



January 25, 2023

Consumer Financial Protection Bureau  
1700 G Street, NW  
Washington, D.C. 20552

**Re: Rulemaking, Consumer Financial Protection Bureau; Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights (October 27, 2022)**

To Whom It May Concern:

The U.S. Chamber of Commerce Center for Capital Markets Competitiveness (“CCMC”) appreciates the opportunity to submit comments to the Consumer Financial Protection Bureau (“CFPB”) regarding its Outline of Proposals and Alternatives Under Consideration for the Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights<sup>1</sup> (the “Outline”).

CCMC welcomes this important and necessary rulemaking under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the “Dodd-Frank Act”). We strongly support maintaining secure consumer access to financial information. We agree that “by accessing their financial data, consumers are better able to manage their financial lives” and that ensuring secure consumer access to financial data can foster further competition, leading to new or improved products and services for consumers.

As the CFPB correctly recognizes, financial institutions and others in the financial services industry are subject to numerous statutory schemes regarding consumer data access, as well as the security and privacy of consumer data. Industry participants take these obligations seriously, and have invested significant time and money in developing technology to help consumers access data in secure ways. For example, the Financial Data Exchange consortium of data providers, data aggregators, data recipients, and other key industry participants has spent significant time and

---

<sup>1</sup> See CFPB, Outline of Proposals and Alternatives Under Consideration, Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights (Oct. 27, 2022), [https://files.consumerfinance.gov/f/documents/cfpb\\_data-rights-rulemaking-1033-SBREFA\\_outline\\_2022-10.pdf](https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf).

resources creating a framework for application programming interfaces that have notably enhanced data security and privacy for participants and their customers.

We substantially agree with portions of the CFPB's approach that build on existing market practices. That said, we believe that there remain opportunities to strengthen the CFPB's approach so that it better serves consumers and eliminates unnecessary burdens on market participants. In particular, we believe that the CFPB can do more to clarify the specific obligations for different members of the data sharing ecosystem and strengthen the security of consumer data sharing, which in turn will support the market pursuing greater innovation. We also believe the CFPB should strongly adhere to its obligations to minimize regulatory burdens imposed on small entities.

We appreciate the CFPB recognizing that promulgating a rule authorized under Section 1033 of the Dodd-Frank Act requires the agency to adhere to its obligations under the Small Business Regulatory Enforcement Fairness Act (SBREFA), but would encourage the agency to provide more attention to the concerns of small businesses. The CFPB correctly acknowledges that the rule may have a significant economic impact on a substantial number of small entities but devotes insignificant discussion to identifying options for limiting burden imposed on small entities, including indirect economic impacts. SBREFA requires the CFPB to collect the advice and recommendations of small entity representatives (SERs) concerning whether the proposals under consideration might increase the cost of credit for small entities and if alternatives exist that might accomplish the stated objectives of applicable statutes and that minimize any such increase.

Miscalibration of the Section 1033 rulemaking could lead to significant negative and unintended consequences and reverse incentives for consumers, as well as for innovation and competition within the marketplace more broadly. We accordingly write to ask the CFPB to carefully consider the following five points as it pursues its next steps in the Section 1033 rulemaking process:

- The CFPB should prioritize the security of consumer data while allowing market participants to continue to innovate.
- The CFPB should establish appropriate and tailored consumer disclosure requirements.
- The CFPB should allow data providers to impose reasonable limits on how third parties access and protect consumer data.
- The CFPB should avoid an approach under which data providers are subjected to unlimited liability for sharing data as required by law.

- The CFPB should partner with the prudential regulators to ensure that Section 1033 rulemaking is consistent with existing laws, regulations, and regulatory guidance.

### Analysis

#### **1. The CFPB should prioritize the security of consumer data while allowing market participants to continue to innovate.**

We agree that market participants should maintain appropriate security standards when making information available to authorized third parties. We agree that making information available in a way that does not rely on “an authorized third party possessing or retaining consumer credentials to authenticate the authorized third party could enhance consumer privacy, data security, and data accuracy.” Any Section 1033 rulemaking should require a sunset of the third-party use of consumer credentials to access consumer data.

Data providers should be permitted to require the use of certain secure methods of data access, such as API-based access. The marketplace has already developed innovative approaches for safe and secure consumer data access. The CFPB must not turn back the clock in favor of less secure approaches, such as credential-based access. Further, the CFPB should provide flexibility so that data providers can continue to create innovative third-party access methods that provide additional data security. Innovative third-party access methods could also lead to the development of new and improved products and services for consumers. Moreover, the CFPB should consider creating incentives for the adoption of more secure data-sharing methods, including through greater liability protections for companies that adopt more secure data-sharing methods.

#### **2. The CFPB should establish appropriate and tailored consumer disclosure requirements.**

As a part of any Section 1033 rulemaking, the CFPB should include requirements for third parties seeking to access consumer data to provide appropriate disclosures to consumers. Establishing disclosure requirements would enable consumers to make informed choices about whether, and to what extent, to authorize third parties to access data. These requirements should include ensuring that any such disclosures are easily accessible and understandable to consumers. At a minimum, disclosures must clearly outline the data obtained, the length and frequency of data access, instructions for revoking access, and the purposes for obtaining the data, including whether the third party may sell or otherwise share the data with other parties. The disclosure requirements under the Gramm-Leach-Bliley Act (“GLBA”) could provide a helpful starting point.

The CFPB should also develop model disclosures that accommodate the unique nature of data access transactions and allow reasonable modifications to accurately reflect the specific product or service. Through model disclosures the CFPB can demonstrate the elements of an effective and informative disclosure, as well as encourage compliance. Model disclosures should be consumer-friendly, and particularly consider readability on mobile devices and the flow of the transaction. Model disclosures also help promote consistency. Such consistency benefits consumers, particularly in enabling consumers to easily compare the terms of similar products or services.<sup>2</sup>

**3. The CFPB should allow data providers to impose reasonable limits on how third parties access and protect consumer data.**

**a. Time, place, and manner restrictions**

The CFPB should allow data providers to place reasonable time, place, and manner restrictions on how authorized third parties may access and use data. Authorized third-party access to data should be limited to the scope and frequency needed to support the authorized request. For example, most authorized use cases can be supported, at most, by a single daily data pull. In such cases, data providers should not be required to permit account mirroring, which requires real-time updates or hourly data pulls. Such unnecessary and overwhelming data access places a significant and undue burden on a data provider's infrastructure. Indeed, by burdening data provider systems, such unnecessary requests can degrade customers' experience in directly accessing their own accounts. In order to ensure consumers continue to have direct access to their account information, data providers should be permitted to impose limitations on third-party data access that are reasonable for the purpose of the data access.

Data providers should also be permitted to place a reasonable time limit on authorized third-party access. In addition, data providers should be allowed to continue to provide consumer control over data access, such as capabilities that allow consumers to revoke third-party data access rights, providing consumers with more control over their personal data. These features help consumers who have received the desired good or service from the authorized third party, or want to revoke access through the authorized third party. In addition, such features help consumers to keep track of the entities that are currently receiving their personal data.

The CFPB should work with financial regulators to establish a standard allowing market participants to maintain reasonable security. A data provider should have the

---

<sup>2</sup> Similar to the approach the CFPB has taken with respect to Remittances or Prepaid Account disclosures.

option to deny access to a third party that fails to meet such appropriate security standards.

#### **b. Confidential commercial algorithms**

The CFPB should not require data providers to share confidential algorithms used in their business processes nor data from which third parties could reverse engineer such confidential algorithms, consistent with the plain language of Section 1033.

Section 1033 specifically exempts a covered person from making available to the “consumer” any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors. This makes good sense; sharing such proprietary algorithms would greatly reduce their value, discouraging further innovation, creating market inefficiencies, and ultimately hurting consumers. Likewise, if data containing the output of confidential models were shared on a large scale, such as with an authorized third party collecting information on behalf of many consumers, confidential commercial tools—including proprietary algorithms—could be reverse-engineered. For example, even if the output of a confidential algorithm is not provided as a specific data field, a confidential algorithm may still be reverse-engineered by using other transaction data. This transaction data could also reveal confidential or material nonpublic information, including a company’s earnings and personal data that the consumer has not authorized a third party to receive. Accordingly, authorized third parties should also be limited in how they may use the various types of data they may receive. Such restrictions should travel with the data and apply even if an authorized third party sells the data to other third parties. Importantly, such limits would not restrict the ability of individual consumers to access their own data.

#### **c. Authentication and Authorization**

In any Section 1033 rulemaking, the CFPB should require that third parties are clearly authorized by the consumer to access particular data types and that consumers and third parties are appropriately authenticated.

Any Section 1033 rulemaking should ensure that third-party data access is limited to the types of data that a consumer has given informed consent to a particular third party to access. The CFPB should require informed consumer control and consent, consistent with the CFPB’s Consumer Protection Principles on Consumer-Authorized Financial Data Sharing and Aggregation. As the CFPB knows, these principles include:

Authorized terms of access, storage, use, and disposal are fully and effectively disclosed to the consumer, understood by the consumer, not overly broad, and consistent with the consumer’s reasonable expectations in light of the product(s) or service(s) selected by the consumer. . . .

Consumers understand data sharing revocation terms and can readily and simply revoke authorizations to access, use, or store data.”<sup>3</sup>

In particular, the CFPB should require informed consumer consent with respect to the specific types of data requested. The CFPB should permit data providers to obtain authorization from its consumers to share specified data with a particular third party, so long as the authorization process is reasonable and would not frustrate the intent of Section 1033. Data providers should also be permitted to authenticate consumers and third parties, so long as the authentication process is reasonable and would not frustrate the intent of Section 1033. Data providers and other industry participants have developed secure and seamless ways for data providers to authenticate consumers and third parties.

#### **d. Other proposed data sharing requirements**

Data providers should not be required to share data that is not typically shared today in the ordinary course of business, especially where the sharing of that data introduces safety and soundness risks to the marketplace. As the CFPB notes in the Outline, Section 1033 specifically excepts data providers from being required to provide the following information:

- any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors;
- any information collected by the data provider for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct;
- any information required to be kept confidential by any other provision of law; or
- any information that the data provider cannot retrieve in the ordinary course of its business with respect to that information.<sup>4</sup>

As detailed in this Letter, some of the proposals in the Outline appear to require sharing data that either is specifically excluded by statute or that if shared, create significant consumer security concerns.

---

<sup>3</sup> See CFPB, Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (Oct.18,2017), [https://files.consumerfinance.gov/f/documents/cfpb\\_consumer-protection-principles\\_data-aggregation.pdf](https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf).

<sup>4</sup> 12 U.S.C. § 5533(b).

For example, data providers should not be required to provide sensitive personal information such as demographic information or social security numbers, back-end payment processing information not typically shared with consumers, transaction-specific data, consumer reporting agency reports, or information on data security incidents. Providing these data elements to authorized third parties would not benefit consumers. In some cases, consumers are the true source of the information, not the data provider. Providing these data elements would increase the risk that personal consumer information would be exposed. By clearly excluding these fields in its forthcoming rule, the CFPB would strike the appropriate balance between consumer access to data and consumer protection from fraud, loss of access to funds, security breaches, and invasions of privacy.

Notably, consumers can receive the benefits of data sharing without actual sharing of sensitive data such as deposit account numbers. For example, data providers can provide tokenized deposit account and routing numbers to help ensure deposit account numbers remain secure. In addition, consumers are best positioned to directly provide highly sensitive data as they see fit, like race, ethnicity, or social security number to a third party, rather than this information being provided by a data provider. Doing so would help ensure the consumer truly intended to provide this sensitive information to a third party and did not inadvertently agree to provide this information because it was included in an extensive list of hundreds of data elements. We consequently would ask the CFPB to allow sharing of alternative data where possible and to require direct sharing of the most sensitive data.

The CFPB should not require sharing of information that data providers are already required to disclose to consumers. For example, entities that obtain consumer reports are subject to extensive requirements under the Fair Credit Reporting Act (“FCRA”) and Regulation B to notify consumers regarding credit pulls and adverse actions. Consumers are also able to obtain a consumer report from each of the three major consumer reporting bureaus annually for free. It is unclear how providing such data to an authorized third party would benefit consumers. Such data sharing could have negative consequences under FCRA if third parties use this information to evaluate consumers for credit, government benefits, or other products or direct advertisements to consumers and may be stale when subsequently used.

Lastly, the CFPB should not require data providers to share certain information described in the Outline that is not typically provided to consumers via online portals. For example, the Outline proposes requiring data providers to share certain payment routing and other transaction-specific information that is not typically displayed to consumers. We do not see a consumer benefit to providing this information. In contrast, providing all this additional information could be confusing to consumers, detract from more pertinent information, and potentially support bad actors in committing fraud and expose the payment ecosystem to additional security risks. If required, data providers

would need to build extensive new functionalities into their online portals, at significant expense, to provide consumers with this information, especially considering that the CFPB proposes providing this information in three formats.

**4. The CFPB should avoid an approach under which data providers are subjected to unlimited liability for sharing data as required by law.**

The Outline does not address liability for misuse of consumer data or other injury to consumers or data providers. Allocation of liability is an important practical consideration for any rulemaking under Section 1033. Data providers should not be required, for example, to make data available to any third party that does not take responsibility for the risks the third party creates, and data providers should be indemnified for any losses or costs that are caused by a third party. Further, data providers should not be required to make data available to a third party that cannot demonstrate meeting reasonable data security requirements. Failure to follow such principles would put consumer data at risk and create a mismatch between responsibility and liability that would not provide appropriate incentives for responsible behavior.

We consequently would ask the CFPB to address allocation of liability in a manner consistent with its statutory authority. While the CFPB has not addressed this topic to date, making it hard to provide specific comments, the CFPB should not require data providers to share data without being able to limit their liability as to a third party's use and maintenance of that data. Currently, data providers and data recipients allocate liability through contract, and should be permitted to do so going forward.

**5. The CFPB should partner with the prudential regulators to ensure that Section 1033 rulemaking is consistent with existing laws, regulations, and regulatory guidance.**

The CFPB requested feedback on whether any of the requirements imposed by the Electronic Fund Transfer Act, FCRA, the GLBA, the Truth in Lending Act, the Truth in Savings Act, and the Real Estate Settlements Procedures Act and their implementing regulations duplicate, overlap, or conflict with the CFPB's proposals under consideration. The CFPB also asked whether any other statutes or regulations could duplicate, overlap, or conflict with the proposal. We appreciate the CFPB's consideration of these key issues and encourage the CFPB to take seriously any concerns about contradictory or duplicative legal requirements. We highlight three such concerns below.

First, requiring data providers to provide consumer reports to authorized third parties could result in violations of FCRA. In addition, under their agreements with consumer reporting agencies, data providers are typically prohibited from sharing credit report data with third parties and it is important that the CFPB considers applicable



contract law. Persons other than consumers who obtain consumer reports must have a permissible purpose under FCRA. Authorized third parties should be required to obtain consumer reports under the terms and pursuant to the consumer disclosure requirements in FCRA. Providing consumer reports to authorized third parties without a permissible purpose could violate FCRA and allow authorized third parties to use the information contained in those reports to evaluate consumers for credit, government benefits, or other products, market information to consumers based on the information contained in the reports, or sell the information further downstream in a way that violates the law. The benefit of historical credit reports that may include bankruptcies, tradelines, or other information that would be inconsistent with the requirements of Section 605 and harm consumers is unclear.

Second, data sharing requirements could conflict with minimum requirements for risk management and conducting business with third parties imposed by the prudential regulators. Financial institutions that would be subject to the Section 1033 rulemaking hold extremely sensitive consumer data, such as social security numbers, deposit account numbers, and credit card numbers. The prudential regulators, and the CFPB itself, require regulated entities to meet certain minimum requirements for risk management and due diligence when engaging with third parties. The CFPB consequently should ensure that any standards imposed under Section 1033 are consistent with existing risk and third-party management obligations. Otherwise, data providers risk being subject to contradictory schemes that do not advance consumer protection or prudential interests in a coherent or effective fashion.

For example, requirements regarding data sharing could conflict with the Office of the Comptroller of the Currency's ("OCC") guidance on managing third-party relationships.<sup>5</sup> The CFPB and the OCC, along with other prudential regulators, should work together to establish a consistent approach to data sharing. Financial institutions must be able to comply with any Section 1033 rulemaking in conjunction with following the laws, regulations, and guidance of their prudential regulators.

Third, in addition to concerns arising under federal law, outlined above, the CFPB must consider how any Section 1033 rulemaking may overlap with existing state law requirements on data access, privacy, contract, technology, and security. Data providers and third parties should not be subject to conflicting or contradictory laws.

We note that the CFPB should also work with industry and prudential regulators to ensure that definitions relevant to any Section 1033 rulemaking are standardized

---

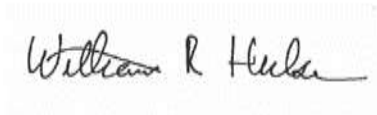
<sup>5</sup> OCC, Bulletin 2020-10, Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29 (Mar. 5, 2020), <https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html>.

across market participants and aligned with existing laws and regulations to reduce implementation friction and costs.

\* \* \* \* \*

We thank you for your consideration of these comments and would be happy to discuss these issues further. We look forward to reviewing the forthcoming report from the SBREFA panel and the solutions it identifies for minimizing regulatory burden.

Sincerely,

A handwritten signature in black ink that reads "William R. Hulse". The signature is written in a cursive style and is centered within a light gray rectangular box.

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