sifma

Invested in America

January 23, 2023

VIA E-Mail to Financial_Data_Rights_SBREFA@cfpb.gov

U.S. Bureau of Consumer Financial Protection
1700 G Street, 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

Dear Small Business Advisory Review Panel,

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to provide feedback on the above-referenced outline issued by the Consumer Financial Protection Bureau ("CFPB"). The outline invites feedback on the proposals under consideration that would implement section 1033 ("Section 1033") of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act"). In relevant part, Section 1033 establishes, subject to rules to be prescribed by the CFPB, a consumer's right to access information in the control or possession of a "covered person,"[2] including information related to any transaction, series of

---

[1] SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate on legislation, regulation, and business policy affecting retail and institutional investors, equity and fixed income markets, and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association ("GFMA"). For more information, visit http://www.sifma.org. SIFMA would like thank Courtney Dankworth, Jehan Patterson, and Catherine Morrison of Debevoise for their work on this letter.

[2] The term "covered person" is defined in section 1002(6) of the Dodd-Frank Act as "(A) any person that engages in offering or providing a consumer financial product

transactions, or their account including costs, charges and usage data and further provides that this information "shall be made available in an electronic form usable by consumers."[3]

SIFMA supports a consumer's right to access financial information in a safe and secure format and in a way that is designed to ensure responsibility and accountability for data aggregators and other parties that access such data, consistent with SIFMA's Data Aggregation Principles.[4] SIFMA is encouraged by the CFPB's efforts to promote consumer-friendly innovation and competition in financial markets. At present, however, there is still uncertainty regarding the types of information to be covered, information security, disclosures, access to information and the accuracy of information. There is also regulatory uncertainty around the potential unintended impacts of covered data providers sharing information with data aggregators or other third parties.

In SIFMA's February 4, 2021, comment letter ("2021 Comment Letter") on the advanced notice of proposed rulemaking ("ANPR"), SIFMA recommended that the CFPB provide additional clarity concerning the application of the security and privacy provisions of the Gramm-Leach Bliley Act ("GLBA") to data aggregators. SIFMA would like to thank the CFPB for now providing such clarification and encourage the CFPB to coordinate with other federal regulators to ensure the requirements imposed on institutions subject to the GLBA are similar to those applicable to data aggregators and non-regulated entities that are operating within this eco-system.

SIFMA's 2021 Comment Letter also recommended that the CFPB (i) limit the scope of data subject to Section 1033; (ii) require data aggregators to provide consumers with clearer disclosures; and (iii) support industry efforts to create interoperable standards that can accelerate innovation.

SIFMA appreciates the consideration that the CFPB has provided to several of the points as reflected in the outline. SIFMA believes the proposals could be further clarified and enhanced to ensure that consumers and its members are not unnecessarily burdened with requirements that lead to unintended consequences. In this regard, we recommend the following clarifications and amendments to the proposals:

- limit the scope of data subject to Section 1033;
- clarify provisions surrounding information security;
- retain proposed provisions regarding authorization disclosures;

---

or service; and (B) any affiliate of a person described in subparagraph (A) if such affiliate acts as a service provider to such person." 12 USC § 5481(6).

3 Pub. L. 111-203, Title X, § 1033(a); codified at 12 USC § 5533(a).

4 See SIFMA Data Aggregation Principles available here.

- support the implementation of industry standards regarding data access and portals;
- consider alternative approaches to ensuring data accuracy; and
- clarify the meaning of certain terms.

A. The CFPB Should Carefully Limit the Scope of Covered Data Subject to Section 1033.

Section 1033 covers a defined scope of information with several defined exceptions. Specifically, Section 1033 applies to "information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data."[5] Section 1033 does not apply to "(i) any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors; (ii) 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; (iii) any information required to be kept confidential by any other provision of law; or (iv) any information that the data provider cannot retrieve in the ordinary course of its business with respect to that information."[6]

The CFPB has indicated that it is considering requiring covered data providers to make the following information available:

(1) periodic statement information for settled transactions and deposits;

(2) information regarding prior transactions and deposits that have not yet settled;

(3) other information about transactions not typically shown on periodic statements or portals;

(4) online banking transactions that the consumer has set up but that have not yet occurred;

(5) account identity information; and

(6) other information.[7]

---

5 12 USC § 5533(a).
6 12 USC § 5533(b).
7 Outline p. 18.

SIFMA appreciates that the CFPB has identified categories of information that it may require covered data providers to make available. However, the proposal is very prescriptive and may result in burdensome implementation costs. For example, in recent years, the CFPB has implemented data minimization efforts by limiting the collection of information to what is needed to accomplish a stated purpose.[8] Requiring covered data providers to make directly available to consumers information such as credit reports appears to be contrary to the data minimization principles to which the agency itself adheres and could undermine the trust by consumers that financial institutions will take care with their information.

SIFMA also encourages the CFPB to define "other information" narrowly. Other than basic identity information needed to confirm identity on the account based on a particular use case (such as name, home address, and e-mail address), a covered data provider should not be required to make available information related to the identity and characteristics of the consumer account holder, including age, gender, race and ethnicity, even if such information is within the data provider's control or possession. While this information may be useful to certain authorized third parties, the sharing of this information with third parties increases a consumer's exposure to identity theft or other breaches of confidentiality, resulting in an unnecessary risk when balanced against the fact that the consumer is more capable of providing this information directly to a data aggregator. Accordingly, the CFPB should exclude such sensitive information from the scope of Section 1033.

"Other information" may also reveal sensitive market information when aggregated. SIFMA recommends that the CFPB coordinate with other federal financial regulators to consider the interplay between the scope of data subject to consumer access and currently undefined statutory terms including "confidential commercial information" or "information the institution cannot receive in the ordinary course of its business" to avoid unintended consequences resulting from access by third parties to data providers' sensitive market or proprietary information.

Furthermore, the CFPB should expressly provide that proprietary data relating to algorithms or artificial intelligence of financial institutions as it relates to their marketing, trading, or other areas of their business fall under one or more of the statutory exclusions. A proposed rule should make clear that financial institutions will not be required to share such information with third parties.

Lastly, the proposed rule's requirement to disclose consumer information should be crafted to avoid inadvertently subjecting covered data providers that do not meet the definition of "consumer reporting agency" ("CRA") under the Fair Credit Reporting Act to statutory obligations in connection with the sharing of consumer reports. Many covered data providers are prohibited by contract with the nationwide CRAs from

---

[8] See CFPB Privacy Policy available here.

disclosing to third parties consumer information received pursuant to those relationships. A proposed rule pursuant to Section 1033 should exclude such information to avoid inducing breaches of those contractual obligations or creating new, unintended legal obligations.

B. The CFPB Should Impose Security Requirements Commensurate with the GLBA.

In the 2021 Comment Letter, SIFMA encouraged the CFPB to prioritize the safeguarding of consumer financial data, regardless of how it is accessed or stored and provide clarity concerning the application of the security and privacy provisions of the GLBA. SIFMA would like to thank the CFPB for clarifying that it will not propose new or additional data security standards to those already imposed by the GLBA on covered data providers' third-party access portals. SIFMA further encourages the CFPB to ensure that any requirements imposed on covered data providers are similar to those applicable to entities that are operating in this ecosystem but are non-regulated or are less regulated.

C. The CFPB Should Ensure Any Authorization Disclosure Regime Adequately Protects Covered Data Providers from Liability After They Share the Information.

SIFMA encourages the CFPB to allow data providers to have discretion in handling data access authorizations. As currently contemplated, the CFPB is considering proposing that to be an authorized third party, a third party would need to provide the consumer an "authorization disclosure" soliciting the consumer's express, informed consent to certain disclosed key terms of access and certifying that it will abide by certain obligations regarding its collection, use and retention of consumer information accessed under the rule. In the 2021 Comment Letter, SIFMA encouraged the CFPB to require that data aggregators provide consumers with clearer disclosures about how their financial information will be used and shared. SIFMA commends the CFPB for clarifying disclosure requirements and encourages the CFPB to further refine the process.

At present, financial institutions often have limited control and information on how consumers choose to share their data with data aggregators. With the proposed requirement for a financial institution to turn over customer information, financial institutions should be provided with the opportunity to communicate with their consumer regarding the scope of information they are about to turn over to the aggregator. This opportunity will allow the financial institution to ensure that the customer did not unintentionally consent to turn over certain information to an aggregator. The financial institution can then tailor such information before sending it to an authorized third party to ensure that they will not be violating any regulatory guidelines imposed on them by their other regulators. Furthermore, financial institutions will likely categorize information in terms different from what a data aggregator's authorization disclosure requests, leading to compliance gaps for both the data provider and receiver. Therefore, SIFMA urges the CFPB to propound as part of a proposed rule a uniform authorization

disclosure request form that institutions may opt to use, and to provide a safe harbor exempting from liability institutions that use this form. Nevertheless, to permit financial institutions to maintain discretion in the process, the CFPB should alternatively allow such institutions to create an authorization disclosure that conforms to the manner in which they maintain consumer information and provide the consumer the option to avoid unintentional or inadvertent disclosures of certain information. However, use of the uniform authorization disclosure form should function as a safe harbor that exempts those institutions from liability arising out of an unauthorized disclosure.

Further, once consumer data information is obtained by third parties, covered data providers lack the ability to meaningfully control how it is used, aggregated or shared. Thus, SIFMA requests the CFPB to include in its rule an allocation of liability for downstream data; specifically, that covered data providers will not be liable for harm to consumers resulting from actions or omissions by authorized third parties with whom they are sharing information subject to the rule. In addition, the CFPB should clarify that covered data providers who are required to share licensed market data will not be held liable for any breach of license if the third party uses such information inappropriately.

The CFPB is also proposing that authorization disclosures to consumers include information regarding how to revoke access. In the 2021 Comment Letter, SIFMA encouraged the CFPB to consider developing options for providing consumers with a clear and easy method of terminating access to their data. Accordingly, SIFMA would like to thank the CFPB for including this in the proposals and urges it to adopt the provisions regarding revocation of access in a final rule.

D. The CFPB Should Support Industry Establishment of Standards for Consumer Data Access.

SIFMA continues to encourage the CFPB to support industry efforts to create standards that accelerate innovation and adapt to future technological advances. At present, there are generally two methods by which covered data providers make information available to third parties (1) through screen-scraping[9] and (2) via portal based on data-sharing agreements that do not require third parties to possess or retain the consumer's credentials. To this point, the CFPB is considering proposing that covered data providers establish and maintain a third-party access portal that would not require use of the consumer's credentials.

In the 2021 Comment Letter, SIFMA suggested that the CFPB require implementation of technologies that do not require consumers to turn over their log-in

---

[9] Screen-scraping occurs primarily by (1) using the consumer's user ID and password or like credentials to log into the data providers online portal on an automated basis(referred to as credential-based screen-scraping); and (2) granting a third party a token to access a portal(referred to as tokenized screen-scraping).

credentials to data aggregators or users, including an eventual transition from credential-based access to Application Programming Interface ("API") access. Accordingly, SIFMA would like to thank the CFPB for including this proposal. However, SIFMA encourages the CFPB to support industry efforts to create interoperable standards, rather than prescribe the means of authorized access. As is, implementation of the proposed third-party access portals could be costly to entities that lack in-house capability or expertise to establish and maintain portals and must instead hire and oversee a vendor to do so. Standards developed by the industry have the benefit of buy-in by parties that helped establish them and thus agree to abide by them. Therefore, SIFMA encourages the CFPB to allow industry stakeholders to collaborate in establishing a flexible framework best suited to facilitate consumer data access.

E. The CFPB Should Clarify Data Accuracy Standards

SIFMA encourages the CFPB to refine and expand on its current proposals for covered data providers to ensure the accuracy of information. Under the current outline, the CFPB first is considering requiring a covered data provider to implement reasonable policies and procedures to ensure that the transmission of information through the covered data provider's third-party access portal does not introduce inaccuracies. Second, covered data providers would be required to establish performance standards relating to the accurate transmission of consumer information through third-party access portals. Third, any conduct by a covered data provider that would adversely affect the accurate transmission of consumer information would be prohibited. Alternatively, the CFPB is also considering implementing a combination of those approaches.

In particular, the second proposed approach would appear to provide clear guidance to the industry by requiring the establishment of performance standards. The first and third proposals introduce standards that are less clearly defined— "reasonable policies and procedures" and "adversely affecting the transmission of consumer information," respectively—and therefore risk the mishandling of consumer data and could result in uneven protections afforded to consumers depending on the data provider or aggregator handling their information.

Additionally, the CFPB should clarify how financial institutions should handle information accuracy challenges from third parties once the information has been transmitted. For example, when a financial institution has transmitted data to a third-party and all of the proposed data accuracy standards have been satisfied internally, there is no guidance on how a financial institution should respond to a third party's claim that there are inaccuracies in the information. Therefore, the CFPB should clarify that all costs associated with challenges to the accuracy of information transmitted by a financial institution should be borne by the third party.

F. The CFPB Should Clarify the Meaning of "High-Risk" Secondary Uses

SIFMA encourages the CFPB to define "high-risk" secondary uses. When a data provider discloses consumer information to third parties, consumers are inadvertently subject to privacy risks. As information is shared between entities, there is a possibility that information may be misused for purposes not intended under Section 1033 or lead to negative market implications. Similarly, the consumer may not appreciate the scope of their data being transferred to third parties and the subsequent retention of such information.

Once third parties have obtained data from thousands of customers, there may be unintended consequences once they aggregate such data. For example, data collected from one data holder is often sufficiently anonymized. However, once combined with other data elements in the aggregator's possession, it may be possible for the aggregator or other third parties to re-identify particular individuals and ascertain sensitive personal attributes. In line with existing data minimization principles, the CFPB should clearly define "high-risk" secondary uses and require third parties to disclose how they will use and share consumer information.

Lastly, financial institutions should not be held liable for any unintended consequences associated with a data aggregator's use of data collected. Therefore, the CFPB should allocate liability for downstream data and specify that financial institutions will not be liable for harm to consumers resulting from actions or omissions by authorized third parties with whom information is shared pursuant to the proposals.

* * *

SIFMA appreciates the opportunity to provide feedback on the CFPB's proposals and would be pleased to discuss these comments in greater detail. If you have any questions or need any additional information, please contact me at mmacgregor@sifma.org.

Sincerely,

Melissa MacGregor

Melissa MacGregor
Managing Director and Associate General Counsel

Cc: Courtney Dankworth, Partner, Debevoise & Plimpton
Jehan Patterson, Counsel, Debevoise & Plimpton
Catherine Morrison, Associate, Debevoise & Plimpton