to data breach notifications, compliance with laws, adherence to minimum control requirements, cooperation to resolve customer issues that may arise, accepting liability for unauthorized transfers or data breaches, indemnification for harm resulting from these incidents, and obtaining adequate insurance as a backstop to ensure its financial capacity is sufficient to make whole the data provider for the liability the third party holds.

to share ideas, listen to diverse perspectives, and develop best practices. We can attest to the immense benefits that come from having subject matter experts work together on the complexities of defining interoperable, scalable standards for data sharing.

While JPMC broadly agrees with the characteristics the CFPB has laid out for a standard-setting body (with a few refinements below), the role for the standard-setting body should be limited to defining a data format and should not extend to establishing a “standard” for any other topics that go beyond explicit regulatory requirements.

The activities of a standard-setting body and the effect of any resulting standards must remain within constitutional limits. The Appointments Clause may be implicated if a standard-setting body exercises too much discretion in carrying out important executive functions on an ongoing basis. In addition, to the extent standard-setting bodies have decision-making power to create qualified industry standards that have the force of law in supervision or enforcement activities, they may constitute an improper delegation of federal regulatory authority to a private entity, especially if the CFPB, and not Congress, delegates such power.

A. The CFPB should balance the need for a “fair, open, and inclusive” SSO with the need for effective governance.

The NPRM provides that the decision-making power of a standard-setting body be “balanced across all interested parties, including consumer and other public interest groups, at all levels of the standard-setting body.”²⁷ Requiring a total “balance in power ... *at all levels*” of the standard-setting body may not be feasible; for example, the standard-setting body may have numerous specialized working groups and struggle to get participation from all constituencies in all working groups. Instead, the CFPB should require the standard-setting body to incorporate input from broad stakeholders into key decisions when setting standards.²⁸

Relatedly, the NPRM calls for “meaningful representation for large and small commercial entities within these categories.” There are a number of ways to ensure that diverse viewpoints are incorporated into decision making, while ensuring the entity’s governing body(s) do not become so large as to be unwieldy or unresponsive to business needs. For example, this could involve establishing transparent, deliberate processes for incorporating input and balancing the interests of large and small entities.

In addition, the NPRM places the majority of the responsibilities on data providers. Accordingly, the balance of the SSO and the framework for consensus-driven decision making must account for this dynamic, with the right checks and balances from the CFPB, to ensure that standards being set can reasonably be implemented. One constituency group should not be able to overrule and mandate adherence to a particular requirement that another impacted constituency (which

²⁷ 88 Fed. Reg. at 74869 (proposed § 1033.141(a)(2)).

²⁸ Balance of power in SSO governance may be difficult to achieve in practice *across all levels of the body*. Consumer groups and small entities have tended to struggle to have the bandwidth and expertise to engage meaningfully in some of the more detailed work of defining technical standards.

bears the obligation to comply, potentially at significant cost) collectively believes is not reasonable or feasible.²⁹

B. The final rule should narrow the role of industry standards body(s) to certain topics.

Areas where a standard-setting body is well-suited to create a qualified industry standard

JPMC agrees with the CFPB's proposal that data providers follow a qualified industry standard when it comes to "data format."³⁰ This helps to effectuate interoperability to support data sharing. The CFPB should clarify that the term "standardized format" includes a data model and a communication protocol for requests and responses for covered data to be exchanged.³¹

It may take some time after the final rule is published for a qualified industry standard for the "data format" to be finalized, and we agree with allowing reasonable flexibility for data providers in the interim as provided in section 1033.311(b)(2). That said, a practical challenge with this subsection, as drafted, is that any given data provider may not be able to ascertain what constitutes "a format that is widely used by the developer interfaces of other similarly situated data providers." The specific formats used by peer institutions may not be publicly available information, and they may differ in minor ways. A more reasonable requirement would be to require that "in the absence of a qualified industry standard, the data provider must make *commercially reasonable* efforts to *broadly conform* the data format of the interface to a format that has been widely used by other data providers with respect to similar data and is readily usable by authorized third parties."³²

Areas where a standard-setting body is not well-suited to create a qualified industry standard

Beyond the development of a standard "format," the proposed rule outlines other areas where conformance to an industry standard would be an "indicia" of compliance. These include:

²⁹ The requirements for "balance in power" should not result in a situation where non-data provider constituencies can dictate unreasonable obligations on data providers without any guardrails, over-ruling the collective view among data providers on what is reasonable and achievable. This is important given that the majority of the "standards" proposed in the regulation are obligations on data providers, with heavier costs to be borne by that constituency than other constituencies. We view the CFPB's focus on "consensus" to be an important principle to address this dynamic.

³⁰ The CFPB should clarify that a qualified industry standard format (on, for example, the data model) could include one "standardized format" or multiple "standardized formats" where reasonably needed and appropriate. For example, as the industry standard data model is updated over time, it may be reasonable for data providers to adapt their developer interfaces to match a recent version but not necessarily the most recent version of that data model. This balances continuous innovation, reasonable cost containment, and the goal of promoting general interoperability.

³¹ Clarifying the definition of "format" will also help avoid SSO scope creep into impermissible areas. For example, if the industry body interprets "format" too expansively it could bleed into forcing data providers to adopt certain schemes for authentication, data security, or authorization that run contrary to a bank's risk management principles, technological capabilities, or vendor integrations. Keeping the definition of "format" focused is also a suitable way to balance the tradeoffs that come from mandating standardization. Mandating a standardized format may increase costs for data providers as they adapt their (diverse) systems, and this cost may increase to the extent that "format" is defined more broadly to include additional aspects of how the developer interface operates.

³² While the existing FDX data model used by many data providers today likely will not fully conform to the scope of the final rule, it could serve as a baseline for broad conformance according to this guideline.

- downtime notice and total amount of scheduled downtime³³
- performance of the developer interface (including response rate and latency)
- revocation method
- frequency of access (caps)
- accuracy (including the data provider's policies and procedures regarding accuracy)
- third party accreditation / security standards (including security and risk management standards as a basis for denying third party access)
- the third party's new authorization request, and
- the third party's policies and procedures regarding accuracy.³⁴

There are several challenges that arise from having a standard-setting body endeavor to define standards for these topics.

1. These activities tend to be in the spirit of regulatory enforcement which exceeds the scope of an SSO
2. Standardization in many of these areas does not bring any interoperability benefit (e.g., for policies and procedures, internal methods of ensuring accuracy). Moreover, to attempt having thousands of companies agree on a single way of doing things in these areas across the industry will be difficult, more so than a single data format. Even if agreed upon, aligning to a single standard will add significant compliance costs by requiring ecosystem participants to align (and maintain alignment) with these standards, with limited interoperability benefits.
3. Many of these topics (API uptime, access frequency, etc.) are not “standards” in the sense of choosing one sensible solution (among many) in the spirit of promoting interoperability. Rather, defining requirements in these areas involves value judgments as to whether one constituency (e.g., data providers) is obligated to perform costly activities, where the benefits may largely accrue to other entities (e.g., third parties). These are not areas that an industry standards body is particularly well suited to adjudicate.³⁴

³³JPMC notes that the CFPB has already dictated a proposed minimum performance level for API performance in the NPRM diminishing the need for an SSO to do so. NPRM, 88 Fed. Reg. at 74871 (proposed § 1033.311). For the industry to reach consensus on a single standard that provides more specificity on other issues would be difficult given the diversity of different systems, processes, and tech stacks that exist among 10K+ data providers and 7K+ third parties, the unique needs of particular third parties, and the varying risk management frameworks that will apply.

³⁴ To give one example: data aggregators and authorized third parties may have a strong incentive to push the industry body to adopt requirements on data providers that are overly onerous, unreasonable, or costly for data providers to implement, while third parties bear none of these costs. This could include, for example: unnecessarily high access caps, unreasonably high API uptime requirements, unreasonably onerous data provider notice requirements, unreasonable restrictions on security dashboard features, unreasonably low standards for data security, or unreasonably narrow conditions under which access can be denied to a third party. This does not mean that a standards-setting body could not play a valuable role in these areas to provide helpful information and transparency that guides industry participants in improving their services. For example, a standard-setting body could publish white papers or facilitate idea sharing. On API performance, the standard-setting body could provide a utility to capture and publish developer interface performance statistics. This information sharing could speed adoption of secure interfaces, but it is different from the industry trying to align around a single “standard” on these topics that industry participants then feel pressured to adopt as a matter of regulatory compliance.

4. Specifically as it pertains to risk management and security standards, as discussed in detail above, the CFPB must be responsible for regulating and conducting ongoing oversight of the data aggregators and third party recipients. Data Providers must also retain the right to conduct independent third party risk assessments, in line with their prudential requirements.

There may be merits to an independent entity that conducts some activities—such as developing a standard risk questionnaire—that data providers can use as an input in the vetting of third parties’ security and data controls.³⁵ However, data providers must not be required to rely solely on such external inputs as a full replacement for comprehensive third-party risk management. Prudential third party risk management requirements are not transferable to third parties.

VI. The important, distinct role of data aggregators

➡ Data aggregators will continue to play a critical role in the data sharing ecosystem. Accordingly, the CFPB must clearly define the role and responsibilities for aggregators, including how they will be held accountable for data security, privacy, collection, and data use; how consumer authorization should be captured by them; and the actions they take as intermediaries.

While the rule may simplify some aspects of an authorized third party connecting *directly* to a data provider, it will remain too costly and impractical for each data recipient to build the connective infrastructure into thousands of data providers individually.³⁶ Therefore, the vast majority of authorized third parties likely still will choose to connect via a data aggregator.³⁷

As such, data aggregators should be subject to no less—and arguably more—oversight and direct, clear requirements than other parties in this ecosystem. They will hold and process the most consumer data of any party, making them attractive targets for hackers. The manner in which data aggregators operationalize authorization flows and processes could impact thousands of third parties. Given this expansive role, it is crucial that the final rule provide clarity on how

³⁵ Banks collaborated to develop the TruSight TPO assessment, which consolidates common data security questionnaire elements to simplify some components of third party security assessments.

³⁶ For example, even with a standardized data format in place across data providers, data aggregators can still make it much easier for third parties to access data from different sources. Data aggregators play a role in routing traffic to different endpoints, streamlining the end-to-end customer experience, offering a single integration point, handling downtime notices, and other dimensions of enabling data sharing.

³⁷ Because this rulemaking adds many new specialized requirements on data providers and third parties, the cumulative result may be *an increase* in the market power, influence, and volume of data sharing facilitated by data aggregators, which may be able to provide some outsourced compliance solutions to authorized third parties.

these important actors in the data sharing ecosystem will be regulated. Specifically, the proposed rulemaking should be clarified as follows.³⁸

1. *Direct obligations for, and oversight of, data aggregators.* As discussed above in Section IV, the CFPB should place affirmative regulatory obligations directly on data aggregators in section 1033.431, and compliance should be assessed through regular Bureau examinations, supervision and enforcement.³⁹ It is not sufficient to rely primarily on oversight by other parties (like consumers, authorized third parties, or data providers).

Currently, the rule provides only a tenuous mechanism for holding data aggregators accountable by requiring them to comply with certification obligations (section 1033.421), then imposing the responsibility for ensuring data aggregator compliance on authorized third parties (section 1033.401(a)), and then ultimately assuming that authorized third party compliance will be confirmed by data providers (section 1033.331(b)(iii)). This accountability framework places too much of the burden of overseeing data aggregator compliance on authorized third parties – most of whom are significantly smaller and have fewer resources than data aggregators and accordingly are not well positioned to police data aggregators’ activities.

The CFPB’s recently proposed “larger participant rulemaking” also does not adequately address this issue. The proposal expands CFPB supervision to roughly 17 large nonbank companies that offer general-use payment applications, but would not cover thousands of companies that receive and process data under section 1033, including large and small data aggregators or authorized third parties that do not offer payment services.

The NPRM clarifies the CFPB’s supervisory authority over third parties by adding section 1001.2(b), clarifying the definition of financial product or service to include “providing data processing product or services.” However, this is not sufficient to ensure that data aggregators and authorized third parties will be held responsible for the full extent of their obligations under this rule. Reliance on UDAAP enforcement alone is not sufficient in the absence of clear, affirmative compliance obligations and a comprehensive CFPB oversight sufficient to cover all parties under this rule.

If the CFPB has another mechanism by which it intends to exercise direct supervisory authority and oversight on data aggregators and other third parties (as we feel is necessary), it should clarify in the final rule what that mechanism is.

³⁸ In doing so, the CFPB should be mindful that in some instances a single company may play the role of both authorized third party for some consumers/services but as data aggregator for other consumers/services; the rights and obligations on that company should be clearly separated based on the role being played.

³⁹ In Section 1033.431(b), the CFPB says that data aggregators “must comply with paragraph (c) of this section”, which in turn requires that “the data aggregator must certify to the consumer that it agrees to the conditions on accessing the consumer’s data in § 1033.421(a) through (f).” This means that a data aggregator has an obligation to certify to the consumer that it will follow all the obligations in 1033.421(a) through (f); however there appears to be no actual *direct regulatory* obligation on data aggregators to comply. The CFPB should, instead, state in 1033.431(b) that that a data aggregator must comply with 1033.421(a) through (f) and the condition in § 1033.421(h)(3) upon receipt of the notice described in § 1033.421(h)(2).

2. *Identifying data aggregators and downstream parties.* The CFPB should modify section 1033.331 to clarify that a data provider should be able, as a condition for responding to a data request, to require receipt of information sufficient not only to authenticate “the third party’s identity” but also, in the case of a data aggregator being used, to identify both the data aggregator and those third parties on whose behalf they are acting. This is essential to enable the data provider to efficiently and accurately conduct appropriate risk management and provide transparency to consumers on who is accessing their data.
3. *Data provider and data aggregator relationship.* The CFPB should give data providers flexibility to work with and through data aggregators, as intermediaries, to operationalize frameworks for holding downstream parties accountable, rather than being expected to hold downstream parties accountable directly.

As a general practice, data providers will continue to deal directly with data aggregators as intermediaries acting on behalf of thousands of authorized third parties. It may not be practically feasible for a data provider to deal independently (for example, to establish terms for liability) with thousands of downstream parties accessing via a data aggregator. Likewise, we anticipate that data recipients also will see the benefits of consolidated dealing via a data aggregator with numerous data providers.

Accordingly, data providers should be able to establish bilateral contracts with data aggregators that collectively address the individual obligations and responsibilities of both downstream parties and the aggregator itself. Given the lack of contractual privity between data providers and authorized third parties when a data aggregator is used, bilateral contracts with data aggregators—including pass-down requirements that flow to third parties—allow data providers to address important items like liability and data security at downstream third parties.

4. *Data provider rights.* The CFPB should make clear in the final rule that a data provider’s right to deny access based on reasonable risk management concerns applies not only to authorized third parties, but also to data aggregators. If a data aggregator has lax security practices, for example, then it is not safe for a consumer’s data to be shared with and stored by that data aggregator.
5. *Clarify the aggregator’s role in capturing authorization.* We have several recommendations for how the CFPB should clarify the respective roles that a data aggregator and an authorized third party play in capturing authorization. These are included in Part 2 of this letter [see pages 55-58]
6. *Data use by aggregators.* When a company is acting as a data aggregator (i.e., enabling data sharing connectivity to a downstream authorized third party), their activities should be constrained to what is necessary to play that role as an intermediary.

Most consumers do not understand the role that data aggregators play or intend for data aggregators to be accessing or using their private financial data for any purposes beyond facilitating access. Accordingly, when acting in the role of a data aggregator, a third party

should not be allowed to collect or use data for any purposes beyond what is needed to enable the authorized third party to provide its product or service to the consumer. For example, a data aggregator should not use data it collects when acting as an intermediary to create its own commercial products or services that are then sold to unrelated parties. [See additional JPMC comments on Data Use further below in Part 1, at pages 25-26.]

VII. Consumer authentication and authorization

➡ Data providers must retain the ability to authenticate the consumer and capture authorization directly from the consumer. Some of the CFPB’s proposed requirements for authorization mechanics—including related to data categories, authorization scope, account selection, dashboards, and third party disclosures—should be modified to make the rule workable at scale and to maximize consumer transparency and control.

JPMC supports the CFPB’s position that data providers must authenticate the consumer and the third party and that data providers must be allowed to collect authorization directly from the consumer. Any dilution of these rights will inhibit data providers from protecting consumers and offering consumers helpful tools (such as a data provider dashboard) to control access to their data.

Requiring consumers to *authenticate* directly with the data provider ensures that the data provider can directly manage against the risk of a bad actor gaining access to the consumer’s sensitive financial data. Consumers should authenticate with the data provider *every time* they authorize a new connection or expand the scope of an authorization, to ensure appropriate security to protect access to sensitive account data. It is not sufficient for only the third party or a data aggregator to authenticate the consumer when the consumer’s authorization is being set or modified, without any authentication with the data provider, as the data provider would be obligated to rely on a third party’s authentication and security protocols.

Relatedly, in cases where a data aggregator is accessing data on behalf of multiple authorized third parties, the data provider should be allowed to require consumer authentication and authorization for each separate authorized third party connection before making covered data available. By contrast, if the consumer only authenticated with the data provider when connecting the *first* downstream application but not for any subsequent third parties connecting through that same data aggregator, the data provider would not be able to ensure it is actually the customer who is giving the relevant authorizations.

With respect to consumer *authorization*, JPMC strongly maintains capturing authorization from the consumer cannot solely be the domain of data aggregators or authorized third parties. Some may argue, for example, that centralizing the capture of data authorization solely in the hands of a single party (for example, a large data aggregator) could allow for greater consistency in how authorization is obtained across numerous data providers. However, this model forces data providers to rely on third parties to know with confidence exactly what the consumer has

permitted. A better way is for data providers to confirm authorization directly with the consumer, which is aligned to FDX standards and is well tested in the marketplace. This model promotes consumer transparency, security, and accurately scoped data sharing.⁴⁰ We also agree with the CFPB's proposal to allow data providers to provide dashboards that give consumers control over their data sharing connections. Many consumers expect to be able to manage their data sharing connections directly with their account provider.⁴¹

One notably important change we recommend pertains to the CFPB's expectations for data providers to verify that a third party has met its obligations (e.g., regarding disclosures). Under proposed section 1033.331(b)(1), "a data provider must make available covered data when it receives information sufficient to: Authenticate the consumer's identity; Authenticate the third party's identity; *confirm the third party has followed the authorization procedures in § 1033.401*; and (iv) Identify the scope of the data requested."⁴² The italicized portion of the proposed text should be modified to clarify that a data provider has the *right but not the obligation* to "confirm the third party has followed the authorization procedures in § 1033.401." It is not feasible for each data provider to confirm every third party has complied with all of its authorization procedure obligations under section 1033.401. Such obligations are extensive, and it would be impossible for every data provider to audit and approve the lengthy Terms and Conditions documents of thousands of third parties.

In several other important areas, the NPRM's requirements for how authorization works should be modified to be feasible to implement at scale and to maximize consumer control. We discuss these in Part 2 of this document (see pages 43-45).

⁴⁰ Many consumer benefits are made possible by the data provider collecting authorization from the consumer directly. These include:

- *Enabling customer transparency and control:* When a data provider captures authorization from the consumer, the data provider holds a copy of the specific authorization the consumer has granted in its own system of record, alongside authorizations across all third parties. This record makes it possible for data provider to give consumers real-time transparency and control over where their data is being shared. We do this through the Security Center dashboard on JPMC's website and mobile app and when customers call a JPMC call center (see Appendix 1). By contrast, under a model where authorizations are solely captured by numerous third parties, JPMC would need to rely upon the authorization records held at those myriad third parties to be able to enable such transparency and control tools. Relying upon and staying in sync with authorization records across numerous external systems of record could be difficult to build and maintain.
- *Enabling accurately scoped data sharing:* By capturing the scope of authorization directly from the consumer, the data provider can efficiently share only the data that the consumer has authorized. By contrast, under a model where authorizations are only captured by third parties (who may define data scopes very differently or unclearly), it may be challenging for the data provider to design API endpoints that enable it to accurately honor requests for data with widely varying (or potentially ill-defined) scopes.

⁴¹ Thousands of JPMC customers use our Security Center dashboard and appreciate the control, transparency, and convenience it provides. See Appendix 1.

⁴² 88 Fed. Reg. at 74871 (proposed § 1033.311(b)).

VIII. Scope of data that must be shared

➡ JPMC is partially aligned with the CFPB's proposal around the scope of data that must be shared. The CFPB should modify the scope relating to terms and conditions, rewards, and bill payment information as these are overly burdensome to share, lack clear consumer benefit, or go beyond the scope of the CFPB's authority to require.

JPMC supports sharing a broad set of data elements. We appreciate that the CFPB has thoughtfully incorporated industry feedback from the SBREFA process in many areas with respect to covered data elements that are reasonably needed to support common use cases, while balancing considerations of privacy and feasibility.

We recommend the following changes to the required “covered data” that must be shared.

1. *Terms and Conditions.* The CFPB should narrowly tailor the type of data to be shared within the category of Terms and Conditions. We support the CFPB's requirement to share certain data elements regarding the terms of an account, such as APY, APR, and realized fees, as these are finite and comparable across similar accounts and reasonably fall within what is prescribed under section 1033. However, other data the NPRM includes in this category (e.g., applicable fee schedule, rewards program terms, whether a consumer has opted into overdraft coverage, whether a consumer has entered into an arbitration agreement, and the undefined term “Terms and Conditions” in general), go beyond section 1033 and do not fall into “costs, charges and usage data.”⁴³

Notwithstanding the CFPB's lack of statutory authority to require sharing this type of data, this requirement is operationally troublesome for several reasons:

- (a) Terms and conditions often do not reflect a consumer's actual costs related to that account; sharing realized fees provides a better reflection of true account costs to consumers. For example, a bank or card issuer may offer refunds, waivers, or reversals based on certain conditions. These conditional items would not be appreciated from bare account terms, but are reflected in a consumer's actual, realized fees and can significantly impact the total consumer costs or benefits.
- (b) It is not feasible to provide Terms and Conditions “data” in a manner that is finite or easily comparable for consumers. Sentences and paragraphs that explain the terms of an account cannot be reduced to discrete data elements without losing important context.
- (c) Account agreements are multi-page documents with paragraphs of text. If a third party pulled these documents regularly (e.g., daily, as a PDF), it would be very taxing on the data provider's infrastructure. These types of files are orders of magnitude more taxing to transmit than structured data elements. Further, it is unclear how a third party could make use of lengthy Terms and Conditions documents, which are not standardized across institutions. We also have not heard

⁴³ 12 U.S.C. § 5533(a). This section requires covered persons to share, “information relating to any transaction, series of transactions, or to the account including information about the customer's use of and interaction with the account.” Broad requests for account terms pulled from customer agreements go beyond the intent of the statutory language.

any consumer demand to be able to share this type of information via developer interface with third parties.

- (d) Documents change regularly, and the ongoing compliance and technology costs to operationalize accurate extraction of individual data elements from such documents would be significant with little benefit to the consumer.

2. *Rewards*. The CFPB should revise the definition of covered data in proposed section 1033.211 to require only sharing rewards balance. The CFPB includes “rewards credits” and “reward program terms” within the definition of “covered data” in proposed section 1033.211. Rewards *balance* is the data element that is commonly shared today.

Information such as “reward points per transaction” should be excluded as confidential commercial information.⁴⁴ For data providers, reward points per transaction may be the output of a proprietary algorithm used to classify individual merchants into reward point categories.⁴⁵ Additionally, sharing this information ultimately can harm consumers by eroding incentives for data providers to invest in merchant categorization tools that provide convenience and accuracy for consumers that use card products.

3. *Bill Payment Information*. The CFPB should revise proposed section 1033.211 to *exclude* information about third-party bill payments scheduled through the data provider and instead require (as the proposed rule already does) data providers to share information about *already-settled bill payment transactions*.

- (a) Information about scheduled bill payments can contain information about billers/payees (and, in many cases, information a consumer provides to the data provider). This is not information about a transaction, series of transactions or the consumer’s account with the data provider and, therefore, is not within the scope of section 1033.
- (b) Information about third-party bill payments scheduled through the data provider includes confidential commercial information. Often, bill pay services are underpinned by a component purchased from a service provider, such as eBill payment. That service has the bank ingest the bill from the biller (receiving this information through a vendor, with content owned by the biller) to present to the bank’s mutual customer.
- (c) Scheduled bill pay information regularly contains highly sensitive information about the consumer’s accounts at other companies, such as full credit card number at another institution or full account number at a utility company (e.g., Verizon Wireless). It is not appropriate for this information to be shared with third parties without the underlying account provider (e.g., Verizon, or my credit card issuer) having visibility or involvement.

⁴⁴ 12 U.S.C. § 5533(b)(1)

⁴⁵ The CFPB should also prohibit data aggregators and authorized third parties from using covered data to reverse engineer confidential commercial algorithms or pricing models of data providers. Without a specific prohibition, data recipients could use covered data to indirectly obtain the confidential information that 12 U.S.C. § 5533(b)(1) was intended to protect.

Instead, requiring (as the proposed rule does) data providers to share information about *already-settled bill payment transactions* provides much of the benefit the CFPB seeks, without the attendant problems.

IX. Secondary data use

↳ We support the CFPB’s proposal to curtail targeted marketing, cross-selling, and sale of data as secondary uses of data shared with third parties. We offer additional suggestions for how the rule can further protect consumers against harmful uses of data.

We strongly support the CFPB’s determination that targeted advertising, cross-selling of other products and services, and sale of data “are not part of, or reasonably necessary to provide, any other product or service” in the context of third parties using consumer-permissioned data obtained under section 1033.

There are a number of unique aspects of the consumer permissioned data sharing ecosystem that warrant limits on secondary data use (including prohibiting entities from getting opt-in / opt-out consent), particularly as it relates to targeted advertising, cross-selling of other products and services, and sale of data.

- The ecosystem of third parties receiving consumer-permissioned data under this rulemaking consists of thousands of companies that are not subject to direct regulatory supervision and enforcement on an ongoing basis to govern their disclosures (e.g., to be sufficiently clear, distinct, and conspicuous), data use (ensure use is in line with disclosures) and privacy practices (ability for customers to revoke consent in an easy manner) equivalent to the financial institutions disclosing the data.
- Many third parties that collect consumer-permissioned data do not have a sustained relationship with the consumer, but may gain access to a consumer’s entire account history solely in service of a one-time transaction.
- There are often other intermediaries involved in the process of sharing data that a customer may not realize are getting access to their data.

The CFPB in its rulemaking has not made clear the regulatory oversight and supervision framework for third parties and aggregators. As a result, it is prudent to prohibit secondary use of data in the context of third parties using consumer-permissioned data obtained under section 1033.

To further enhance consumer protections, JPMC recommends that the Bureau strengthen section 1033.421(a)(1)-(2) as follows.

1. *Explicitly prohibit the sale of data.* The CFPB should separate 1033.421(a)(2)(iii) and explicitly prohibit a third party from selling covered data—including de-identified covered data—to another entity *under any circumstances*. Entities should not be able to

avoid the rule's obligations on authorized third parties by simply buying the data from another company. The risks to consumers from such sale of data are significant, including the lack of appropriate safeguards around risk management, data security, oversight, traceability, and liability on entities that purchase such data,⁴⁶ and loss of consumer trust that they are in control of their data. Any rule that allows for resale of data would need to mandate appropriate data handling by, and provide for adequate oversight of, data purchasers.

2. *Clarify the permitted scope of data collection.* The CFPB should make clear that authorized third parties are prohibited from *collecting* more data than is reasonably necessary to provide the *core product or service* requested by the consumer. Specifically, the scope of data collected from a data provider should be narrowly tailored to enable the consumer's core service, not broadened to serve other third-party secondary uses such as product development.⁴⁷
3. *More fully scope targeted advertising and cross-selling.* The CFPB should amend section 1033.421(a)(2)(i)-(ii) to cover general "marketing activities." While we interpret the existing NPRM terms "targeted advertising" and "cross-selling" to fall under "marketing activities", the term "marketing activities" will more comprehensively capture the types of activities that warrant appropriate limitations on use.
4. *Clarify limitations on use by other parties.* When a company is acting as a data aggregator, vendor, subcontractor, or agent on behalf of an authorized third party, that party must not be able to use data collected or processed in that capacity for any targeted advertising, marketing activities or cross-selling. We urge the CFPB to clarify this in the final rule.
5. *De-identified data.* The restrictions the CFPB has proposed with regard to use of data for targeted advertising, cross-selling, and sale of data should also apply to de-identified data in this context. Until there exists legislated standards for de-identification, with appropriate oversight mechanisms applicable to non-GLBA governed third parties, the risk of re-identification and consumer harm justifies prohibiting certain secondary uses and sale.

⁴⁶ The NPRM does not address oversight and accountability mechanisms to ensure sold data is not used for other, impermissible purposes.

⁴⁷ For example, if a consumer links their account to a third party app to use a budgeting tool, the third party should not be able to collect additional data beyond what's needed to enable the budgeting tool, for its use in developing new products.

In summary...

JPMC supports and understands the value of consumer permissioned financial data sharing. Our goal is to ensure that our customers know with certainty what information they are sharing and with whom, and that they are sharing it securely. We strongly support our customers' ability to access financial data and to have full control and visibility in sharing it securely with the third parties they choose.

The CFPB's final rule implementing section 1033 should be predicated on the use of secure developer interfaces that ensure that consumers will give explicit consent to share their financial information while protecting their username and password. Customers should be able to give, and data providers should be able to capture, explicit consent for third parties to use specific data from specified accounts. Customers also should be able to easily revoke access for each account and each third party at any time without friction or delay.

Moreover, the CFPB should bear the responsibility for, and clearly define in the final rule, how it will regulate and supervise data aggregators and third parties before the final rule is implemented. Data aggregators and third parties must be subject to continuous supervision and all regulatory obligations, including data handling, data use, and cybersecurity standards equivalent to those applicable to financial institutions to protect customers' sensitive financial information. Data Providers should not be responsible for oversight and supervision of data aggregators and third parties.

JPMC supports the CFPB's efforts to finalize this first instalment of rulemaking on section 1033. The effort to improve data sharing and increase competition should be phased, deliberate and unrushed, with full engagement of prudential regulators to appropriately address safety and soundness concerns, particularly with respect to payments. This will enable the financial services industry to fully deliver on the promise of safe data sharing that will benefit consumers for years to come.

Sincerely

Rohan M. Amin

Rohan Amin
Chief Product Officer, Chase

Part 2 |

Additional Detailed Feedback on NPRM

Below, JPMC offers additional comments on specific sections of the proposed rule.

Quotations from the proposed regulatory text are shown in blue, followed by JPMC's comments relating to the text.

§ 1033.111 Coverage of data providers.

(b) *Definition of covered consumer financial product or service.* Covered consumer financial product or service means a consumer financial product or service, as defined in 12 U.S.C. 5481(5), that is:

- (1) A Regulation E account, which means an account, as defined in Regulation E, 12 CFR 1005.2(b);
- (2) A Regulation Z credit card, which means a credit card, as defined in Regulation Z, 12 CFR 1026.2(a)(15)(i); and
- (3) Facilitation of payments from a Regulation E account or Regulation Z credit card.

(c) *Definition of data provider.* Data provider means a covered person, as defined in 12 U.S.C. 5481(6), that is:

- (1) A financial institution, as defined in Regulation E, 12 CFR 1005.2(i);
- (2) A card issuer, as defined in Regulation Z, 12 CFR 1026.2(a)(7); or
- (3) Any other person that controls or possesses information concerning a covered consumer financial product or service the consumer obtained from that person.

JPMC Comment: The current definition of data provider is problematic. The Bureau should instead define a data provider as a company that provides a covered financial account or service directly to a consumer (i.e., is the financial account provider), and exclude the third component of the definition (i.e., “any other person that controls or possesses information concerning a covered consumer financial product or service the consumer obtained from that person.”)

Relatedly, in 1033.111(b), the CFPB should remove from the definition of “covered consumer financial product or service” the third component of “facilitation of payments from a Regulation

E account or Regulation Z credit card.” Instead, the CFPB should directly state that a digital stored-value wallet account is also a covered financial account.

The principle underlying these recommended changes is that when a company provides a financial account (such as a Reg E account) to a consumer, the consumer will generally expect that account provider to protect the data and will look to that company when something goes wrong (e.g., with a payment or account information compromise). Furthermore, prudential regulators expect account providers to protect data on the accounts they provide. If another company (like a digital wallet, data aggregator, or payment processor) possesses information about the account (by virtue of consumer permissioning, payment facilitation, or otherwise), such data should not be able to be shared onward (with *those* companies acting as the “data provider”) without the underlying *account provider* being involved. Otherwise, the account provider will lack visibility into downstream data access and find itself unable to manage risk, address any potential harms or issues, or adequately provide transparency and control to the consumer through the data provider’s customer control dashboard about who has access to their information. The consumer may also be left confused about where their data has been shared from and where and how to terminate sharing.

Consumers (who typically do not know the mechanics of how data sharing works) expect their underlying account provider to protect their data and actively assist if something goes wrong. Consumers will be confused and frustrated if their account provider can’t help them as expected and instead must refer them to one or more downstream parties (such as payment processors or wallets) to deal with the problem.

From the current definition of a “data provider”, it may be unclear to market participants what the CFPB means by a “*service* the consumer obtained from that person”. It should be made clear that if the “service” a company provides to the consumer is a service involving *display of information* about that consumer’s *accounts at other covered institutions*, those other accounts are not in scope for what the company would share (though it possesses this information). A company should only be allowed and obligated to share data pertaining to the financial *accounts* it provides to the consumer directly; it should not be sharing data pertaining to accounts offered by other companies.

The CFPB should also clarify that the obligation on digital wallets to share data applies only to sharing covered data about the digital wallet provider’s own *stored-value accounts*. The consumer should *not* be able to permission from a digital wallet their data pertaining to a covered account provided by another company, which may also be displayed to the consumer in that digital wallet.

The obligation to share data should not apply to pass-through wallets that do not provide *stored-value financial accounts* to consumers. That is, when a digital wallet is acting as a “pass-through” wallet (e.g., Apple Pay today), account and transaction details pertaining to a linked account (e.g., Bank A card data) should not be shared by the digital wallet to an authorized third party. The consumer should always be prompted to authorize sharing their data about a covered account directly from the company that provides that underlying account (Bank A, in this case),

not from any downstream party like a wallet, a data aggregator, payment processor, or an authorized third party that has obtained access to that data.

By contrast, the obligation to share data with consumers and authorized third parties *should* apply to *stored-value* digital wallet accounts (for example, like those offered by Venmo and Cash App today). In this case, the stored-value *account* is offered directly by the digital wallet provider and no other institution, so consumers should be able to share information pertaining to that account from the digital wallet provider.⁴⁸

§ 1033.121 Compliance dates.

A data provider must comply with §§ 1033.201 and 1033.301 beginning on: (a) Approximately six months after the date of publication of the final rule in the Federal Register, for depository institution data providers that hold at least \$500 billion in total assets and non-depository institution data providers that generated at least \$10 billion in revenue in the preceding calendar year or are projected to generate at least \$10 billion in revenue in the current calendar year.

JPMC Comment: The CFPB should extend the date by which the largest institutions must comply as data providers to at least 24 months from finalization of the rule because the current timeline is not feasible. As a data provider with extensive experience providing customers access to their accounts through a developer interface, JPMC views the CFPB's required first compliance date for 6 months (after publication of the final rule) to be unreasonably short. Below, we lay out four important factors to consider in setting compliance dates.

Data Provider work to comply:

At JPMC, we have a sizable team (of engineers, product managers, analytics, design, legal, and other support functions) that is dedicated full time to building and maintaining our program to enable safe permissioned sharing of JPMC customer data with third parties. We estimate that it would require this team at least two years to come into compliance with the regulation as we currently understand the requirements of the NPRM, while keeping our developer interface running in the meantime (to avoid disruptions for our millions of customers who use it every month).

Even the largest data providers like JPMC will need to do extensive work to modify their API platforms and programs to comply with these new rules. For example, some of the largest data

⁴⁸ Here are two examples to illustrate the difference between stored-value and pass-through wallets. (1) If Oscar connects his Bank1 credit card to his PassThruWallet, then transactions on his Bank1 credit card may be visible in his PassThruWallet. However, those transactions do not involve PassThruWallet as an actual account provider, and authorized third parties should not be able to obtain access to this Bank1 data from PassThruWallet, but only from Bank1. This helps ensure Bank1 can conduct appropriate risk diligence on companies accessing Bank1 data. (2) By contract, if Oscar connects his Bank1 deposit account to HoldWallet, he may transfer \$100 from Bank1 to his HoldWallet account. The next day, Oscar initiates a \$25 payment transaction from his HoldWallet stored value account to another party (e.g., a merchant or a friend). This transaction involves HoldWallet as a counterparty of the transaction. Oscar should be able to share information about his HoldWallet account (e.g., balance = \$75) and his HoldWallet account transactions (e.g., \$25 payment) to an authorized third party.

providers would need to do significant work to: enhance public-facing websites to meet the NPRM’s requirements around public disclosure of required information; generate and publish performance metrics that meet the CFPB’s new definitions; enable support for required data elements they don’t already share (e.g., including bill payment data, certain terms and conditions); develop and operationalize the policies, procedures and processes required under this rule; potentially upgrade underlying technology infrastructure substantially to meet API performance standards as currently defined; potentially build new functionality pertaining to “machine readable” files accessible by consumers, depending on requirements in the final rule; appropriately manage consumer impacts of the new maximum access duration requirements; operationalize a process for providing notices on developer interface denials; build and operationalize third party notifications for consumer access revocations; adapt customer servicing operations to account for the new scope of activities and functionality; perform robust testing to ensure a safe and resilient implementation of new functionality; adapt current data access agreements; significantly adapt third party oversight processes; and implement numerous other requirements in the rule. Giving sufficient time to implement is essential to enable data providers to meet their obligations accurately, reliably, safely, and with necessary controls and compliance in place.

Alignment with industry standards:

The challenge with a six-month timeline is compounded by a critical dependency: some of the industry standards mentioned by the CFPB do not yet exist, and they will not exist until qualified industry body(s) are recognized and publish such standards. To meet the CFPB’s goal of promoting standardization and to benefit from the significant industry work done to date, the CFPB should recognize that substantial work needs to be done after final rulemaking for a standard-setting body to adapt governance, develop new capabilities, hold balanced and inclusive discussions to decide upon recalibrated standards, adapt documentation, and to create, operationalize and scale certification schemes. It will take time to fold the final requirements of the rule into a set of compliant standards for ecosystem participants to adopt; conformant standards will not be available prior to (or even immediately after) the final rule is released.

It would be more constructive for the industry if this standard-setting work can be completed before the largest data providers and all data aggregators and data recipients go about the extensive work of adapting their platforms and programs to the new rule. That way, the ecosystem can benefit sooner from the efficiencies and interoperability benefits that conformance to industry standards provide. This sequencing will also help to avoid ecosystem participants being required to build once to meet a short implementation timeline then rebuild or adapt their platforms soon afterward when an industry standard is finalized. Not only would that be costly but also potentially disruptive to consumers.

Interplay with third party readiness:

Extending the compliance date is also supported by the need for *data recipients* and *data aggregators* to have time to adapt their practices to comply with these new rules.

At JPMC, we have a sizable cross-functional team dedicated to enabling the import of consumer-permissioned data from other institutions (i.e., with JPMC acting in the role of authorized third party). We roughly estimate that this existing team would require over a year to come into compliance with the rule's obligations for authorized third parties, many of which are incremental to common industry practice today and/or would require extensive coordination with our data aggregator vendor (who would also need time to build and operationalize significant changes to comply). If the first compliance date is not extended, we and other data recipients would be at significant risk of failing to meet the required obligations in time to qualify as an "authorized" third party and therefore could lose access to data from the largest data providers.

Broadly, if data providers are forced to be ready before other parties in the ecosystem are ready and compliant, then the mismatch could disrupt access to data under the current rules. Section 1033.121 puts compliance dates on data providers but does not put obligations directly on data aggregators or authorized third parties to comply with their obligations by a certain date. The lack of compliance dates for third parties creates an incentive for third parties to screen scrape as long as possible, or to remain non-compliant with parts of the regulation to the extent they can get away with it. While the CFPB has said (though not made explicit in the proposed regulation) that data providers have a right to block screen-scraping attempts, this enforcement mechanism should not be overly relied upon for reasons we describe above.

If the CFPB puts obligations *directly* on data aggregators and third parties and assigns compliance dates to each, it would help the industry to collectively move toward the CFPB's desired future state more quickly and efficiently while reducing operational risk. As it stands under the NPRM, a third party's status as an "authorized third party" hinges on meeting certain criteria, which seemingly would be verified by each data provider in deciding whether to enable access to that party. While elements of this construct make sense, it also presents a problem for large data providers when it comes to the first 6-month compliance date. If there is no target date by which the universe of data recipients must comply, then each data provider must independently assess each authorized third party's readiness and compliance. Given the massive volume of data sharing already happening today on APIs between numerous data providers and thousands of third parties, a lack of calibration between data provider and third party compliance dates could create a "cliff" that would materially disrupt the flow of data and thereby harm consumers.

If a third party is not compliant by the CFPB's required compliance date for the data provider, then that third party may lose access to data from that source. If this is the intent, the CFPB needs to consider in setting the compliance date for the largest data providers not only the feasibility of those large data providers being able to comply in time, but also the feasibility of all current data recipients (including thousands of small companies) being able to come into compliance with their own new extensive obligations on the same timeframe.

Awaiting clarity from the CFPB:

Finally, the CFPB's final determinations on the roles and responsibilities of various parties in the ecosystem is another significant dependency for data providers to come into full compliance. We expect that the CFPB's review of comments received in response to this NPRM will result in

modifications that appear in the final rule. Data Providers cannot reasonably move forward in confidence to adapt their processes and platforms before having clarity on the final rules. For example, a data provider will need clarity around the specific obligations it has with respect to authorization management, third party oversight, and the respective roles, obligations, and oversight of data aggregators and third parties. As discussed above, these are all topics that require significant clarification or modification by the CFPB in the final rule.

§ 1033.131 Definitions.

For purposes of this part, the following definitions apply: *Authorized third party* means a third party that has complied with the authorization procedures described in § 1033.401.

JPMC Comment: The CFPB should clarify that the obligation on data providers to make covered data available to authorized third parties only applies if the authorized third party is domiciled within the United States. This will ensure that the third party is subject to relevant requirements mentioned throughout this rule (e.g., GLBA or FTC Safeguards, for data security) and to appropriate regulatory supervision. Expecting data providers to share data with non-US-domiciled companies, who may be subject to different privacy or data protection laws, could substantially undermine customer protections and complicate matters of risk management or liability.

Relatedly, the CFPB also should clarify that the obligation to share data with third parties does not apply to *consumers* who are domiciled outside of the United States. Mandating data providers to enable data sharing for such persons may trigger laws or other obligations in other jurisdictions, in a way that conflicts with obligations or assumptions underlying this rule. If US-domiciled data providers provide Reg E, Reg Z, or digital stored value accounts to non-US-domiciled consumers, foreign requirements for data protection and privacy will be triggered, impacting data handling and protection that vary widely across countries.

* * *

Consumer means a natural person. Trusts established for tax or estate planning purposes are considered natural persons for purposes of this definition.

JPMC Comment: In section 1033.131, a consumer is defined as a “natural person.” We agree that this definition of consumer is an appropriate and necessary definition. A consumer should not be defined to include any agent of the consumer. If it did, substantial confusion would ensue in terms of the rest of this rulemaking, as there are arguably numerous parties that could be acting as agents of the consumer in the process of transmitting and collecting permissioned data. These parties play different roles and should bear different responsibilities, so it is appropriate the CFPB has named them as distinct from the consumer.

To the extent that the CFPB wants to include “trusts established for tax or estate planning purposes” within the definition of consumer, the CFPB should clarify how it envisions these

parties authorizing the sharing of data. Data Providers should not be obligated to share data with such parties without proper authentication and authorization.

§ 1033.201 Obligation to make covered data available.

(a) *Obligation to make covered data available.* A data provider must make available to a consumer and an authorized third party, upon request, covered data in the data provider's control or possession concerning a covered consumer financial product or service that the consumer obtained from the data provider, in an electronic form usable by consumers and authorized third parties. Compliance with the requirements in §§ 1033.301 and 1033.311 is required in addition to the requirements of this paragraph (a).

JPMC Comment: In section 1033.201, the CFPB should make it clear that regardless of how third parties use covered data (including when third parties, or their subcontractors or intermediaries, are consumer reporting agencies and are generating consumer reports with the consumer-permissioned data), the CFPB does not intend to create a framework where data providers would be deemed furnishers under the Fair Credit Reporting Act when they provide data to consumers (including through third party data recipients) pursuant to the consumer's request.

§ 1033.211 Covered data.

Covered data in this part means, as applicable...

Information to initiate payment to or from a Regulation E account.

Example 1 to paragraph (c): This category includes a tokenized account and routing number that can be used to initiate an Automated Clearing House transaction. In complying with its obligation under § 1033.201(a), a data provider is permitted to make available a tokenized account and routing number instead of, or in addition to, a non-tokenized account and routing number.

JPMC Comment on Tokenized Account Numbers:

To protect safety and soundness and to promote greater consumer control, data providers should not be obligated to share untokenized account numbers with third parties and should have the option to make available tokenized account and routing numbers (TANs). We broadly encourage banks to adopt tokenization of account numbers as a way to protect consumers and the broader financial system. At JPMC, we enable consumers to share a tokenized account number with third parties; this provides several security and control benefits to consumers, while minimizing disruptions to their financial life.

- JPMC TANs allow our customers to see, through a dashboard on the bank website, which third parties they have stored TANs with and turn them off easily, at any time, without needing to close their deposit account. When an untokenized account number is stolen/compromised, the impact can be widespread because that single number is often used for numerous purposes. By contrast, separate TANs are issued to each different authorized third party, lessening the effects of a compromise.
- TANs can be quickly suspended or replaced without requiring changes to the underlying deposit account; this makes it easier for consumers and banks to respond to potential breaches without the hassle of shutting down the account.
- In the event of fraud or a breach, TANs could be used to enable better traceability to the source of the problem (e.g., a breach at a particular company) because separate TANs are uniquely issued to specific companies.

By contrast, the sharing and storage of non-tokenized deposit account numbers among thousands of third parties can create major risks for consumers. Such a practice can make third parties a major target for data breaches. Notably, large data aggregators today may store deposit account numbers for tens of millions of consumers spanning thousands of financial institutions. Theft of an untokenized deposit account number can harm consumers when a breach does occur. For one, such theft can contribute to ACH fraud, costing time and worry for the consumer to remediate. Theft of an untokenized deposit account number may also require a consumer or their bank to close the compromised deposit account and open a new one to prevent unauthorized transactions. This can create a substantial inconvenience and disruption in the consumer's financial life. In such instances, the consumer may need to replace their debit card on file with merchants; get new checks; re-route their direct deposit; identify auto-debits and update their account information across numerous payees; work with various companies to ensure critical payments like rent or utilities are not disrupted; and take additional actions to reconfigure their new account.

* * *

(d) Terms and conditions.

Example 1 to paragraph (d): This category includes the applicable fee schedule, any annual percentage rate or annual percentage yield, rewards program terms, whether a consumer has opted into overdraft coverage, and whether a consumer has entered into an arbitration agreement.

(e) Upcoming bill information.

Example 1 to paragraph (e): This category includes information about third party bill payments scheduled through the data provider and any upcoming payments due from the consumer to the data provider.

JPMC Comment: See, Part 1 at pp. 23-24 for detailed comments on this section.

(f) Basic account verification information, which is limited to the name, address, email address, and phone number associated with the covered consumer financial product or service.

JPMC Comment: We support the scope of the NPRM’s requirements on basic account verification information being limited to the name, address, email address, and phone number associated with the covered consumer financial product or service. This appropriately balances consumer privacy, data provider implementation costs and feasibility, and supporting common beneficial use cases.

JPMC Comment: (on section 1033.211 more broadly)

The CFPB has also requested comment on whether additional specific data fields should be named within the proposed rule. Aside from the comments we have given on specific elements elsewhere in this letter, the proposed categories of information provide the right level of guidance while also preserving sufficient flexibility for market participants to fill in the details, including through collaboration at an industry standards body.

The CFPB also requested comment on whether and how the rule should require that data providers make available historical data for other categories of information, such as account terms and conditions, and whether such historical data are kept in the ordinary course of business today. This should not be included as mandatory information that should be shared; it could be confusing to the consumer, would involve significant cost and complexity for data providers to make available, and would be of questionable use to third parties.

§ 1033.301 General requirements.

(a) *Machine-readable files upon specific request.* Upon specific request, a data provider must make available to a consumer or an authorized third party covered data in a machine readable file that can be retained by the consumer or authorized third party and transferred for processing into a separate information system that is reasonably available to and in the control of the consumer or authorized third party.

Example 1 to paragraph (b): A data provider makes available covered data in a machine readable file that can be retained if the data can be printed or kept in a separate information system that is in the control of the consumer or authorized third party.

JPMC Comment: We encourage the CFPB to clarify what it means by “machine-readable file” that can be accessed and retained by a consumer. While the NPRM commentary states that the CFPB does not see this obligation as creating a substantial incremental burden beyond what data providers commonly do today, the actual regulatory text could be understood otherwise and thereby create a major, costly new burden for data providers.

This obligation could be interpreted to mean making the covered data available to consumers via the consumer portal, where (for example) such information may be viewable on several different

pages of a website which the consumer could print out (on paper, or saved as a PDF file). If this would suffice to meet the obligation, the CFPB should clarify it as such.

On the other hand, this requirement could be interpreted to mean that data providers must create a new, single, downloadable file that holds *all of* the covered data, along with a means for consumers to download such a file. The incremental cost to build this would be large and extend well beyond the work required to share covered data via the developer interface.

- Data providers do not generally provide this type of file today.
- At JPMC, we do allow customers today to download monthly statements in PDF form and to download files containing *some* covered data (e.g., card transaction history), but these are much narrower in scope than what the CFPB may be requiring here.
- Also, the benefits do not outweigh the heavy costs to enable and support this. Consumers can generally find their covered data directly on the consumer portal.
- If data providers were to be required to generate separate dedicated files containing all of the covered data, those files would not be in standardized formats across data providers, making it difficult for consumers to use them in other machine applications.

§ 1033.311 Requirements applicable to developer interface

(c) *Performance specifications.* The developer interface must satisfy the following performance specifications:

(1) *Commercially reasonable performance.* The performance of the interface must be commercially reasonable.

(i) *Quantitative minimum performance specification.* The performance of the interface cannot be commercially reasonable if it does not meet the following quantitative minimum performance specification regarding its response rate: The number of proper responses by the interface divided by the total number of queries for covered data to the interface must be equal to or greater than 99.5 percent.

* * *

(D) A proper response is a response, other than any message such as an error message provided during unscheduled downtime of the interface, that meets all of the following criteria:

(1) The response either fulfills the query or explains why the query was not fulfilled;

* * *

(3) The response is provided by the interface within a commercially reasonable amount of time. The amount of time cannot be commercially reasonable if it is more than 3,500 milliseconds.

(ii) *Indicia of compliance.* Indicia that the performance of the interface is commercially reasonable include that it:

- (A) Meets the applicable performance specifications set forth in a qualified industry standard; and
- (B) Meets the applicable performance specifications achieved by the developer interfaces established and maintained by similarly situated data providers.

JPMC Comment: At JPMC, our existing developer interface for third party data access is a critical priority channel for serving our customers, just as our consumer portal is. We believe strongly that high performance and uptime in this channel benefits consumers. We have spent the past several years modernizing and optimizing our developer channel in the pursuit of high performance levels.

We invest significant resources to make this possible. We have product, engineering, production management, analytics, and other personnel that are focused on building and enhancing the performance and the reliability of our third party portal. And just as with our consumer portal, our third party channel adheres to a set of firmwide controls for systems stability, technology change management, and incident and problem management.

It is with this posture and practical experience running a developer interface that we recommend the following to the CFPB:

1. Modify the requirement that the response time on every data request must be under 3,500 milliseconds in order for that request to be considered a “proper response”. At JPMC, we have invested heavily over several years in creating, modernizing, and maintaining high quality APIs with fast response times to serve our developer interface. While our *average latency* is below 3,500 milliseconds, a significant percentage of our API responses take longer than 3,500 milliseconds. For example, sending a larger payload (e.g., when there is an especially lengthy transaction history, or when a customer has a large number of accounts) can require a much longer response time. Additionally, we put extra encryption on sensitive personal identifying information (like name and address), and that encryption process can lengthen the response time. Accordingly, a better minimum performance requirement would be to require the *average* latency of all responses to be under a certain threshold, rather than requiring *every response’s latency* to be below a certain threshold to be valid. Additionally, the CFPB should clarify that latency should be defined to exclude internet or network time, which is not within the data provider’s control.
2. Set modestly less stringent minimum thresholds for latency and uptime when it pertains to *customer-not-present* data refreshes. The vast majority of third party data access requests are recurring (e.g., daily) “background” refreshes by the third party, where the customer has not prompted the refresh and is not waiting for the data to show up. Accordingly there is less of a pressing need for this data to be returned quickly, and third parties can retry failed refreshes without impacting the consumer. In the future, some data providers may want to set up their technology in a way that prioritizes the fast delivery of API responses to customer-present pulls. This compromise could significantly help data providers manage their overall traffic loads so they can optimize consumer data access across human and third party channels.

3. Clarify the definition of response rate. Today, the CFPB defines the response rate as the “number of proper responses by the interface divided by the total number of queries for covered data to the interface”. In turn, a “proper response” is defined in part to include a requirement that “the response either fulfills the query or explains why the query was not fulfilled.” The CFPB should clarify that this requirement applies to when an authorized third party sends a request for specific covered data *after* the consumer has completed the process for authenticating and authorizing access. This authentication and authorization process is not a “query for covered data” per se, but a set-up step that precedes such data queries. In this set-up step, the consumer may need to type in their username and password, which can take much longer than 3.5 seconds.
4. Amend the definition of “response rate” so that measured response rates are not distorted by repeated “retry” attempts. Presently, the NPRM defines the response rate as the “number of proper responses by the interface divided by the total number of queries for covered data.” In the event of a short, unexpected outage in a data provider’s developer interface, third parties may repeatedly and automatically retry sending the same data access query (e.g., dozens of times) until they get a successful response, dramatically inflating the volume of failed requests and painting a worse picture of the interface’s performance (under this measurement definition) than is warranted.
5. Maintain some elements of the current definition of “proper response”, namely that (1) a proper response is a response that either fulfills the query or explains why the query was not fulfilled; and that (2) any responses by and queries to the interface during scheduled downtime for the interface must be excluded from the calculation. A response explaining why the query was not fulfilled should be considered a proper response because there are many instances when a query cannot be fulfilled by the data provider (e.g., if the request was malformed or for an account or data element not currently authorized for sharing by the consumer). Additionally, data providers must be able to have reasonable scheduled downtime to maintain and upgrade their systems.
6. Modify the minimum uptime performance requirement so that it applies to a 3-month rolling lookback window, rather than (for example) a one-month lookback period. Hitting a high threshold *every month* could be very challenging even for a diligent data provider. If there is a channel outage (which happens in technology), even if a team is rapidly deployed to diagnose the issue, develop a patch and deploy a fix within 48 hours, hitting a high threshold in a 30-day period is very difficult. Additionally, hitting a high performance threshold *every month* makes it harder for smaller institutions processing a low number of requests to weather any hiccups. Measuring average performance over a longer period (such as 3 months) can help smooth out these idiosyncrasies while still maintaining accountability for strong overall performance.
7. Remove the statement that “indicia that the performance of the interface is commercially reasonable include that it: (1) Meets the applicable performance specifications set forth in a qualified industry standard.” The CFPB has already set minimum performance standards in the rule. We do not view an industry standards body as being particularly well suited to reach a consensus view on an alternate standard for uptime or latency than

what the CFPB has already mandated. Instead, the industry standards body could provide a single utility to capture and publish developer interface performance statistics across the industry. This would be an effective means of promoting transparency and encouraging performance.

8. Remove the statement that “indicia that the performance of the interface is commercially reasonable include that it... (2) Meets the applicable performance specifications achieved by the developer interfaces established and maintained by similarly situated data providers.” It is impossible for 100% of data providers to meet this requirement. By definition, if there are 100 companies that are “similarly situated”, then half of those companies will have performance below the median of the group. The aforementioned recommendation to have an industry body gather and publish comparable performance stats across data providers is a more pragmatic way of promoting transparency and comparison.

* * *

(2) *Access cap prohibition.* Except as otherwise permitted by §§ 1033.221, 1033.321, and 1033.331(b) and (c), a data provider must not unreasonably restrict the frequency with which it receives and responds to requests for covered data from an authorized third party through its developer interface. Any frequency restrictions must be applied in a manner that is non-discriminatory and consistent with the reasonable written policies and procedures that the data provider establishes and maintains pursuant to § 1033.351(a). Indicia that any frequency restrictions applied are reasonable include that they adhere to a qualified industry standard.

JPMC Comment: An SSO should not be involved in setting standards for access frequency, to which data provider conformance is an indicia of regulatory compliance.⁴⁹ We urge the CFPB to strike the final sentence of this subsection and solely keep to the existing language requiring data providers to not act unreasonably with regard to limits on access frequency. This balances the needs of authorized third parties, while also giving data providers room to reasonably protect their systems as needed. Otherwise, there is a risk that access frequency standards are set so unreasonably high as to cause outages that crowd out consumer or third party traffic.

The requirement on third parties in section 1033.421(a)—to only access data as frequently as needed for the beneficial purpose the consumer authorized—is appropriate but not sufficient to protect against the risk of excessive third party traffic causing outages that harm consumers. Some third parties could subjectively interpret the frequency that is “needed” to include dozens (or more) customer-not-present refreshes per day for each authorized connection. It is imperative

⁴⁹ The CFPB has limited authority over prohibitions on frequency restrictions on data requests and responses. Section 1033(a) provides that covered entities must make certain information available “upon request.” This provision envisions a discrete affirmative act (i.e., making a “request”) on the part of the consumer or third party before information is made available. It does not envision an ongoing, automated demand and continuous, automated responses. To the extent authorized third parties use automated requests to demand continuous responses via developer interfaces, they do not meet the terms of the statute and, thus, data providers are not required to respond to them. By extension, the CFPB lacks authority to do more than prohibit unreasonable frequency restrictions by covered entities.

that data providers not be put in a position where consumer or third party access is threatened because the data provider is unable to put any protections in place. We believe a “reasonableness” standard around access frequency is appropriate.

The cumulative infrastructure burden of third party traffic under this rule will be large, variable, and potentially unpredictable. If third parties begin programmatically sending very high frequency requests to data providers (e.g., hourly refreshes), the cumulative digital infrastructure load on a data provider (inclusive of traffic to both the consumer portal and developer interface, which commonly rely upon the same underlying digital infrastructure) could increase multi-fold. This incremental load could be very costly to support and go far beyond any offsetting reduction in infrastructure strain from a reduction in screen-scraping.

The CFPB requested comment on whether the final rule should include a presumption that access caps are unreasonable unless undertaken for a period only as long as necessary to ensure a third party request does not interfere with the receipt of and response to requests from other third parties accessing the interface. We do not support this position. A data provider must be able to comprehensively manage the current and projected cumulative burden on shared digital infrastructure from both consumer portal traffic and third party traffic. This can be complex, and data providers must have flexibility to design reasonable processes to protect their systems and prevent outages.

* * *

(d) *Security specifications—(1) Access credentials.* A data provider must not allow a third party to access the data provider’s developer interface by using any credentials that a consumer uses to access the consumer interface.

JPMC Comment: We support the CFPB’s position that tokenized screen-scraping should not be allowed, as it does not mitigate many of the inherent risks associated with screen-scraping including a lack of consumer control over which data is collected.

Additionally, we support the CFPB’s stance, as mentioned in the NPRM commentary, that the CFPB is not proposing to require that data providers permit screen scraping as an alternative method of access, such as to address unavailability when the data provider’s system interface is down for maintenance. We agree that screen scraping presents risks to consumers and that relying on screen scraping as a “fall-back” access method would be unsafe. It would also complicate the mechanics of data access with respect to authentication and authorization procedures for data providers. If a consumer creates an API-based, secure data connection one day, then is prompted by a third party to establish a screen-scraping-based data connection the next day (for example, during a temporary planned or unplanned API outage at the same data provider), all of the benefits that come with the secure access method—including consumer transparency, control, security, and privacy—will go away the minute that the “fall-back” scraping happens. This practice would make it very difficult for data providers to protect consumers, protect their systems, and provide transparency to consumers about who has access to their data.

§ 1033.321 Interface Access

(2) *Reasonable Denials.* To be reasonable pursuant to paragraph (a) of this section, a denial must, at a minimum, be directly related to a specific risk of which the data provider is aware, such as a failure of a third party to maintain adequate data security, and must be applied in a consistent and non-discriminatory manner.

JPMC Comment: As discussed at length in Part 1 (topic IV) of this document, the CFPB should strike the requirement that any denial be “directly related to a specific risk of which the data provider is aware” from section 1033.321(b). This standard for denying access to sensitive information is too narrow and unreasonable. There is a range of risks that covered entities should be able to assess in deciding whether to deny access, but might not be able to under the “specific risk” formulation of the proposed rule.

* * *

(d) *Denials related to lack of information.* A data provider has a reasonable basis for denying access to a third party under paragraph (a) of this section if:

(1) The third party does not present evidence that its data security practices are adequate to safeguard the covered data, provided that the denial of access is not otherwise unreasonable; or

(2) The third party does not make the following information available in both human readable and machine-readable formats, and readily identifiable to members of the public, meaning the information must be at least as available as it would be on a public website:

(iv) Contact information a data provider can use to inquire about the third party’s data security practices.

JPMC Comment: In section 1033.321(d)(2)(iv), the NPRM indicates that a third party would be required to make available to a data provider “Contact information a data provider can use to inquire about the third party’s data security practices.” A third party should not be required to provide (for example) a phone number that is readily available to the public where any outside party can inquire about security practices. Information about security practices is confidential and in some cases highly confidential. In the wrong hands, such information could compromise the third party’s data security. Only subject to strict, legally enforceable confidentiality provisions should a company be expected to divulge sensitive information about its security practices to another entity.

§ 1033.331 Responding to requests for information.

(a) *Responding to requests—access by consumers.* To comply with the requirement in § 1033.201(a), upon request from a consumer, a data provider must make available covered data when it receives information sufficient to:

- (1) Authenticate the consumer’s identity; and
- (2) Identify the scope of the data requested.

JPMC Comment: Building off our comments above in Part 2 relating to section 1033.301 (pages 36-37) (regarding “machine-readable” files for consumers), we recommend that the CFPB add a clarifying example to this paragraph providing that a data provider responds to a consumer request appropriately if it authenticates a consumer using its standard consumer portal authentication processes and provides navigation to covered data within its consumer portal in a printable or downloadable form.

Absent such a clarification, it is unclear if data providers have an obligation to create (1) a new type of file or (2) a new way of identifying “the scope of data requested” by the consumer. Data providers do not have in place today a way to (1) capture from the consumer a “scope of data requested” and then, somehow, (2) generate (for example) a bespoke, machine-readable file that is available for download by the consumer, matching the scope of data requested. Enabling this would be complex and costly.

* * *

(b) *Responding to requests—access by third parties.*

(1) To comply with the requirement in § 1033.201(a), upon request from an authorized third party, a data provider must make available covered data when it receives information sufficient to:

- (i) Authenticate the consumer’s identity;
- (ii) Authenticate the third party’s identity;
- (iii) Confirm the third party has followed the authorization procedures in § 1033.401; and
- (iv) Identify the scope of the data requested.

(2) The data provider is permitted to confirm the scope of a third party’s authorization to access the consumer’s data by asking the consumer to confirm:

- (i) The account(s) to which the third party is seeking access; and (ii) The categories of covered data the third party is requesting to access, as disclosed by the third party pursuant to § 1033.411(b)(4).

JPMC Comment: The following proposed revisions would make the NPRM’s authorization requirements more workable at scale.

1. *Data Categories.* The CFPB should revise proposed section 1033.331 to make it more practical for data categories to work across the ecosystem. Specifically, where the proposed rule says, “the data provider is permitted to confirm ... the categories of

covered data the third party is requesting to access, as disclosed by the third party”, the CFPB should clarify that the data provider can reasonably require authorized third parties to use *standardized categories* when submitting the request for data. Such standardized categories could be defined by an industry standards body. Absent such use of standardized data categories, it would be practically impossible for data providers to satisfy (potentially thousands of) different permutations of data requests presented. Data providers need to be able to build their API endpoints around standardized, pre-configured categories of data. Otherwise, overcollection of data (e.g., by data aggregators) will be the likely outcome, as there will be no match between the scope of data requested and the ability of the data provider to respond to that exact scope.

2. *Authorization scope.* The CFPB should revise the proposed rule to allow data providers to confirm the scope of authorization along other dimensions (beyond accounts and data categories, as currently proposed). First, the data provider should be permitted to ask the customer to confirm the *companies* that will receive the data, including the authorized third party and any data aggregator[s] (as relevant). Second, the CFPB should leave room for collecting other dimensions of the authorization. For example, the industry may continue to innovate and improve upon how consumer authorizations are captured, adding the ability for a consumer to grant shorter-*duration* access for certain use cases and longer-duration access for other use cases. It would be helpful for data providers to be able to confirm access duration as an attribute of the authorization scope, to further promote data minimization. Helpful consumer features like this should not be foreclosed by an overly narrow definition on what dimensions of the authorization scope a data provider is allowed to confirm directly with the consumer.
3. *Account selection.* The CFPB should revise section 1033.331, which says that the data provider can ask “the consumer to *confirm*: (i) The account(s) to which the third party is seeking access.”⁵⁰ The present language, in using the word “confirm,” falsely suggests that the consumer will have already conveyed to the third party which accounts at that data provider he or she wants to share. However, the third party will not yet know that information (which accounts the consumer has at that institution). Even a list of the customer’s eligible accounts at the data provider should not be shared with any third party prior to customer consent, as this is sensitive data. This section should be modified so the data provider can “*ask the consumer which accounts* the consumer wants to share with that authorized third party.”

* * *

(e) *Mechanism to revoke third party authorization to access covered data.* A data provider does not violate the general obligation in § 1033.201(a) by making available to the consumer a reasonable method to revoke any third party’s authorization to access all of the consumer’s covered data. To be reasonable, the revocation method must, at a minimum, be unlikely to interfere with, prevent, or materially discourage consumers’ access to or use of the data, including access to and use of the data by an authorized third party. Indicia that the data

⁵⁰ 88 Fed. Reg. at 74871 (proposed § 1033.331(b)(2))

provider's revocation method is reasonable include its conformance to a qualified industry standard. A data provider that receives a revocation request from consumers through a revocation method it makes available must notify the authorized third party of the request.

JPMC Comment: Currently, proposed section 1033.331(e) would permit data providers to make available a method for revoking a third party's access to "*all of the consumer's covered data*" (emphasis added).⁵¹ The CFPB should modify the language to *also* permit a data provider to make available a method through which the consumer could *partially revoke* a third party's access to the consumer's data (specifically, to revoke access to some of the *accounts* the consumer had authorized, but not other accounts). For example, if the consumer consented to share their deposit and credit card data with a budgeting app, the data provider could provide a dashboard where the consumer can revoke access to the deposit account but not the credit card account. This gives consumers more granular control over their data. At JPMC, we have thousands of consumers using this functionality today (i.e., partially modify their data sharing connection) on a voluntary basis.

§ 1033.341 Information about the data provider.

(c) *Developer interface documentation.* For its developer interface, a data provider must disclose in the manner required by paragraph (a) of this section documentation, including metadata describing all covered data and their corresponding data fields, and other documentation sufficient for a third party to access and use the interface.⁵² The documentation must:

(1) Be maintained and updated as the developer interface is updated;

JPMC Comment: The underlined portion of the text above should be modified to provide for the disclosure of "documentation that informs the third party on *how to access and use* the interface." It is not appropriate for a public website to contain information that is fully "sufficient for a third party to *access and use* the interface." This prevents data providers from conducting reasonable due diligence on third parties *before* they get access and use of the interface. This requirement could also be understood to require disclosing, for example, private API keys that should not be made public for security purposes.

Furthermore, in section 1033.341(c)(1), the CFPB proposes that developer interface documentation must "be maintained and updated as the developer interface is updated."

This proposed requirement would be costly and onerous for data providers to comply with as written. Developer interfaces are frequently updated and while some changes will be meaningful, many changes are frequent and minor and do not significantly affect access or use. While some of the largest data providers are already compliant with some of the developer interface

⁵² Emphasis added.

documentation requirements in this rule, the CFPB should be mindful that these obligations are quite costly to meet in practice and will be very burdensome for smaller data providers. A public “developer portal” is a significant investment, and keeping documentation *completely* up-to-date at all times on every change to an API is a level of obligation that even the largest and most sophisticated API-publishing companies may not do today. To require this of every data provider is a very burdensome requirement.

A more practical and achievable alternative would be to require data providers to reasonably cooperate with authorized third parties and data aggregators to make available documentation in a timely manner that enables the connectivity requirements provided in the final rule.

* * *

(d) *Performance specification.* On or before the tenth calendar day of each calendar month, a data provider must disclose in the manner required by paragraph (a) of this section the quantitative minimum performance specification described in § 1033.311(c)(1)(i) that the data provider’s developer interface achieved in the previous calendar month. The data provider’s disclosure must include at least a rolling 13 months of the required monthly figure, except that the disclosure need not include the monthly figure for months prior to the compliance date applicable to the data provider. The data provider must disclose the metric as a percentage rounded to four decimal places, such as “99.9999 percent.”

JPMC Comment: We encourage the CFPB to give more time to data providers, for example, 45 calendar days beyond the end of the elapsed calendar month, before they are required to externally publish developer portal performance statistics, for three reasons:

1. It can take time (e.g., over a week) for internal databases to populate underlying data needed for such reporting,
2. Once automated reports are generated, some data providers may need to do extra manual work to create the specific reporting statistics that meet the CFPB’s definition of a “proper response”.
3. These statistics may need additional manual review to ensure accuracy before being reported externally (e.g., to investigate potential reporting anomalies that can arise due to hiccups in error codes, temporary reporting database failures, or other causes.)

Reporting on a 45-day lagging basis is more pragmatic and would not materially diminish the benefit of holding data providers accountable, compared with 10 days.

Additionally, we encourage the CFPB to maintain flexibility in how performance statistics are made publicly available. Currently, the NPRM requires that each data provider make such information *readily identifiable to members of the public* (1033.341(a)(1)). In the future it may be efficient for an industry body to collect and publish this information in a single place for multiple data providers, rather than for each data provider to publish separately (e.g., on their own disparate websites). This industry solution could be more cost-effective and also more consumer-friendly. We understand the current language to allow for this, and we encourage the CFPB to ensure the final rule preserves flexibility for an industry reporting solution to suffice for meeting a data provider’s obligations.

§ 1033.351 Policies and procedures.

(a) *Reasonable written policies and procedures.* A data provider must establish and maintain written policies and procedures that are reasonably designed to achieve the objectives set forth in subparts B and C of this part, including paragraphs (b) through (d) of this section. Policies and procedures must be appropriate to the size, nature, and complexity of the data provider's activities. A data provider must periodically review the policies and procedures required by this section and update them as appropriate to ensure their continued effectiveness.

(b) *Policies and procedures for making covered data available.* The policies and procedures required by paragraph (a) of this section must be reasonably designed to ensure that:

(1) *Making available covered data.* A data provider creates a record of the data fields that are covered data in the data provider's control or possession, what covered data are not made available through a consumer or developer interface pursuant to an exception in § 1033.221, and the reasons the exception applies. A data provider is permitted to comply with this requirement by incorporating the data fields defined by a qualified industry standard, provided doing so is appropriate to the size, nature, and complexity of the data provider's activities. Exclusive reliance on data fields defined by a qualified industry standard would not be appropriate if such data fields failed to identify all the covered data in the data provider's control or possession.

JPMC Comment: The obligation in 1033.351(b)(1) is problematic to operationalize for data providers and we recommend that it be removed. Instead, the requirement to share covered data, standing on its own, serves as a reasonable incentive for data providers to create internal processes to comply. Data providers should have flexibility in how they operationalize that obligation. The CFPB has also separately required that data providers make available publicly (e.g., on a website) a list of the data elements they make available via the developer interface, and this serves as a mechanism for transparency on each data provider's available data (to regulators, third parties, and consumers).

* * *

(3) *Denials of information requests.* When a data provider denies a request for information pursuant to § 1033.331, the data provider:

(i) Creates a record explaining the basis for the denial; and

(ii) Communicates to the consumer or third party, electronically or in writing, the type(s) of information denied and the reason(s) for the denial, and that the communication occurs as quickly as is practicable.

JPMC Comment: The NPRM’s requirement under section 1033.351(b)(3) should be removed as it is not feasible to implement under the current regulatory text. Below are a few, non-exhaustive examples demonstrating why:

1. *Example 1:* A data provider has denied an access request by a third party because the data provider could not authenticate the third party's identity or because the third party hasn't followed the authorization procedures. This denial would typically happen before the consumer has even authenticated with the data provider, so the data provider would have no way of knowing which consumers to inform about the denied access.
2. *Example 2:* A data provider denies a third party's access to the developer interface due to reasonable risk management concerns. The data provider has no way of identifying which consumers *might have* tried to share their data with that third party, so it does not know which consumers to notify.
3. *Example 3:* A third party has sent a malformed data request to a data provider, failing to specify the requested data categories. A data provider may reject this malformed request before the consumer has a chance to authenticate, removing any opportunity for the data provider to notify the impacted consumer (which it cannot identify). Even in cases where it is possible to identify which consumer was behind the data request, it would be a bad experience for the consumer to get notifications from the Data Provider every time a third party (for example) sent malformed data requests on his or her behalf (given third parties may send malformed requests daily, or retry numerous times, until the problem is fixed).

We appreciate the CFPB’s desire to ensure data providers are held accountable to making covered data available and not denying information requests without reason. However, the most practical accountability mechanism in this case is covered separately under section 1033.351(2). The additional obligations in section 1033.351(3) would be either unsuitable or impossible to implement across numerous valid use cases where a denial of a consumer or third party information request is reasonable and appropriate to protect the consumer or ensure data flows appropriately.

* * *

(d) *Policies and procedures for record retention.* The policies and procedures required by paragraph (a) of this section must be reasonably designed to ensure retention of records that are evidence of compliance with subparts B and C of this part.

(1) *Retention period.* Records related to a data provider’s response to a consumer’s or third party’s request for information or a third party’s request to access a developer interface must be retained for at least three years after a data provider has responded to the request.

JPMC Comment: The CFPB should clarify if this record retention requirement is meant to include an obligation on data providers to retain for three years the records of every consumer portal login by a consumer. For many data providers, all consumer portal logins could arguably involve a “request for information” under 1033 by the consumer; a data provider does not necessarily know if a consumer logging into the consumer portal came to check their deposit balances (for example) or to conduct other activities (such as to make a payment). If this

requirement does apply to consumer portal logins, it could present a significant incremental record retention burden on some data providers.

* * *

(2) *Certain records retained pursuant to policies and procedures.* Records retained pursuant to policies and procedures required under paragraph (a) of this section must include, without limitation...

(iii) Copies of a third party's authorization to access data on behalf of a consumer;

JPMC Comment: The CFPB should clarify what it means here by “a third party’s authorization.” If this is meant to be something like a single yes/no indicator passed by the third party to the data provider, attesting to having collected the required authorization from the consumer, then this may be achievable.

On the other hand, this requirement could be read to mean that the data provider must obtain and retain a copy of the full authorization disclosure provided by the third party to the consumer on the third party’s own website or app. If so, then this requirement would be very hard for data providers to operationalize. A data provider is not typically in a position to obtain a copy of the third party’s authorization disclosure form for every single data access request. Such authorizations could come in myriad different formats and be lengthy documents. It is reasonable to *allow* data providers to scrutinize these disclosures *periodically* as part of reasonable third party risk management, but it is not practical at scale for each data provider to ingest, scrutinize, and store these third party authorization forms for every third party data access request (numbering in the billions). As we stated in Part 1 above, a data provider should not be responsible for ensuring a third party is complying with its obligations under this rule. Rather, the CFPB must take responsibility for directly regulating, supervising, and enforcing regulatory obligations—including pertaining to authorization—that apply to third parties and data aggregators under this rule. It exceeds the CFPB’s authority under section 1033 to shoulder data providers with an obligation to enforce third parties’ compliance, and data providers should never be in a position where a third party’s regulatory non-compliance raises regulatory scrutiny on the data provider.

As the NPRM provides, a data provider should be able to capture its own authorization directly from the consumer in a single form and format, on its own site. This is a more effective and scalable control for data providers consistently ensuring that the right data is being shared with the right parties, with appropriate record-keeping that is scalable for data providers across thousands of third parties.

§ 1033.411 Authorization disclosure.

(a) *General requirements.* To comply with § 1033.401(a), a third party must provide the consumer with an authorization disclosure electronically or in writing. The authorization disclosure must be clear, conspicuous, and segregated from other material.

JPMC Comment: The CFPB should clarify what it means by “clear, conspicuous, and segregated from other material.” For example, the CFPB should require that a data sharing authorization disclosure be separate and distinct from the general terms & conditions that a consumer agrees to (e.g., when first signing up to use the app or service). Also, the rule should specify that the data sharing authorization disclosure should be presented to the consumer at or near the time that the data sharing request first occurs. This will help increase the likelihood that the consumer is truly making an informed choice.

Separately, the CFPB had requested comment on whether there are certain third parties for whom proposed section 1033.401 would not be appropriate, citing smaller or non-commercial parties as an example. No such exclusions should be allowed. Consumers deserve transparency, control, security, and privacy when their data is shared with third parties. Clear authorization requirements must apply equally to all third parties that seek access to sensitive financial data.

* * *

(b) *Content.* The authorization disclosure must include:

- (1) The name of the third party that will be authorized to access covered data pursuant to the third party authorization procedures in § 1033.401.
- (2) The name of the data provider that controls or possesses the covered data that the third party identified in paragraph (b)(1) of this section seeks to access on the consumer’s behalf.
- (3) A brief description of the product or service that the consumer has requested the third party identified in paragraph (b)(1) of this section provide and a statement that the third party will collect, use, and retain the consumer’s data only for the purpose of providing that product or service to the consumer.
- (4) The categories of covered data that will be accessed.
- (5) The certification statement described in § 1033.401(b).
- (6) A description of the revocation mechanism described in § 1033.421(h)(1).

JPMC Comment: In section 1033.411(b), the CFPB proposes that third parties must provide consumers with authorization disclosures containing numerous pieces of mandatory information. We agree with the requirement that this information must be presented clearly to the consumer. However, there is a risk that, if the CFPB requires *all* of that information to be presented in a single authorization disclosure at the time of account linking, the disclosure will necessarily become so long as to make it very unlikely most people will read any of it. As such, striving for

more disclosures may have the unintended practical effect of making the consumer less aware of how their data is being accessed and used.

Accordingly, the CFPB should consider which components may be the most important to be presented in the linking flow directly, and which components could be referenced (e.g., via a hyperlink made available in the authorization flow). For example, the CFPB could provide an option for the “certification statement described in § 1033.401(b)” (which could be quite lengthy) to be included by reference in a link.

Additionally, in section 1033.411(b)(2) the CFPB should remove the requirement that the authorization disclosure—as presented to the customer in the linking flow—include the name of the data provider. It would be operationally difficult for third parties to create and save a dynamic authorization disclosure document, where the name of the data provider (of which there are thousands) is dynamically inserted. Indeed, the process for a consumer to select which data provider they want to link most commonly happens with a data aggregator, *after* the consumer has completed giving authorization to the authorized third party. Backwardly folding this information into the signed authorization disclosure could be challenging. Instead, an authorized third party could be obligated to keep a separate record of the data provider connection to which a given authorization applies. This could be used by the third party for record-keeping and to provide visibility to the consumer on an ongoing basis (e.g., via a dashboard where the consumer can view and revoke access connections to specific data providers).

§ 1033.421 Third party obligations.

(a) *General limitation on collection, use, and retention of consumer data—*

(1) *In general.* The third party will limit its collection, use, and retention of covered data to what is reasonably necessary to provide the consumer’s requested product or service.

(2) *Specific activities.* For purposes of paragraph (a)(1) of this section, the following activities are not part of, or reasonably necessary to provide, any other product or service:

- (i) Targeted advertising;
- (ii) Cross-selling of other products or services; or
- (iii) The sale of covered data.

JPMC Comment: See Part 1 at pp. 25-26 for detailed comments on this section.

* * *

(b) *Collection of covered data -*

(1) *In general.* Collection of covered data for purposes of paragraph (a) of this section includes the scope of covered data collected and the duration and frequency of collection of covered data.

(2) *Maximum duration.* In addition to the limitation described in paragraph (a) of this section, the third party will limit the duration of collection of covered data to a maximum period of one year after the consumer's most recent authorization.

(3) *Reauthorization after maximum duration.* To collect covered data beyond the one year maximum period described in paragraph (b)(2) of this section, the third party will obtain a new authorization from the consumer pursuant to § 1033.401 no later than the anniversary of the most recent authorization from the consumer. The third party is permitted to ask the consumer for a new authorization pursuant to § 1033.401 in a reasonable manner. Indicia that a new authorization request is reasonable include its conformance to a qualified industry standard.

JPMC Comment: We agree with the CFPB's proposal to require third parties to seek a reauthorization from the consumer annually to continue accessing data. Consumers commonly set up data-sharing connections that they soon forget about. In our years of experience closely monitoring third party access patterns via both screen-scraping and API, we have seen that third parties often continue performing regular (e.g., daily) "background" data refreshes beyond the point when the consumer is aware or are actively using the app. When mandatory reauthorization is required, we have witnessed that a large share of consumers (~40%) whose data was still being regularly pulled do not take action to fix the broken connection. A large portion of this population may be consumers who stopped using the third party app a long time ago.

While the CFPB requires third parties to limit the duration of access to what is reasonably needed to serve the permissioned purpose (in section 1033.421(a)), this requirement alone is not sufficient to ensure that third parties discontinue data access after it is no longer desired by the consumer.

Additionally, we recommend that:

1. The CFPB should allow for any periodic reauthorization to be a "lightweight" re-authorization (e.g., a customer interaction seeking affirmative action to consent, akin to "do you still want us to continue accessing your 'Entity ABC' data? Click yes to confirm or no to cancel"), and not require the authorized third party to meet all the requirements for the initial authorization disclosure described in § 1033.401.

That said, the CFPB should not define "reauthorization" in such a broad way that a consumer's mere use of an authorized third party product or service is deemed to constitute reauthorization. Such a policy would not do enough to ensure that consumers truly understand and intend for the data to continue flowing. In many cases, a consumer may continue using certain features within a third party service (for example, a banking app) for years but have forgotten that app was continuing to access held-away account information.

2. The CFPB should (1) require third parties to make available to the data provider, upon the data provider's request, evidence of each time the consumer has reauthorized the sharing of data and (2) allow providers to discontinue allowing access if authorization has lapsed. This improved information sharing between parties will foster transparency and help ensure consumer expectations are met.

* * *

(c) *Use of covered data.* Use of covered data for purposes of paragraph (a) of this section includes both the third party's own use of covered data and provision of covered data by that third party to other third parties. Examples of uses of covered data that are permitted under paragraph (a) of this section include ...

(2) Uses that are reasonably necessary to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; and

JPMC Comment: We recommend that the CFPB clarify 1033.421(c)(2). While third parties should be allowed to use data for preventing actual or potential fraud, this should be appropriately limited. For example, a third party may interpret this section expansively and use consumer-permissioned data to create a new tool that it then *commercializes and sells* as a service to other, unrelated companies, using consumer-permissioned data under the broad auspices of protecting against "claims" or "unauthorized transactions" or the (especially broad term) "other liability." Indeed we already see in the marketplace some data aggregators creating commercial products related to preventing unauthorized transactions as a secondary use, leveraging vast troves of consumer-permissioned data. This use may go far beyond what the consumer ever intended their data to be used for, and the CFPB should consider what unintended consequences might arise from the creation, monetization, and use of such commercial tools.

* * *

(d) *Accuracy.* The third party will establish and maintain written policies and procedures that are reasonably designed to ensure that covered data are accurately received from a data provider and accurately provided to another third party, if applicable...

(3) *Elements.* In developing its policies and procedures regarding accuracy, a third party must consider, for example: ...

(i) Accepting covered data in a format required by § 1033.311(b); and

(ii) Addressing information provided by a consumer, data provider, or another third party regarding inaccuracies in the covered data.

JPMC Comment: Accuracy of data is the responsibility of the data provider. Authorized third parties are not in a position to be able to attest to, or even reasonably detect, the accuracy of data they receive from other parties. That said, it is reasonable for the authorized third party to have operational responsibilities to use best practices when handling the data. This should be rewritten to require authorized third parties to maintain policies and procedures around data handling to prevent the introduction of data inaccuracies. Additionally, pertaining to section 1033.421(d)(3)(ii): developing policies and procedures around inaccuracies would be challenging and should be limited to obligating authorized third parties to make reasonable efforts to investigate, communicate, and resolve inaccuracies.

Additionally regarding 1033.421(d)(3)(i), the CFPB proposes that a third party must consider accepting covered data in a format required by § 1033.311(b). In the future, we expect that most third parties will continue to source most of their data indirectly via data aggregators, not directly

from data providers, due to the high costs of building direct pipes to thousands of data sources. As such, it should be noted here that the vast majority of third parties likely will *not* consume covered data in an industry-standard data format. Rather, they will consume data from data aggregators, which typically expose the data in a format proprietary to each data aggregator.

While data aggregators will *consume* data via standardized APIs from data providers, data aggregators generally expose the data further downstream via custom-formatted APIs, and nothing in this rulemaking appears to mandate data aggregators to expose information to their downstream data recipient clients using an industry standard format. Accordingly, unless the CFPB plans to mandate that data aggregators act otherwise, the CFPB should revise this section to remove the requirement on authorized third parties to consider accepting covered data in an industry standardized format.

* * *

(e) *Data security.* (1) A third party will apply to its systems for the collection, use, and retention of covered data an information security program that satisfies the applicable rules issued pursuant to section 501 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801); or (2) If the third party is not subject to section 501 of the Gramm-Leach-Bliley Act, the third party will apply to its systems for the collection, use, and retention of covered data the information security program required by the Federal Trade Commission’s Standards for Safeguarding Customer Information, 16 CFR part 314.

JPMC Comment: The only direct method the CFPB cites for regulators holding third parties accountable for data security directly is via GLBA (for some) and the FTC Safeguard Rule (for others). However, this creates an uneven playing field. GLBA is focused more on data use and privacy and has a more robust oversight process; the FTC Safeguards Rule focuses more on data security but without a strong oversight mechanism. This creates a patchwork of rules and varying levels of oversight.

A more appropriate requirement would be for all third parties to comply with the FFIEC Security Handbook, which is more relevant and comprehensive than GLBA and the FTC Safeguards Rule. Mandatory adherence to the FFIEC Security Handbook would better ensure the level of robust protection that consumers expect for sensitive financial services data. The CFPB should also tailor its supervision of third parties relating to those FFIEC Security Handbook requirements. Adopting these revised requirements for data security could also substantially smooth the conversations between data providers and third parties when it comes to data security.

Separately, in the NPRM commentary the CFPB stated that it “expects that third parties that comply with the data security requirements of the proposed rule or the GLBA Safeguards Framework would not be denied access to data providers’ interfaces.” However, as we stated above in Part 1, it is important that the final rule not define eligible risk management concerns too narrowly. A third party’s compliance with the GLBA Safeguards Framework alone may not be not sufficient to address reasonable risk management concerns that a data provider may have.

* * *

(f) *Provision of covered data to other third parties.* Before providing covered data to another third party, subject to the limitation described in paragraphs (a) and (c) of this section, the third party will require the other third party by contract to comply with the third party obligations in paragraphs (a) through (g) of this section and the condition in paragraph (h)(3) of this section upon receipt of the notice described in paragraph (h)(2) of this section.

JPMC Comment: The circumstances under which an authorized third party would be allowed to provide covered data to another third party under this section are unclear. The regulatory text says that the receiving third party would be contractually obligated to comply with “the third party obligations in paragraphs (a) through (g)”, but it is not clear how that would work. If the consumer originally shared data with Company1 for Purpose1, it is not clear how Company2 could have any beneficial allowable purpose for obtaining that data. It is also unclear if this section is only targeted at subcontractors that enabled Company1 to provide its services. We encourage the CFPB to clarify the wording here, including as it ties back to sections (a) through (g).

Additionally, we recommend the CFPB raise the requirement in the rule from, “require... by contract” to, “require and ensure.” It should be made clear that the authorized third party has responsibility for ensuring protection of the data they have been entrusted with, including having responsibility for additional third parties it engages.

* * *

(h) *Revocation of third party authorization.*

(2) The third party will notify the data provider, any data aggregator, and other third parties to whom it has provided the consumer’s covered data when the third party receives a revocation request from the consumer.

JPMC Comment: The CFPB should clarify that if a third party accesses data via a data aggregator, then the third party can satisfy its revocation notification obligations by providing notice of revocation to the data aggregator it employs as a vendor (as applicable), which would then provide the revocation notice onward to the data provider.

Section 1033.431

(a) *Responsibility for authorization procedures when the third party will use a data aggregator.* A data aggregator is permitted to perform the authorization procedures described in § 1033.401 on behalf of the third party seeking authorization under §1033.401 to access covered data. However, the third party seeking authorization remains *responsible for compliance with the authorization procedures described in §1033.401....* (emphasis added)

JPMC Comment: We have worked closely with data aggregators over the past several years, both as a data provider and as a data recipient, to enable safe and seamless data sharing for millions of our customers. Based on our experience from these engagements, we recommend several changes to section 1033.431(b) to ensure consumers have appropriate transparency and control when sharing their data via data aggregators.

1. While it makes sense for the data aggregator to perform *some* of the authorization procedures described in section 1033.401, it does not make sense for the data aggregator to perform *all* of these procedures. The CFPB should elaborate more clearly which of the obligations in section 1033.401 must be carried out by the authorized third party, and which activities could be carried out by the data aggregator. To give a few examples:
 - (a) There are some components of the authorization disclosures described in 1033.411 that should still be the responsibility of the authorized third party to provide to the consumer directly, describing and attesting to *its own* activities. For example, if FinTech1 uses Aggregator1 to access data, then FinTech1 should still be required to provide a description of *its own* product or service to the consumer. It wouldn't make sense for Aggregator1 to solely provide a description *of the Aggregator's service* (of facilitating data access) to the consumer.
 - (b) It should be made clear that the authorized third party (e.g., Fintech1) must itself provide a certification statement to the consumer, covering many of the requirements in section 1033.421. Otherwise, for example, Fintech1 would be able to forego providing any direct certification to the consumer around how it will protect or use data. Customers would have a hard time holding authorized third parties responsible for misuse or harm in the absence of such a direct certification.
 - (c) In some areas, it is unclear in the current NPRM language to which entity the obligation applies, when the CFPB states that "a data aggregator is permitted to perform the authorization procedures ... *on behalf of* the third party seeking authorization." For example, where in section 1033.421 it states that "the third party will limit its collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service," it is unclear whether "third party" here refers to the end-user app or to the data aggregator. It is also unclear whether the "requested product or service" refers to the end-user-facing app or the aggregator's service of enabling connectivity. This ambiguity, if not clarified, could give rise to Data Aggregators collecting more data than is actually needed for the role they are serving as an intermediary (or pass-through) function serving the data needs of that particular downstream third party.
2. Where the NPRM says that "the third party seeking authorization remains responsible for compliance with the authorization procedures," the CFPB should clarify that the third party is responsible for *its own compliance* with all the relevant obligations and also for *the data aggregator's compliance* with these obligations (as a service provider to the

authorized third party). Absent this clarification, it is unclear which party's compliance is being described.

3. The Bureau should distinguish the data aggregator's role when acting as an intermediary for authorized third parties, versus when it is acting in the role of authorized third party. The Bureau should add to proposed section 1033.431 that when a data aggregator is acting on behalf of an authorized third party to facilitate data sharing, the data aggregator is prohibited from capturing a separate authorization from the consumer to use data for its own, unrelated purposes as part of the same account linking flow in which it is acting as an intermediary (i.e., for purposes beyond what is needed to facilitate the data sharing with that specific downstream third party). Prohibiting this activity is consistent with the CFPB's goal of ensuring that data is collected and used solely for the beneficial purpose the consumer intended.

Consumers generally do not engage in data sharing with an authorized third party with the intent of having their data be accessed and used for other purposes by a data aggregator. Some data aggregators engage in this "piggybacking" practice today, collecting consent from consumers to use data for their own separate purposes, and many consumers may not realize it because the consent form is presented in the middle of an account linking flow when the consumer is connecting another, downstream app. Here, the consumer may not realize or reasonably expect that there is an intermediary that is getting access to data for its own uses. Even if the consumer does realize it in the moment, the consumer may quickly forget who the data aggregator is or not know how to revoke that aggregator's distinct access or use of the data.

Relatedly, JPMC requests that the CFPB add the following to section 1033.431 on "direct consumer services": "When a data aggregator is facilitating data access on behalf of an authorized third party, that activity (of facilitating access) may be not considered "providing a requested product or service to the consumer" directly under section 1033.421(a)." ⁵³

4. The CFPB should clarify proposed section 1033.431 to require that when a data aggregator is acting on behalf of an authorized third party (section 1033.431(a)), the data aggregator must fulfill all of its obligations under the rule independent of other connections the data aggregator may have facilitated for the same consumer.

That is, each and every time a consumer permissions their data to an authorized third party, even if the consumer's access and/or authorization is being facilitated by a data aggregator that has already facilitated access for that same consumer on behalf of a

⁵³ A data aggregator may provide some consumer-facing functionality when acting as a service provider to an authorized third party (e.g., helping that third party capture and manage consumer authorization), but that should not be taken to mean the data aggregator is "providing a requested product or service to the consumer." Consumers do not request or seek out separate "data connectivity" services in the marketplace; rather, such connectivity services are provided by data aggregators to authorized third parties, in service of the core service (e.g., a budgeting tool) the consumer has sought from the authorized third party. Indeed, consumers generally do not have choice which data aggregator is used to enable connectivity when they want to link their accounts to an underlying app.

different authorized third party, all parties in the chain should treat that engagement as a new request and follow all obligations independently under the rule.⁵⁴ This is important to avoid a blurring of responsibilities or comingling of data or authorization scopes that could ultimately harm consumers.

5. It is unclear in the proposed rule whether an authorized third party would be obligated to provide the consumer with a means of ceasing access or if the data aggregator would perform that function for the authorized third party. We recommend that the requirement apply to the authorized third party, given it is the authorized third party's product or service the consumer has intentionally engaged with and will generally be more familiar with. Data Aggregators should be obligated to react, in a timely fashion as per industry standards, to requests for revocation received from data providers and authorized third parties and to no longer collect, use, or retain covered data.

* * *

(c) *Data aggregator certification.* When the third party seeking authorization under § 1033.401 will use a data aggregator to assist with accessing covered data on behalf of a consumer, the data aggregator must certify to the consumer that it agrees to the conditions on accessing the consumer's data in § 1033.421(a) through (f) and the condition in § 1033.421(h)(3) upon receipt of the notice described in § 1033.421(h)(2) before accessing the consumer's data.

JPMC Comment: We recommend the CFPB modify this requirement in a several ways to be better tailored to the specific role that data aggregators play as agents acting on behalf of the authorized third party. The data aggregator should be required to certify to the consumer that it agrees to the following conditions on accessing the consumer's data:

1. *Limitations on collection, use and retention.* The data aggregator will limit its collection, use and retention of covered data to what is reasonably necessary to *provide a data access service that enables that particular authorized third party to provide the consumer's requested product or service.*
2. *Collection of covered data.* The scope, duration and frequency of a data aggregator's collection of covered data, as well as the storage and use of the covered data by the data aggregator, should be limited to what is reasonably necessary to provide the product or service that the consumer requested *from the authorized third party.*


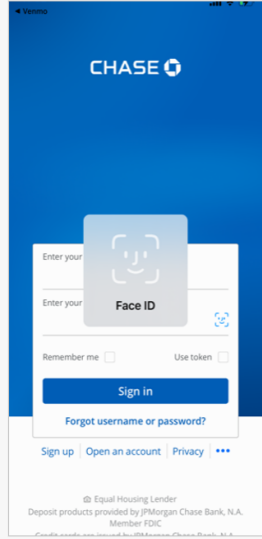
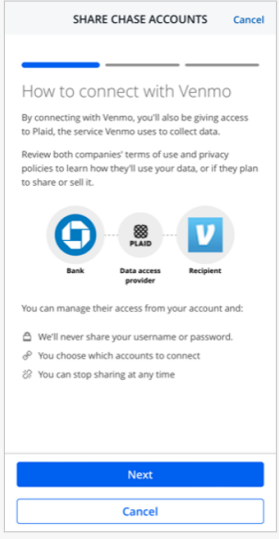
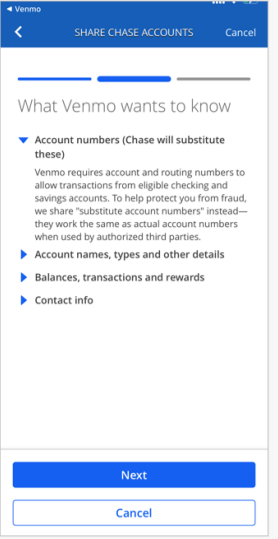
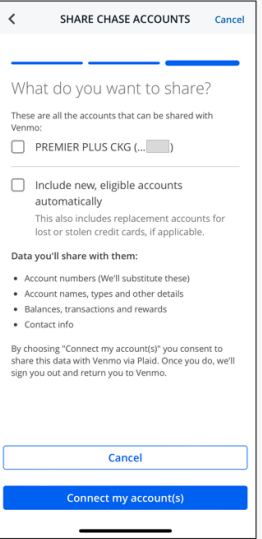
⁵⁴ This is important to avoid a blurring of responsibilities or comingling of data or authorization scopes that could ultimately harm consumers. For example, consider a consumer that (1) shares his BankA data via Aggregator1 with App1, then later (2) shares the same BankA data via Aggregator1 with App2. In this (very common) scenario, Aggregator1 should be obligated to act on behalf of App1 and carry out its obligations under this rule pertaining to App1 independent of the role it plays on behalf of App2. Otherwise, Aggregator1 may seek to claim (for example) that a consumer's authorization or reauthorization for App1 also applies to App2.

3. *Policies and Procedures.* The data aggregator should maintain written policies and procedures covering how it fulfills its obligations, including the appropriate handling of covered data.
4. *Data security.* The data aggregator must abide by the same data security standards as authorized third parties in section 1033.421(e).
5. *Ensuring customers are informed.* The data aggregator will deliver a copy or make readily accessible a copy of the 'Data Aggregator Certification' to the consumer. The data aggregator must make available contact information that enables a consumer to receive answers to questions about the data aggregator's access, use, and protection of covered data.

* * * * *

Appendix 1

To share his Chase account information with a third-party app, a consumer is redirected to Chase to authenticate and authorize access

CHASE

Enter your
Enter your

Face ID

Remember me ☐ Use token ☐

Sign in

Forgot username or password?

Sign up | Open an account | Privacy

Equal Housing Lender
Deposit products provided by JPMorgan Chase Bank, N.A.
Member FDIC

SHARE CHASE ACCOUNTS Cancel

How to connect with Venmo

By connecting with Venmo, you'll also be giving access to Plaid, the service Venmo uses to collect data.

Review both companies' terms of use and privacy policies to learn how they'll use your data, or if they plan to share or sell it.

Bank Data access provider Recipient

You can manage their access from your account and:

- We'll never share your username or password.
- You choose which accounts to connect
- You can stop sharing at any time

Next Cancel

SHARE CHASE ACCOUNTS Cancel

What Venmo wants to know

Account numbers (Chase will substitute these)

Venmo requires account and routing numbers to allow transactions from eligible checking and savings accounts. To help protect you from fraud, we share "substitute account numbers" instead—they work the same as actual account numbers when used by authorized third parties.

Account names, types and other details

Balances, transactions and rewards

Contact info

Next Cancel

SHARE CHASE ACCOUNTS Cancel

What do you want to share?

These are all the accounts that can be shared with Venmo:

☐ PREMIER PLUS CKG (...)

☐ Include new, eligible accounts automatically

This also includes replacement accounts for lost or stolen credit cards, if applicable.

Data you'll share with them:





- Account numbers (We'll substitute these)
- Account names, types and other details
- Balances, transactions and rewards
- Contact info

By choosing "Connect my account(s)" you consent to share this data with Venmo via Plaid. Once you do, we'll sign you out and return you to Venmo.

Cancel

Connect my account(s)

A dashboard on the Chase website and mobile app enables the customer to see and manage which third parties have access to his Chase account data

View third parties that I've given access to my data

9:51

Linked apps and websites

We make it easier for you to keep track of what apps and websites you connected to your account and provide transparency over what's being shared. No longer want an app or website to have access to your account info? You have the power to stop sharing it here.

Get more information in our [FAQs](#).

Active (5)

- NerdWallet via Plaid Dec 21, 2023 at 9:37 PM ET
- Empower via Empower | Yodlee Dec 21, 2023 at 11:11 AM ET
- Robinhood via Plaid Dec 20, 2023 at 8:19 AM ET
- Venmo via Plaid Aug 30, 2023 at 4:46 PM ET
- Intuit Mint via Intuit Jun 28, 2023 at 9:33 AM ET

Inactive (0)

You don't have any inactive linked apps or websites

See details on data they can access & revoke sharing at any time

Linked apps and websites

NerdWallet via Plaid Nov 21, 2023 at 3:07 PM ET

Data currently shared

- Account names, types and other details
- Balances, transactions and rewards
- Contact info
- Account numbers (We'll substitute these)

Sharing data from these accounts

- CREDIT CARD (...)
- PREMIER SAVINGS (...)
- PREMIER PLUS CKG (...)

Eligible accounts that have not been shared

- CREDIT CARD (...)
- CREDIT CARD (...)

Include new, eligible accounts automatically

This also includes replacement accounts for lost or stolen credit cards, if applicable.

Access stats

Last accessed by NerdWallet Nov 21, 2023 at 3:07 PM ET

Started sharing on Jan 29, 2023

Edit sharing

Stop sharing data

Modify which accounts those companies can access

Edit sharing Close

Data shared

Data currently shared

Stop sharing account info

Account(s) shared

You can manage the eligible accounts you share with NerdWallet by adding or removing them below.

Shared accounts

Select all accounts

- ☒ CREDIT CARD (...)
- ☐ CREDIT CARD (...)
- ☐ CREDIT CARD (...)
- ☒ PREMIER SAVINGS (...)
- ☒ PREMIER PLUS CKG (...)

Extra permissions

☐ Please include future accounts

This includes new accounts and replacement accounts for a lost or stolen credit card.

Do you agree to update what you're sharing with NerdWallet via Plaid?

Cancel

I agree