U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

December 22, 2023

Comment Intake—FINANCIAL DATA RIGHTS
c/o Legal Division Docket Manager
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Required Rulemaking on Personal Financial Data Rights

To Whom It May Concern:

The Center for Capital Markets Competitiveness ("CCMC") appreciates the opportunity to submit comments to the Consumer Financial Protection Bureau ("CFPB") regarding its Notice of Proposed Rulemaking for the Required Rulemaking on Personal Financial Data Rights (the "Proposed Rule").[1]

CCMC welcomes the CFPB's work to implement section 1033 of the Dodd-Frank Act. We strongly support maintaining secure consumer access to financial information, consistent with section 1033. Industry participants take their consumer data access, privacy, and security obligations seriously, and have invested significant time and money in developing technology to help consumers access data in secure ways. In doing so, regulated financial institutions have met stringent data privacy and security requirements that prioritize consumer protection. Stakeholders with diverse interests have also risen to the challenges inherent in the increasingly digital marketplace. For example, the Financial Data Exchange ("FDX"), a consortium of data providers, data aggregators, data recipients, and other key industry participants has spent significant time and resources creating a framework for sharing information through application programming interfaces ("APIs") that have notably enhanced both data security and ease of use for participants and their customers.

Contrary to some of the statements in the CFPB's press release on the Proposed Rule, competition among industry participants has driven much of this innovation in consumer access to financial data. These technological solutions have been developed in a marketplace with diverse interests, differing products and

[1] *See Proposed Rule; Request for Public Comment: Required Rulemaking on Personal Financial Data Rights*, CFPB-2023-0052, 88 Fed. Reg. 74796 (October 31, 2023).

services, and various-sized entities. The CFPB should support such market-based competition so that consumers benefit from continued innovations and improvements in data access, security, and privacy.

Missteps in the section 1033 rulemaking could harm consumers given the important privacy and security implications associated with the handling of consumer data. Impractical or unduly burdensome regulations would also create inefficiencies in the market and could have unknown negative and unintended consequences for market participants and consumers. While we agree with many of the provisions in the Proposed Rule, the CFPB should revise key elements in any final rule. For example, the Proposed Rule would leave key interpretive questions unresolved, leading to unnecessary and counterproductive regulatory uncertainty and market disruption. The Proposed Rule also does not fully articulate the cost-benefit analysis on key elements of the rule, leaving doubt as to whether certain aspects of the Proposed Rule are justified. Moreover, the compliance timelines contemplated by the Proposed Rule are unreasonably short and the interaction with other forthcoming regulations is unclear, creating risk to consumers.

We accordingly make the following points:

- The CFPB should clarify key aspects of the Proposed Rule.
- The CFPB failed to engage in a thorough and accurate cost-benefit analysis of key aspects of the Proposed Rule.
- The CFPB should lengthen the deadline for compliance with a final rule.
- The CFPB should finalize this rule before proposing a new rule regulating data brokers under FCRA.

I. The CFPB should clarify key aspects of the Proposed Rule.

We welcome the portions of the Proposed Rule that would effectively promote consumer data access. We also appreciate that the CFPB has addressed many of the comments submitted in response to the rulemaking outline it issued pursuant to the Small Business Regulatory Enforcement Fairness Act ("SBREFA").[2] However, the Proposed Rule fails to resolve several important questions. In particular, requirements and restrictions surrounding screen scraping remain unclear. Further, the process for

[2] *See Outline of Proposals and Alternatives Under Consideration for the Personal Financial Data Rights Rulemaking* (October 27, 2022), available at: https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf.

recognizing a standard setting body (or bodies) lacks important process details and appropriate timelines. The Proposed Rule also does not sufficiently address certain risk management concerns, nor whether particular types of consumer data fall within the scope of the Proposed Rule. The CFPB should provide clarity on these points in any final rule in order to ensure that market participants have clear rules of the road, which would maximize consumer benefits and protections.

a. The CFPB should facilitate a transition away from screen scraping through clearer and more comprehensive standards.

Recent years have seen the market shift away from the use of screen scraping to obtain consumer data. As the CFPB recognizes, screen scraping has certain "inherent overcollection, accuracy, and consumer privacy risks."[3] As a result, "there is nearly universal consensus that developer interfaces should supplant screen scraping."[4] To this end, we understand the Proposed Rule to require certain data providers[5] to develop an API through which authorized third parties can obtain data as directed by the consumer, otherwise known as the "developer interface." The Proposed Rule thus would clearly continue pushing the industry-led movement away from screen scraping.

While the CFPB appears to share the broad interest in eliminating screen scraping, the Proposed Rule is ambiguous about whether screen scraping can be performed in certain circumstances, or whether data providers can block screen scraping. The CFPB should clarify a timeline and process for transitioning away from screen scraping, recognizing that APIs are the preferred technological solution if stakeholders are able to adopt them in a cost-effective manner. Relatedly, the Proposed Rule is unclear on whether third parties are required to comply with the proposed certification, disclosure, and use limitation requirements for non-covered data.

It is important for the CFPB to provide clarity on these points given the significant risks screen scraping poses to consumers and data providers. Failure to affirmatively address the risks could lead to negative unintended consequences for consumers by inviting irresponsible actors to skirt the requirements the CFPB intends to impose. The CFPB cannot fully address these risks by treating screen scraping as a violation of Section 1033 or other federal consumer financial laws. Any effort to regulate by enforcement would not effectively address underlying areas of regulatory

---

[3] *See Proposed Rule* at 74813.

[4] *See id.* at 74798.

[5] Specifically, data providers that have developed a consumer interface by the compliance date.

uncertainty. The CFPB instead should issue clear rules on whether and how legal requirements apply to screen scraping.

b. The CFPB should clarify the role of standard-setting bodies.

The CFPB acknowledges that "[c]omprehensive and detailed technical standards mandated by Federal regulation could not address the full range of technical issues in the open banking system in a manner that keeps pace with changes in the market and technology."[6] As a result, the CFPB preliminarily concludes that "[i]ndustry standard-setting bodies that operate in a fair, open, and inclusive manner have a critical role to play in ensuring a safe, secure, reliable, and competitive data access framework."[7] We agree that standard setting bodies can play important roles in this field. We are concerned, however, by the Proposed Rule's failure to ensure that the process for recognizing standards would be transparent,[8] include appropriate protections, and draw appropriately on existing work by key stakeholders. We would ask the CFPB to address these gaps in any final rule.

First, the CFPB should provide more detail on the process for selecting a standard setting body. To this end, the Proposed Rule allows the CFPB to recognize standard-setting bodies. However, the Proposed Rule does not detail the process the CFPB would use for granting such recognition, other than identifying certain general attributes the standard-setting body must possess. In addition, the Proposed Rule does not clarify whether the CFPB would only recognize certain standards set by that body. Nor does the Proposed Rule address whether and under what circumstances the CFPB may either rescind its recognition or refuse to recognize particular standards issued by a recognized body. Further, the Proposed Rule fails to address whether a standard setting body must apply to be recognized or can be recognized *sua sponte* by the CFPB. Without certainty on these points, it will be very difficult for industry stakeholders to rely upon any standards promulgated by standard-setting bodies. The CFPB should resolve these areas of doubt and ensure that industry participants are able to readily understand how they will be able to rely on qualified industry standards ("QIS"). Such understanding is necessary to achieve compliance with relevant requirements and increase efficiency in the market to benefit consumers.

---

[6] *See id.* at 74801.

[7] *See id.*

[8] The CFPB should however, ensure that members of standard setting bodies are not required to share confidential or commercially sensitive information.

Second, the CFPB should ensure that the process used for recognizing standard-setting bodies includes appropriate process-based protections, such as appeal rights. While the CFPB requires that the standard setting body itself provide an appeal process, among other protections, the CFPB does not include similar process-based protections to its own work. This is a mistake. We would urge the CFPB to apply similar requirements in its process for recognizing standard-setting bodies while also ensuring that this process moves efficiently.

Third, the CFPB should ensure that its selection of standard setting bodies builds on the significant work already performed by industry stakeholders. In particular, the CFPB should strongly consider recognizing FDX as a standard-setting body for API standards. FDX has created the most widely used framework for APIs. It has devoted significant time and resources toward promoting open banking in a way that maintains data security and privacy for consumers. FDX's work reflects the input of a wide variety of market participants and other stakeholders who have a deep understanding of the applicable technology. Considering the significant work by this group to-date and the wide adoption of FDX standards in the industry, failing to recognize FDX as a new standard-setting body would represent a significant missed opportunity.

c. The CFPB should clarify its rules on third party risk management, including addressing third party liability.

Under the Proposed Rule, authorized third parties would connect to a data provider's API to obtain covered data at the direction of a consumer. It is important that authorized third parties can access this information at the request and direction of consumers—consumers should be able to access data and use it for desired financial products and services. That said, data providers have a strong interest in protecting customers' data from unscrupulous or unsafe practices by these third parties. To that end, we are glad that the CFPB recognizes that data providers appropriately manage their risk as a condition of authorized third parties accessing a data provider's API. We particularly appreciate the CFPB's inclusion of provisions permitting data providers to block third party access if there is a bona fide and particularized risk management concern. We believe that the CFPB can provide more clarity on this point, however.

To further bolster consumer data protection, the CFPB and the prudential regulators should issue guidance around the applicability of third-party risk management standards in connection with the final rule to ensure there are no conflicts between the expectations of the CFPB and prudential regulators. At the very least, the CFPB should maintain close communication with the prudential regulators

when finalizing the rule, issuing guidance, developing examination standards, and initiating enforcement actions. The CFPB should use the final rule or additional guidance to explain how to comply under practical scenarios and circumstances. As the CFPB knows, the prudential regulators' current guidance on best practices for safety and soundness and third-party risk management is subject to change. Those regulators may also have differing views from the CFPB with respect to appropriate risk mitigation measures, including what constitutes appropriate due diligence and risk-based denials. And those views could change in response to market developments. Data providers should not be subject to contradictory or inconsistent federal regulatory standards or be forced to forgo actions required by prudential regulators to maintain safety and soundness. The CFPB should work with those fellow regulators to create a harmonious regulatory approach.

Finally, the CFPB should specify in the final rule that responsibility and liability flow with the data. The CFPB should affirm through regulation that a data provider sharing data in compliance with the section 1033 rule cannot be held financially liable for a breach of a third-party provider. Addressing liability is key to data providers' ability to appropriately manage third party risk while complying with the section 1033 rule. Including liability in the final rule would incentivize third parties to maintain security and privacy standards that meet applicable legal requirements, including the Gramm-Leach-Bliley Act regulations. Specifying that liability will flow with the data wouldalso promote accountability and responsibility throughout the data flow. The risk management protections provided under the Proposed Rule would be significantly undermined if any entity receiving covered data lacks required safeguards to protect it.

d. The CFPB should provide additional clarity regarding other aspects of the Proposed Rule and revise other provisions that could have unintended consequences.

The Proposed Rule includes a number of other unclear provisions that could cause unintended consequences. We would ask that the CFPB address each of the following aspects of the Proposed Rule in the final rule:

- Section 1033(d) requires the CFPB to "prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers under [section 1033]." The Proposed Rule includes certain requirements for standardization of covered data made available by data providers. However, it does not adequately address standardization of data formats as the data moves from data aggregators to authorized third parties, or otherwise from one authorized third party to

another. The CFPB should make clear how (and why) standardization requirements apply to this data as well as whether companies may rely upon QISs in the handling of such data.

- The Proposed Rule could prohibit third parties from using covered data in certain fraud prevention efforts. Fraud prevention is a key use of covered data for most industry participants. The use of covered data for fraud prevention benefits both consumers and the overall marketplace. Excluding fraud prevention uses could have the unintended consequence of reducing consumer data security and privacy. The CFPB accordingly should make clear that third parties may use covered data without restriction, and beyond the provision of the requested product or service, in fraud prevention efforts or provide clear exceptions to that general rule.

- The Proposed Rule includes digital wallet providers as an example of data providers. However, the Proposed Rule does not define digital wallet providers.[9] It is therefore unclear whether the CFPB considers digital wallet providers to include both stored value digital wallet providers, whose products can be used to transact with multiple sellers, and pass-through digital wallet providers. Stored value and pass-through digital wallets operate differently from each other, and it is unclear whether the CFPB intends both to be included as covered products under the section 1033 rule. The CFPB should clarify this definitional point.

- The CFPB should also make clear the implications of any new or novel interpretations of the term "funds" under Regulation E, either in the final rule or through appropriate commentary. If the CFPB intends for the section 1033 rule to apply to accounts that have not traditionally been considered Regulation E accounts by regulators, it should provide clear guidance as to the intended scope and to reduce market uncertainty. The CFPB should also acknowledge the role of the Securities and Exchange Commission as the primary regulator of broker-dealers and investment advisers, and coordinate appropriately.[10]

- Finally, the CFPB should provide more clarification on the standalone product exception to proposed section 1033.421(a)(2), which states that targeted advertising, cross-selling of other products or services, or the sale of covered data are not part of, or reasonably necessary to provide, any other product or service. A clear definition of what the CFPB considers targeted advertising,

[9] The CFPB, in other contexts, has proposed to define these activities and should provide similar clarity on the definition of a "digital wallet" as part of any final rule.
[10] See 12 U.S.C. §5517. "The Bureau shall have no authority to exercise any power to enforce this title with respect to a person regulated by the Commission."

cross-selling, or selling is needed to navigate whether a product qualifies for this exception.

The CFPB should clarify how it intends to enforce the requirements that apply to third parties. The proposed rule does not make clear whether certain requirements imposed on third parties would be enforced by the CFPB or by, for example, the Federal Trade Commission, which enforces its Safeguards Rule. In addition, the CFPB should make the following discrete changes in the final rule to ensure that the relevant provisions do not have unintended consequences:

- The CFPB should narrow the definition of "consumer" to a natural person with at least one current account with the data provider.
- The CFPB should only permit an account holder to authorize data access requests under the rule. Authorized users should not be permitted to authorize data access requests.
- The CFPB should reduce the API response retention period for data providers.
- The final rule should limit the terms and conditions data providers are required to provide to third parties to items such as actual fees incurred, annual percentage rate, and annual percentage yield.
- Business to business products and services, including credit cards that are generally issued for business purposes, such as corporate cards, should not be included in the scope of covered products in the final rule.

II. The CFPB failed to engage in a thorough and accurate cost-benefit analysis of key aspects of the Proposed Rule.

Any final rule implementing section 1033 would have significant financial implications for both industry participants and consumers. It is important that the CFPB accurately consider the potential costs and benefits of the rule. While the CFPB attempts to conduct a cost-benefit analysis, we believe that the CFPB should do more to fully and accurately analyze costs and benefits to impacted parties before finalizing the rule. We highlight three areas where the CFPB should engage in a more fulsome cost-benefit analysis.

First, the CFPB has not demonstrated the benefits to consumers of requiring data providers to provide them certain types of data in certain ways. Accordingly, the CFPB has not shown that the benefit of providing this data would outweigh the cost of providing it in the ways proposed by the CFPB. This is especially true as consumers generally can access the covered data directly through the data provider today and the

incremental costs for data providers to provide a second means of access, in a specific way, are likely to be significant. For example, the CFPB has not demonstrated a use case for providing terms and conditions in a machine readable format that is not otherwise satisfied by providing the data electronically. To the extent a PDF is not a machine readable format, data providers will be required to spend resources putting terms and conditions into a machine readable format. It is unclear how consumers would benefit from terms and conditions being provided in such a format when they are already provided to the consumer at account opening and made available in a retainable form. Terms and conditions do not frequently change and are not specific to individual consumers in the same way account balances and transactions are, so it is unclear why third parties will need this information hourly or daily. In addition, any changes to the terms and conditions must be noticed well in advance of becoming effective, further reducing the need for frequent data requests.

Second, the CFPB preliminarily concluded that pending transaction and upcoming bill information supports beneficial use cases, including fraud detection and personal financial management. However, the CFPB did not specify how pending transaction or upcoming bill information would be used in support of those cases. The CFPB also did not analyze whether the benefits of those uses outweigh other consumer interests or costs associated with providing the information. For example, reliance on pending transaction or upcoming bill data could cause confusion with respect to account balances or transactions, increase costs to offer a product or service, or the risk that authorized third parties misread certain pending transactions in ways that harm consumers. In particular, an authorization may be for an amount that will later increase (such as nominal holds at a gas station, for online purchases, or charges that do not yet include a tip) or later decrease (such as security hold by a hotel). A consumer cannot initiate a notice of error or dispute for unsettled transactions given the inherent uncertainty associated with unsettled transactions. Similarly, the upcoming bill amount may be an estimate, or may not reflect recent information, such as a payoff or change in terms. The CFPB should thoroughly assess the costs and benefits of requiring such information to be provided in any final rule.

Third, the CFPB has not adequately considered the costs and benefits of prohibiting data providers from charging fees to authorized third parties to access covered data. Under the Proposed Rule, the CFPB would require private entities (here, data providers) to offer a unique and specific product or service, while simultaneously expressly prohibiting that private entity from charging a reasonable fee or recovering costs associated with the required offering of the specific product or service. At a minimum, the CFPB should conduct strong cost-benefit analysis to justify this aspect of the rule.

III. The CFPB should lengthen the deadline for compliance with a final rule.

The Proposed Rule promises an "accelerated shift" and a sea change in the way that consumer financial data is shared with third parties. If implemented, the rule would require significant and costly changes throughout the industry and raise many questions as stakeholders attempt to move quickly—but carefully—to comply with the law. As written, the Proposed Rule would require the largest data providers to comply with a final rule six months after the rule's publication, while giving smaller data providers up to four years to comply. This does not provide large companies adequate time to come into compliance with significant new regulatory requirements given the complexities of their various product offerings and associated backend data retention practices. Six months is also too short of a time frame for authorized third parties to build systems that work with the APIs of many different data providers. This is especially true given the lack of clarity for how the CFPB would recognize a standard setting body. Accordingly, we ask the CFPB to extend the compliance deadline to at least two years from the date of publication in the *Federal Register* for the largest data providers.

The CFPB significantly underestimates the real challenges the Proposed Rule would present for data providers and authorized third parties, including the potential implications other CFPB rulemakings may have on the same systems, sets of data, and means of delivery. The CFPB's proposed deadline particularly fails to recognize that the Proposed Rule would require significant adjustments even as it relates to data currently made available. These include adjustments to the API availability and structure, data format and availability, and access. For example, data providers will need to develop APIs and format them to ensure that multiple authorized third parties can access the API across a range of products and services, while maintaining appropriate security. These changes will be costly and take years for even the largest entities to completely implement. Six months is simply not enough time given the proposed changes for even large, sophisticated entities to accomplish these goals.

Relatedly, authorized third parties will need significant time to build systems to work with APIs before they launch, so that the authorized third parties can continue to have access to covered data. Building these systems will take time and resources, especially because authorized third parties may need separate API connections for each provider. Authorized third parties will also need longer than six months to build the required authorization and revocation systems. Imposing too short of a compliance deadline could result in consumers having less access to covered data.

Moreover, no entity should be required to come into compliance with any final rule before the CFPB recognizes a standard setting body. The CFPB rightly anticipates

such standard setting bodies playing an important role in this field. It makes little sense to require compliance before such a body even has been recognized, let alone published QISs. Pushing forward with such an approach could lead to highly undesirable outcomes for the market and consumers. For example, a data provider might begin or even fully implement certain standards in order to meet the CFPB's proposed compliance date, only for the CFPB to later recognize a standard-setting body that has different QISs. This would create significant waste and inefficiency for those early adopting institutions, as well as unfair compliance risk and uneven cost distribution. Accordingly, entities should not be required to comply with a final rule any earlier than six months after the CFPB has recognized a standard-setting body.

Conversely, setting the compliance date after the CFPB has recognized a standard setting body (or bodies) would help to achieve greater initial consistency in the provision and flow of covered data by encouraging alignment around established standards. In contrast, if data providers have already started to implement a particular set of standards prior to CFPB recognition of a standard-setting body, they are less likely to shift course to a different set of standards. As a result, entity-specific preferences may get further entrenched.

Compliance with any final rule should not be required before the CFPB issues appropriate clarifying guidance such as a small entity compliance guide, model disclosures, illustrative commentary and examples, and examination procedures, as well as other regulatory implementation material the CFPB deems appropriate. This is especially important given the inherently novel nature of this rule. Particular issues that may require industry guidance may not fully present themselves until after the final rule is published and entities begin implementing its requirements.

For all these reasons, we believe that the CFPB should establish at least a two-year implementation period for even the largest data providers.

IV. The CFPB should finalize this rule before proposing a new rule regulating data brokers under FCRA.

The Proposed Rule appears to overlap with the CFPB's recently issued SBREFA outline considering amendments to Regulation V. If the CFPB were to issue a proposed rule on Regulation V without first finalizing the section 1033 rule, the finalized section 1033 and the proposed Regulation V rule could generate inconsistencies and confusion. In particular, it is unclear based on the Proposed Rule and the CFPB's SBREFA outline on Regulation V whether data providers could be considered data furnishers and/or consumer reporting agencies by virtue of providing covered data in order to comply with the section 1033 rule. Where concurrent rulemaking occurs by a single agency over a set of related activities or specific

product offerings, the ability for the public to meaningfully comment on each proposal as it relates to the other(s) is adversely impacted, if not outright impossible.

Given the potential significant consumer impacts and for purposes of regulatory and compliance efficiency, the CFPB should finalize this section 1033 rule before proposing a new rule regulating data brokers under FCRA. Regardless of timing, the CFPB should also ensure that the two rulemakings are consistent with each other, reflecting appropriately coordinated efforts.

* * * * *

We thank you for your consideration of these comments and would be happy to discuss these issues further.

Sincerely,

Bill Hulse
Senior Vice President
Center for Capital Markets Competitiveness
U.S. Chamber of Commerce