Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

P 202 371 0910

Writer's direct dial: +1 (202) 408-7407

CDIAONLINE.ORG

January 25, 2023

Via Electronic Delivery at Financial_Data_Rights_SBREFA@cfpb.gov

Consumer Financial Protection Bureau
1700 G St. NW
Washington, DC 20552

RE: Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights: Outline of Proposals and Alternatives Under Consideration

To Whom It May Concern:

The Consumer Data Industry Association submits this comment letter as written feedback to the Consumer Financial Protection Bureau's ("CFPB") Outline of Proposals and Alternatives Under Consideration for the Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights (the "Outline").[1]

The Consumer Data Industry Association ("CDIA") is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers' access to financial and other products suited to their unique needs.

CDIA members have been complying with laws and regulations governing the consumer reporting industry for decades. Members comply with the Fair Credit Reporting Act ("FCRA"),[2] which has been called the original federal consumer privacy law. The FCRA governs the collection, assembly, and use of consumer report information and provides the framework for the U.S. credit reporting system. In particular, the FCRA outlines many consumer rights with respect to the use and accuracy of the information contained in consumer reports. Under the

---

[1] Consumer Financial Protection Bureau, *available at* https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf (Oct. 27, 2022).
[2] 15 U.S.C. §§ 1681 *et seq.*

FCRA, consumer reports may be accessed only for permissible purposes, and a consumer has the right to dispute the accuracy of any information included in his or her consumer report with a consumer reporting agency ("CRA").

CDIA members have been at the forefront of consumer privacy protection. Fair, accurate, and appropriate use of consumer information is necessary for any CDIA member client to do business effectively.

The Outline and accompanying High-Level Summary and Discussion Guide of Outline of Proposals and Alternatives Under Consideration for SBREFA: Required Rulemaking on Personal Financial Data Rights ("Guide")[3] set forth an innovative process for consumers to exercise their personal financial data rights afforded to them under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank"). CDIA encourages the CFPB to use a guidance-based approach in drafting regulations under 1033, similar to the approach taken in Regulation V's Furnisher Rule, so as to not stifle innovation in the marketplace. CDIA provided comments to the CFPB's 2020 Advance Notice of Proposed Rulemaking[4] ("ANPR") to this effect and refers the CFPB to those comments for a more fulsome discussion on this point.

As the CFPB aptly points out in the Outline and Guide, many industry participants have been diligently working on creating processes that are consumer friendly and secure and have already invested significant time and money in this development. The CFPB should take care to support these innovative endeavors by drafting regulations that will help guide industry without risking valuable intellectual property or limiting creative solutions that would benefit industry and consumers alike. Thus, CDIA supports a guidance-based approach (or general framework) supportive of the hard work already invested by industry participants who are in the best position to set standards for best practices (**Question 57**).

Additionally, and just as importantly, the CFPB should take care to ensure that any regulation it drafts supports the consumer financial industry's responsibility to prevent fraudulent actors from obtaining access to sensitive consumer information. This is a responsibility that the consumer financial industry takes very seriously and embraces with consumer protection in mind. Thus, the CFPB's concerns about "fraud, privacy, and other consumer protection risks that could arise through compelling covered data providers to make available this information to authorized third parties" must guide the purview of the regulations that the CFPB ultimately drafts.[5]

---

[3] Consumer Financial Protection Bureau, *available at* https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA-high-level-summary-discussion-guide_2022-10.pdf (Oct. 27, 2022).
[4] Consumer Financial Protection Bureau, Consumer Access to Financial Records, 85 FR 71003 (Nov. 6, 2020).
[5] Outline, p. 23.

The CFPB has identified certain closely-related statutes and regulations in the Outline[6] and asks for feedback on whether "any of the requirements of the closely related statutes and regulations identified in Appendix C duplicate, overlap, or conflict with the CFPB's proposals under consideration" (**Question 1**).[7] The following points provide CDIA's comments with respect to areas of existing consumer financial services law that overlap with the CFPB's proposals contained in the Outline and suggested approaches given such overlap.

1. Consumer Report Information is Regulated Under the FCRA.

The CFPB proposes that a covered data provider would need to make consumer reports previously obtained from CRAs available as part of the "other information" covered data set.[8] The CFPB asks for feedback on potential challenges of requiring this information to be disclosed (**Question 29**).

For the reasons discussed below, CDIA strongly disagrees with the proposal that consumer reports provided to other financial institutions generally be available to consumers or third parties and requests that consumer reports and information derived from consumer reports be explicitly excluded from the definition of covered data. The FCRA and Regulation V are cited in Appendix C as closely related Federal statutes and regulations.[9]

First, the FCRA is at its core a privacy statute, designed to ensure that consumer report information is kept confidential,[10] with disclosure only under the enumerated circumstances identified in the FCRA. Allowing a third party to access consumer reports pursuant to consumer authorization from a covered data provider undermines this confidentiality tenet of the FCRA. Additionally, Section 1033(b)(3) of the Dodd-Frank Act states that "a covered person may not be required by this section to make available to the consumer . . . (2) any information required to be kept confidential by any other provision of law." Therefore, because the FCRA requires CRAs and end users to keep consumer reports confidential as a matter of law, the CFPB is prohibited from including consumer reports in the data set available under a 1033 request.

Second, the FCRA details specific requirements to access consumer report information, with fines and criminal penalties attaching for access to or provision of access under false pretenses.[11] Specifically, the FCRA requires that CRAs maintain reasonable procedures designed to require prospective users of consumer report information to "identify themselves" and the CRA must "make a reasonable effort to verify the identity of the new prospective user."[12] The FCRA also requires that a CRA obtain proper identification from a consumer prior to providing

---

[6] See Appendix C.
[7] Outline, Q1, p. 9.
[8] Outline, p. 23.
[9] Outline, p. 70.
[10] 15 U.S.C. § 1681.
[11] 15 U.S.C. §§ 1681(q), (r).
[12] 15 U.S.C. § 1681e(a).

a consumer with access to consumer report information.[13] Thus, CRAs are required to verify the identity of any requestor of consumer report information prior to providing the information. The CFPB's proposal to require covered data providers to provide consumer reports upon a 1033 request would undermine the FCRA's identity verification requirements without added benefit to the consumer.

Third, the FCRA specifies when a consumer report may be provided by an end user, such as a covered data provider, to a consumer directly. Section 607 states that a CRA "may not prohibit a user of a consumer report furnished by the agency on a consumer from disclosing the contents of the report to the consumer, if adverse action against the consumer has been taken by the user based in whole or in part on the report."[14] The FCRA is designed to encourage consumers to obtain their consumer report information directly from the CRA that provided the information to the end user,[15] and thus the FCRA does not restrict CRAs from prohibiting end users from disclosing consumer reports they have obtained directly to consumers outside of cases of adverse action. This approach facilitates more efficient dispute processing and allows the consumer to obtain the most up-to-date information available from the CRA. Accordingly, the CFPB's proposal that covered data providers make consumer reports available upon a 1033 request would be inconsistent with the FCRA.

Fourth, consumer report information provided by a CRA to a covered data provider often is not in a format that is usable to the average consumer. For example, a covered data provider may receive consumer report information from a CRA in a machine-readable format, where descriptions, headings and other helpful information is not readily apparent. Thus, a covered data provider would be required to provide a consumer with a hodgepodge of information readable only by a computer.

Further, a covered data provider may ingest the machine-readable consumer report information into a software application that parses the information into categories or data sets important to the covered data provider. It might be impossible in these instances for the covered data provider to then provide the consumer with a copy of the consumer report information originally obtained by the covered data provider. In this case, Section 1033(b)(3) of the Dodd-Frank Act is implicated: "a covered person may not be required by this section to make available to the consumer . . . (4) any information that the covered person cannot retrieve in the ordinary course of its business with respect to that information."

Fifth, there are significant intellectual property implications that could affect innovation and competition if the CFPB moves forward with requiring covered data providers to make available consumer report information upon a 1033 request. Just like companies in any other

---

[13] 15 U.S.C. § 1681h(a)(1).
[14] 15 U.S.C. § 1681e(c).
[15] *See, e.g.*, 15 U.S.C. § 1681g (requiring CRAs to provide file disclosures directly to consumers) and 15 U.S.C. § 1681m(a)(3) (requiring end users to provide consumers in their adverse action notice the contact information for the CRA that provided the report and advise them of their right to obtain a copy of their report).

industry, CRAs invest significant time and money in developing new products and services and improving existing products and services. Additionally, the covered data provider likely paid the CRA for the consumer report. Despite this, the covered data provider would then be required to make this report available to a third party at no cost. Allowing third parties to access these products and services at no cost and without going directly to the CRA would, therefore, actually lower the incentive for CRAs to innovate and could result in disclosure of trade secrets, harming consumers, and impacting commerce generally. As to innovation by covered data providers, any positive impact gained by downstream and secondary access to and use of consumer reports would be significantly outweighed by risks to consumers, including privacy risks (protected by the FCRA's permissible purpose limitations) and greater risks of unnecessary adverse action (where there is reliance on dated consumer reports that potentially contain information no longer current).

Sixth, requiring a covered data provider to include consumer reports in a covered data request does not fit within the scope or purpose of Section 1033 of the Dodd-Frank Act. "Section 1033 provides the consumer a statutory right to information that consumers could use to obtain a product or service from an entity other than the covered data provider or enable the consumer to better evaluate the consumer's use of a consumer financial product or service from the covered data provider."[16] Section 1033 was not intended to provide a back door to information governed and protected by the FCRA, which already provides for consumer access to the information.

Seventh, a consumer report obtained by a covered data provider from a CRA, potentially months or years prior to the 1033 request, would be unlikely to aid a consumer in evaluating the consumer's use of the product or service obtained from the covered data provider and another entity would be remiss to somehow use the consumer report to provide the consumer with products or services. Accordingly, including consumer report information under "other information" required by covered data providers to disclose would circumvent FCRA protections.

2. **Covered Data Providers Are Likely Financial Institutions Required to Comply with the Safeguards Rule.**

The CFPB states that: "nearly all—if not all—covered data providers must already comply with either the Safeguards Rule or Guidelines issued under the Gramm-Leach-Bliley Act (GLBA) . . ."[17] CDIA agrees with the CFPB on this point, as most covered data providers as defined in the Outline would also be considered financial institutions under the Safeguards Rule. The CFPB indicates that it is not considering adding additional data security requirements on a covered data provider's provision of a third-party access portal, except that the CFPB is considering requiring that a covered data provider authenticate a third party through a means

[16] Outline, p. 25.
[17] Outline, p. 35.

other than possession of the consumer's login credentials. The CFPB asks for feedback on its approach on data security (**<u>Question 69</u>**).[18]

CDIA agrees that the CFPB should not implement additional data security requirements given that covered data providers are likely financial institutions under the Safeguards Rule and thus subject to its requirements. As a fundamental security measure, CDIA agrees that a third party should not be granted access to customer information simply because the third party possesses the consumer's password or login credentials. This concept, however, is already addressed in the recent amendments to the Safeguards Rule through the requirement that a financial institution implement multi-factor authentication on all information systems that can be accessed by an individual.

The recently amended Safeguards Rule requires financial institutions to:

- Reasonably design an information security program that protects against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to the consumer.[19]
- Authenticate any individual accessing any information system using multi-factor authentication.[20]

An information system is defined very broadly as:

> a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing customer information or connected to a system containing customer information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains customer information or that is connected to a system that contains customer information.[21]

Multi-factor authentication is defined as:

> authentication through verification of at least two of the following types of authentication factors: (1) Knowledge factors, such as a password; (2) Possession factors, such as a token; or (3) Inherence factors, such as biometric characteristics.[22]

Given the broad definition of "information system," it appears that the third-party access portal would be considered an "information system" under the Safeguards Rule, thus already

[18] *Id.*
[19] 16 C.F.R. § 314.3.
[20] 16 C.F.R. § 314.5.
[21] 16 C.F.R. § 314.2(j).
[22] 16 C.F.R. § 314.2(k).

necessitating the implementation of multi-factor authentication on the portal. Thus, to avoid duplicative regulation, data security is not a topic that should be addressed under the CFPB's rulemaking.

3. The Identity of Third Parties Should be Verified and Their Access Request Authenticated.

Identity verification and authentication are complex and interdependent topics. As a starting point, if the covered data provider is required to comply with the Bank Secrecy Act or similar requirements, then the covered data provider has verified the consumer's identity during the course of the covered data provider's account relationship with the consumer. Once that consumer's identity has been verified, the covered data provider is then required under the Safeguard's Rule to use multi-factor authentication to authenticate a consumer as authorized to access the account information.

The CFPB has provided a helpful "Illustration of Interaction of Proposals Under Consideration (Third-Party Access)" ("Illustration") in the Guide of the next several steps in the process. Specifically relevant here is the first step under "Data Access" where the CFPB indicates that a covered data provider would need to receive "evidence of third party's authority to access consumer's information held by the covered data provider."[23] With respect to the third party's access, the CFPB has asked about methods that can be used to securely authenticate a third party without requiring a consumer to share credentials with the third party (**Question 70**). CDIA believes that this question is asking, in part, about whether possession of a consumer's credentials would be sufficient evidence of the third party's authority. CDIA agrees that possession of a consumer's credentials alone should not be considered sufficient evidence that the consumer has granted the third party authority to access the consumer's information. Rather, the third-party recipient should be required to provide something more affirmative to demonstrate the consumer's intention to provide an identified third party with access to the covered data.

Next, turning back to the Illustration, the third party's identity must be verified. The CFPB proposes that prior to providing covered data, CDIA believes that the first step is that a covered data provider would be "to receive information sufficient to authenticate the identity of the third party."[24] Confirming the third party's identity would be confirming that the third party is who it says it is. The CFPB requests feedback on this approach (**Question 80**). CDIA agrees with the CFPB's approach in that a third party should be required to provide proof of identity as a condition of access to covered data and the covered data provider would need to verify this information. In fact, without this initial step of identity verification, a covered data provider would have no way to determine whether the third party is who they claim to be or an imposter fraudulently accessing information. Consistent with CDIA's previous comments,

---

[23] *Id.*
[24] Outline, p. 38.

however, a guidance-based approach, similar to the Red Flags Rule,[25] would be more effective for the industry than specific and prescriptive procedures defined by the CFPB (**Question 81**).

The Red Flags Rule requires many businesses, and likely most covered data providers, to develop written identity theft prevention programs designed to identify and detect red flags of identity theft, take action against red flags, and periodically update the program.[26] The guidelines appended to the Red Flags Rule provide helpful risk factors and sources of red flags that financial institutions may use in developing their written identity theft prevention programs.[27] This approach should be a model for the CFPB in developing any identity verification requirements under its 1033 rulemaking authority.

Finally, turning back to the Illustration provided in the Guide, prior to the recipient being granted access to the covered data, CDIA believes the covered data provider needs to complete two tasks, in addition to receiving evidence of the third party's authority and confirming the third party's identity, to fully authenticate the third party. The covered data provider needs to authenticate that the recipient requesting access is the third party whose identity has been verified. While confirming the third party's identity means confirming that the third party is who it says it is, this additional task would be to confirm that the third party identified in the consumer's authorization is the recipient requesting access. A financial institution is already required under the Safeguards Rule to authenticate each individual that accesses an information system, and simple possession of a consumer's credentials would likely not satisfy the Safeguards Rule's multi-factor authentication requirements. Given that this is already a Safeguards Rule requirement, the CFPB does not need to implement any additional requirements in its 1033 rule related to the authentication of the third party. In addition, the covered data provider should be required to verify that the authorization presented by the recipient is from a consumer authorized to access the account held by the covered data provider.

4. **The Definition of Third Party Should Exclude Individuals and Certain Other Entities Subject to Other Federal Laws**.

The CFPB defines "third parties" as data recipients and data aggregators.[28]

> A "data recipient" means a third party that uses consumer-authorized information access to provide (1) products or services to the authorizing consumer or (2) services used by entities that provide products or services to the authorizing consumer... . A "data aggregator" (or aggregator) means ***an entity*** that supports data recipients and data providers in

[25] CDIA notes that the Red Flags Rule is not identified under the FCRA, but it is closely related to the various topics under consideration by the CFPB in its Outline.
[26] 16 C.F.R. §§ 681.1 *et seq*.
[27] Appendix A to 16 C.F.R. § 681.
[28] Outline, Footnote 9.

> enabling authorized information access. Depending on the context and its activities, a particular entity may meet several of these definitions.[29]

The term "data aggregator" includes in its definition the appropriate limitation that the third party be ***an entity***. The term "data recipient" however does not include in its definition the same appropriate limitation. CDIA urges the CFPB to use consistent language in its definitions to eliminate the likelihood of confusion. Thus, CDIA proposes that the definition of "data recipient" be revised as: "***an entity*** that uses consumer-authorized information access to provide (1) products or services to the authorizing consumer or (2) services used by entities that provide products or services to the authorizing consumer."

Additionally, CRAs offer some products and services under the FCRA directly to consumers that could require the CRA to obtain information directly from a covered data provider. For example, a CRA may allow a consumer to add positive information to a credit report after the CRA has verified the information with the financial institution holding the account with the consumer. In this context, the financial institution is not a furnisher of information directly to the CRA. Because the CRA is acting in its capacity as a CRA under the FCRA, the CRA is required to follow the requirements of the FCRA. For this reason, CDIA urges the CFPB to exclude from the definition of "third party" any entity that is offering a product or service to a consumer under a separate Federal statute or regulation such as the FCRA.

* * *

Thank you for the opportunity to respond to and share our views on the Outline and the Guide. Please contact us if you have any questions or need further information based on these comments.

Sincerely,

Eric J. Ellman
Senior Vice President, Public Policy & Legal Affairs

---

[29] *Id.* Internal quotations and citations omitted; emphasis added.