sifma

Invested in America

December 20, 2023

VIA E-Mail to 2023-NPRM-Data-Rights@cfpb.gov

U.S. Bureau of Consumer Financial Protection
1700 G Street, NW
Washington, DC 20552

Re: Docket No. CFPB-2023-0052 - Required Rulemaking on Personal Financial Data Rights

SIFMA[1] appreciates the opportunity to provide feedback on the above-referenced Notice of Proposed Rulemaking ("NPRM") issued by the Consumer Financial Protection Bureau ("CFPB").

The NPRM invites feedback on the CFPB's proposed rule to implement Section 1033 of the Dodd-Frank Act. In relevant part, Section 1033 establishes, in accordance with 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 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]

As stated in SIFMA's January 23, 2023, comment letter on the Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights Outline of Proposals and Alternatives Under Consideration for the Personal Financial Data Rights Rulemaking ("SBREFA Comment Letter"), SIFMA supports consumers' right to access their financial

---

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.

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 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 U.S.C. § 5481(6).

3 12 U.S.C. § 5533(a).

information in a safe and secure format.[4] SIFMA likewise continues to advocate for that access right to be achieved in a manner 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.[5] SIFMA is encouraged by the CFPB's efforts to promote consumer-friendly innovation and competition in financial markets. However, there remains uncertainty regarding definitions, access, data fields, industry standards and liability for misuse or misappropriation of shared information, and the proposed rule leaves many of these issues to be solved later by standard-setting bodies. There is also uncertainty around the potential unintended impacts of the proposal's limitation on access caps and prohibition on charging fees to request and access data.

Executive Summary

SIFMA believes the proposals should be further clarified and enhanced to ensure that SIFMA's members are not unnecessarily burdened with requirements that lead to unintended consequences without a tangible benefit to consumers' access rights under Section 1033. In this regard, SIFMA recommends the following clarifications and amendments to the proposals:

- address liability for shared information;
- amend the definition of consumer to mean current customer;
- impose and define access caps based on reasonableness;
- clarify the scope of covered data fields;
- amend the definition of covered data to exclude the sharing of payment initiation information;
- ensure that the final rule will not impose any recordkeeping requirements;
- allow the assessment of fees for market and reference data and reimbursement for reasonable costs associated with building, maintaining and making covered data available in the developer interface;
- ensure at least one standard-setting body is recognized pursuant to a public and transparent process and operating well in advance of the first compliance date and extend the first compliance date to two years after a standard-setting body has been recognized and issued qualified industry standards;
- amend the definition of qualified industry standards to be more prescriptive and implement guidelines for the promulgation of non-mandatory qualified industry standards;
- provide an explicit safe harbor so there is a rebuttable presumption of compliance when operating pursuant to the rule and qualified industry standards;
- clarify that Regulation E accounts held by Securities and Exchange Commission-registered entities are not within scope of the rule;
- clarify whether the final rule will apply to certain fiduciary accounts and ensure that the final rule will not conflict with a data provider's fiduciary duties;

---

[4] On February 4, 2021, in response to the advanced notice of proposed rulemaking published by the CFPB on November 6, 2020, SIFMA submitted a comment letter recommending among other things, that the CFPB limit the scope of data subject to Section 1033 and support industry efforts to create interoperable standards that can accelerate innovation.

[5] See SIFMA Data Aggregation Principles available here.

- clarify that certain data uses, such as information shared across institutions or within an institution among affiliates, are permissible;
- allow data providers to confirm the scope of their authorization with consumers regarding accounts and duration of sharing; and
- set a framework for diligence and supervision of authorized third parties and data aggregators.

A. The CFPB's Rulemaking Must Address Liability for Shared Information.

The CFPB's final rule should provide that liability follows the covered data—in other words, data providers must not be held liable for misuse or misappropriation of covered data that occurs once that data leaves their control in response to a request by an authorized third party. Under the proposed rule, the CFPB intends for liability to be agreed upon in the contract between the data provider and the third party, through network rules and/or commercial law. Bilateral contracts remain a helpful method by which data providers can address data safety and security concerns outside of the data provider's institution and ensure that they align with the data provider's own risk management practices. But the legal, operational and reputational risks of a data breach or misuse involving consumer financial information are too severe for all parties, including consumers, for the CFPB to delegate resolution to private contracts among industry participants of unequal sizes and negotiating power. The final rule will permit consumers to exercise a statutory right that the CFPB believes will be transformative in a shift to open banking. The CFPB's final rule should not remain silent on liability arising out of the exercise of that right.

Addressing liability in the final rule is necessary to avoid disparate results between regulated financial institutions and nonbanks that may operate outside regular supervisory processes. Indeed, even in a situation involving a data breach or misuse by a nonbank, the regulated institution may be subject to enforcement actions or other penalties notwithstanding a contractual allocation of liability that places responsibility for the misuse of data on the nonbank entity.[6] But unlike those situations governing a regulated institution's voluntary business relationships, authorized third parties within the meaning of the CFPB's proposed rule are not acting as service providers or vendors of the regulated institution, and it would be unfair to impose liability on the regulated institution for the conduct of an entity with which it may be required to disclose covered data under the rule. Accordingly, SIFMA encourages the CFPB to protect data providers from liability and regulatory scrutiny of an authorized third party's (or their service providers') mishandling of data that occurs after the data provider has otherwise provided covered data in compliance with the rule. Therefore, in the event of a bad-actor breach or a negligent third party spreading or misusing consumer information, the CFPB should clarify that liability, including enforcement of limited liability provisions under Regulation E and/or Regulation Z, will attach to the party that acted unreasonably in handling covered data and will not be imposed on the data provider for something that happens to the data provided in compliance with the rule once it leaves their control.

Leaving the crucial issue of liability for data breaches and unauthorized use to individual contract negotiations and implementation, as proposed under the NPRM, would conflict with the

[6] Third-Party Relationships: Interagency Guidance on Risk Management | OCC.

Bureau's policy objectives. As an initial matter, it would lead to inconsistent terms and practices, contrary to the CFPB's specific purpose of adopting a rule to establish dependable standards for the sharing and protection of consumer information. The problem is further exacerbated by the lack of privity between data providers and the ultimate third-party data recipients and their partners, vendors, etc., none of which would be bound by the contract terms except perhaps, at best, by the most attenuated chains of oversight by the contracting parties. Moreover, dominant market players (e.g., large data aggregators) could dictate the contract terms against smaller entities, negotiating away key compliance obligations and liability—including obligations to ensure compliance by third-party data recipients—while maximizing their access and use of consumer information. Addressing liability in the final rule ensures that smaller data providers that may lack leverage against large data aggregators will not be disadvantaged by imbalanced contract provisions that impose liability on them, even in part, when they played no causal role in the misuse or mishandling of covered data. Most important, the lack of definitive allocation of liability to each entity that comes into possession of consumer information would reduce the incentives for these entities (from data aggregators to third-party recipients, their partners and vendors) to expend the resources necessary to protect that consumer information from data breaches and unauthorized use, as compared to focusing on maximizing their access and returns.

In short, the CFPB's allocation of liability by regulation is essential to incentivize all parties, including data aggregators and third-party recipients, to protect consumer information against data breaches and misuse, as well as to ensure consistent practices across the ecosystem. SIFMA encourages the CFPB to allocate joint and several liability for parties that obtain consumer information from data providers pursuant to the rule and share that information with third parties, thus maximizing their incentives to maintain oversight to protect the integrity of the information.

In addition, SIFMA encourages the CFPB to clarify that sharing information pursuant to Section 1033 does not grant a license to the recipient of data nor constitute furnishing credit information to a credit reporting agency ("CRA") if the recipient data aggregator or broker ultimately is deemed by the CFPB to be a CRA, as is currently under consideration by the CFPB's Fair Credit Reporting Act ("FCRA") rulemaking. For example, where licensed information flows when providing information pursuant to the rule, the CFPB should clarify that the sharing of such information does not negate the obligations of an entity to obtain a license to use such data. Therefore, the final rule should state that where licensed data is shared in compliance with the rule, the data provider does not provide a license to the recipient by virtue of sharing such information. The final rule likewise should make clear that disclosure of covered data does not constitute the furnishing of credit information to a CRA if the recipient data aggregator or broker ultimately is deemed by the CFPB to be a CRA.

B. The CFPB Should Amend the Definition of Consumer.

SIFMA encourages the CFPB to amend the definition of "consumer." As is currently contemplated, "consumer" means "a natural person." However, SIFMA encourages the CFPB to amend the definition to specify that a consumer is a natural person "that has at least one current account with the data provider." From a risk perspective, the financial and other information of former customers of a data provider is not maintained in the same way that current client information is maintained. Specifically, the ability for a former customer to access the consumer interface may differ from those methods used by customers with current accounts. As such, it

would be overly burdensome and is likely to require at least some data providers to undergo significant changes to current policies, procedures and platforms to require data providers to retrieve and provide information in the manner contemplated by the proposed rule.

While former customers are likely to continue to have the ability to access information under existing industry standards and practices in ways similar to current consumers, the NPRM proposes a significant change in the ways data is made available that would frustrate many of the CFPB's 2017 Consumer Protection Principles[7] if the CFPB were to include a former customer in the definition of "consumer." Moreover, requiring data providers to furnish information that is outdated and stale to former customers would not appreciably advance the portability objectives underpinning the Section 1033 access right. Therefore, SIFMA encourages the CFPB to amend the definition of the term "consumer" to clarify that it only pertains to current customers.

C. The CFPB Should Definitively Impose and Define Access Caps.

SIFMA encourages the CFPB to impose reasonable access caps to aid data providers in meeting performance standards, mitigate initial and ongoing compliance costs associated with Section 1033 rulemaking and further the CFPB's goal of making sure the data being accessed is truly needed to provide the consumers' authorized product or service. As currently contemplated, unless otherwise subject to specific, narrow exceptions, a data provider must not unreasonably restrict the frequency with which it receives and responds to requests for covered data from an authorized third party. Instead, it may restrict frequency only where permitted under Sections 1033.321, 1033.331(b) and (c) and in a manner that is non-discriminatory and consistent with the data provider's reasonable written policies and procedures. SIFMA appreciates the CFPB allowing for frequency restrictions under limited circumstances but encourages the CFPB to permit data providers to prescribe broader limits on both the frequency and quantity of requests to meet the specific product or service. For example, depending on the size and systems of a data provider, multiple or repetitive requests each day for all covered data in the possession of a data provider could cause systems outages, impede consumer access through the consumer interface or alternatively slow the production of the requested information, rendering data providers out of compliance with the final rule's performance standards while hindering other regulatory obligations that depend on systems availability.

In other instances, it may make sense to permit data providers to restrict access when a third party makes multiple or repeated requests for information that is unlikely to change often, if at all. Such information includes basic account verification information, an account's terms and conditions or information to initiate payments to or from a Regulation E account. For example, the complete terms and conditions for a Regulation E account or Regulation Z credit card product typically involve a considerable amount of data that would render delivery in response to repeated requests unmanageable for data providers' systems, particularly if the final Section 1033 rule requires a machine-readable format other than the PDF format that is currently used to deliver such information. SIFMA believes a final rule that limits the sharing of an account's terms and conditions to those that directly implicate the costs to a consumer of a covered financial product or service (such as the annual percentage rate or annual percent yield) would best align with

[7] CFPB, Consumer Protection Principles available here.

Section 1033's text and purpose to facilitate the flow of information to "relating to any transaction, series of transactions, or to the account including costs, charges and usage data."[8]

Specific use cases also would render subsequent requests for certain covered data or repeated requests for covered data unreasonable. For example, if an authorized third party needs information to initiate a single payment, requesting information repeatedly after the consumer initiates the payment is not necessary. The general limitation on collection, use and retention under proposed Section 1033.421(a) does not do enough to prevent repeated and unnecessary data requests from an authorized third party in the absence of data caps. As such, the CFPB should impose access caps limiting the quantity and frequency of requests, given that unlimited requests may become overly burdensome and, among other things, impact the performance of the developer interface and significantly increase compliance costs and risks to the consumer data with little, if any, benefit to consumers.

Lastly, when a third party seeks to obtain information without otherwise complying with applicable requirements of any final rule, it should be *per se* permissible for a data provider to block access by that third party through both the consumer and developer interface, as applicable.

D. The Final Rule Should Clarify the Scope of Covered Data Fields.

The CFPB should define the scope of covered data fields prior to adopting a final rule. The NPRM proposes that data fields will be defined by a qualified industry standard that will be issued by CFPB-recognized standard-setting bodies. To be a standard-setting body, an entity may request that the CFPB recognize it as an issuer of qualified industry standards. However, under the proposed rule, a standard-setting body may not be recognized or issue qualified industry standards sufficiently in advance of the first proposed compliance date. The consequent lack of clarity regarding covered data fields would lead to inconsistent implementation across the data ecosystem, leading to consumer confusion as well as increased potential for delay, error and cost of compliance. It also would likely reduce any compliance cost savings the CFPB's own cost-benefit analysis appears to assume from the establishment of a standard-setting body and qualified industry standards. Accordingly, at a minimum, the CFPB should provide clarity and define the scope of covered data fields before the first compliance date. In particular, SIFMA encourages the CFPB to define "data fields" as "a piece of data that relates to a consumer financial product or service that the consumer has contracted for with the data provider."

E. The CFPB Should Amend the Definition of Covered Data to Exclude Payment Initiation Information.

The CFPB should revise the proposed definition of "covered data" to exclude "information to initiate payment to or from a Regulation E account." First, including payment initiation information is beyond the scope of the CFPB's authority under the Consumer Financial Protection Act of 2010 ("CFPA") to prescribe rules to require covered data providers to make available upon a consumer's request information "concerning the consumer financial product or service that the

[8] 12 U.S.C. § 5533(a).

consumer obtained from such person." By its terms, information "concerning the consumer financial product or service" does not encompass information that concerns money movement.[9]

Furthermore, mandating data providers to share information that allows the enabling of payments to a third party may also increase risks within the payments ecosystem. Specifically, it potentially increases systemic risk and exposes consumers to the risk of unauthorized payment initiation by third parties that currently may not bear full responsibility for addressing customer inquiries and disputes regarding payments, data breaches, or fraud. It also: (1) forces data providers to assume risks and costs for which they are not compensated, from investigating and resolving inquiries and disputes, to bearing losses on transactions where Regulation E gives consumers liability protection; (2) requires data providers to become uncompensated insurers for fraud and scam risks; and (3) poses reputational, regulatory, and political risks to data providers stemming from their obligations to make customers whole, when such risks cannot be easily mitigated.

In addition, this mandate also expands "pay-by-bank"—which allows consumers to pay merchants directly using their bank's Automated Clearing House rails—to new use cases for which it is not fit, which in turn will decrease consumer protections. Thus, as proposed, financial institutions offering a Regulation E account will be at a significant disadvantage compared to other data providers because they will bear potential liability for actions by non-affiliated third parties that violate Regulation E.

Moreover, disclosure of payment-initiation information could pose reputational, regulatory, and political risks to data providers that cannot easily be mitigated because Regulation E requires financial institutions to make customers whole for unauthorized funds transfers. Responsible management of these systemic and consumer risks requires the CFPB to undertake a comprehensive review of the current regulatory framework under Regulation E in close coordination with other prudential regulators. This is necessary to identify and make revisions to Regulation E that ensure that third party payment initiators are responsible for the risks they create and to appropriately align rights and responsibilities to those engaging in the marketplace. Unless and until that review occurs, however, the CFPB should delete "information to initiate payment to or from a Regulation E account" from the definition of covered data.

F. The Final Rule Should Not Impose Any Recordkeeping Requirements.

The proposed rule requires data providers to maintain all records of both covered data made available and not made available through a consumer interface for three years.

Section 1033(c) instructs that the CFPB may not "impose any duty on a covered person to maintain or keep any information about a consumer."[10] The proposed rule's broad requirement for data providers to maintain records for three years is thus incompatible with the statutory language. The three-year recordkeeping requirement is also inconsistent with the 24-month retention periods in Regulation E and Regulation Z to which data providers are already subject, without any accruing

[9] 12 U.S.C. § 5533(a).

[10] 12 U.S.C. § 5533(c).

benefits to consumers attributable to that additional year. In fact, the additional year poses unnecessary data security risks and costs and thus does not serve the purposes of Section 1033.

The final rule should not—consistent with Section 1033's language and purpose—impose any recordkeeping requirements about a consumer and instead only require a retention of records for two years, aligning with the applicable record retention period for the substantive regulations within scope, sufficient to demonstrate compliance with applicable provisions.

G. The CFPB Should Allow Data Providers to Recover Costs Associated with Making Data Available in Certain Instances.

The CFPB should allow data providers to recover reasonable costs associated with building, maintaining and making available covered data through the developer interface. Doing so would recognize the significant costs that data providers will incur to come into compliance with the rule and respond to data requests. It would also avoid undesirable disparities whereby national banks may charge fees that are incidental to permissible banking activities under the National Bank Act, but non-nationally-chartered banks and nonbank data providers are prohibited from doing the same.

1. Prohibiting Data Providers from Recovering Their Significant Compliance Costs May Result in Decreased Consumer Access to Covered Products and Services.

There are significant costs associated with changes required to comply with the NPRM, even in instances when a data provider has an Application Programming Interface ("API") established to share certain data with a third party. That is because, under the proposed rule, the API must be made available to an unknown number of third parties.[11] Given the proposed rule's systems performance requirements and restrictions on a data provider's discretion to cap data requests, the NPRM fails to account for significant ongoing costs of developing and maintaining the developer interface. Initial estimates for some data providers to come into compliance with the proposed rule could be as much as $100 million in the first year with ongoing maintenance costs of approximately $15 million beyond what is currently spent to provide consumers and third parties with covered data through existing APIs. The inability of data providers to recover some or all of those additional costs is likely to significantly impact access by consumers to covered products or services, an issue that may be exacerbated if the CFPB continues to take the general position that any imposition of fees impedes a consumer's ability to obtain information about a financial product or service.[12] Thus, SIFMA encourages the CFPB to permit data providers to recover reasonable costs associated with developing and maintaining the developer interface.

---

[11] Authorized third parties, in turn, will need to configure their systems to support establishment of multiple and separate connections with data providers.

[12] *Infra*, n.17 at p. 10. ("As a general matter, requiring a consumer to pay a fee or charge to request account information, through whichever channels the bank uses to provide information to consumers, is likely to unreasonably impede consumers' ability to exercise the right granted by section 1034(c), and thus to violate the provision. Some consumers cannot afford to pay even a small fee to obtain information about their accounts. Even for consumers who can afford such fees, the fees can operate as a significant deterrent to making an information request").

The CFPB's proposal further fails to account for costs incurred by data providers to protect consumer data and make such data available across use cases.[13] Specifically, data providers will have high costs to enable the safe data sharing required under this regulation. Furthermore, making available certain market and reference data in the manner required by the CFPB's proposal requires the data provider to pay to license that data, a cost for which the proposed rule does not appear to account. And providing covered data for certain use cases will require data providers to incur different costs depending on the data requested because certain use cases (such as facilitating payments) require more resources and processes than other use cases (such as data shared to a third party to provide consumers with a holistic view of their financial standing). For example, Regulation E imposes obligations on financial institutions to address error resolution claims. Significant resources are required to investigate disputed payments. Consumers have and will continue to rely on their financial institution to address their error resolution claims, even when a data aggregator or other third party would be the appropriate party to investigate and resolve such claims. Financial institutions should be able to at least partially recoup expenses for maintaining the developer interface to avoid the inequitable result of data aggregators and third parties that reap the benefits of the developer interface and data access but bear none of the associated costs. Therefore, SIFMA strongly encourages the CFPB permit data providers to recover reasonable costs associated with certain use cases because of the burdens producing such documents places on data providers.

Indeed, as Section 1033 implicitly realizes, consumer data has value, and the costs associated with providing that data should be spread among those benefiting from its collection and use. The proposed rule's failure to permit data providers to recover costs associated with making data available to authorized third parties—including those for secondary uses as discussed in Section M, in which information is not made available in turn to consumers—encourages free riding while increasing costs to consumers for "covered consumer financial product[s] or service[s]" that millions of consumers use daily. The CFPB should not propose rulemaking that is likely to reduce consumer access to consumer products or services by making markets less competitive or assigning costs only to certain market participants, especially where a reasonable and easy fix is otherwise available.[14]

By permitting data providers to recover reasonable costs associated with making the data available, the market—not the CFPB—will determine a reasonable cost balancing approach and do so from a pro-competitive perspective.

2. Prohibiting Data Providers from Charging Fees for Access Is Inconsistent with Other Federal Law and the CFPB's Own Guidance.

The proposed rule's prohibition on data providers from charging fees in response to making data available under this rule is inconsistent with other federal law and CFPB interpretive guidance. The proposed rule purports to define as the offering of a consumer financial product or service as "providing financial data processing products or services by any technological means, including processing, storing, aggregating or transmitting financial or banking data, alone or in connection with another product or service, where the financial data processing is not offered or

[13] § 1033.301(c).

[14] 12 U.S.C. § 5512(b)(2)(A)(i).

provided by a person who, by operation of 12 U.S.C. 5481(15)(A)(vii)(I) or (II), is not a covered person".[15] But the National Bank Act and its implementing regulations provide that national banks may, subject to certain conditions, "charge its customers non-interest charges and fees, including deposit account service charges."[16] Failing to reconcile the final Section 1033 rule with the National Bank Act's regulations means national banks will have conflicting federal regulations directly on point with respect to the permissibility of certain charges and fees on its customers.

A blanket prohibition on fees likewise is inconsistent with the recent CFPB Advisory Opinion interpreting Section 1034(c) of the Dodd-Frank Act as allowing large banks in certain instances to assess fees for repeated requests for information already provided. The final rule should permit data providers to impose a fee or charge in circumstances where, for example, the data provider has repeatedly received and produced information on the same request. In this circumstance, the data provider would have already met its obligation and the information is unlikely to materially change (*e.g.*, providing the terms and conditions repeatedly to the same authorized third party).[17]

H. The CFPB Should Extend the First Compliance Date.

SIFMA encourages the CFPB to recognize at least one standard-setting body well in advance (at least 12 months) of the first compliance date, which is currently contemplated to be six months after the publication of the final rule. In addition, any standard-setting bodies that seek to be recognized by the CFPB will likely need time to establish an appropriate governance structure, secure funding mechanisms and create programs that aid data providers in coming into and remaining in compliance.[18] Further, SIFMA encourages the CFPB to ensure that its own recognition process is transparent and solicits participation from interested public stakeholders. Doing so adheres to principles of good government and offers the benefit of increased industry acceptance of any recognized standard-setting body. That public input process itself will take time that the CFPB should consider in establishing the final rule's first compliance date.

Qualified industry standards need to be established with sufficient time to redesign the backend frameworks in order for the data provider to avail themselves of the reduced costs that such standards offer. In addition, no such body is currently recognized in the United States, and the NPRM fails to account for the lead time that is required for any such body to commence functioning as a standard-setting body and establish qualified industry standards consistent with the final rule as well as the time for market participants to implement such standards. In the absence of a standard-setting body by the first compliance date, data providers and authorized third parties alike will need to expend additional resources to design and implement their own compliance programs. This could result in inconsistent and uneven data access by consumers and greater costs

---

15 § 1001.2(b).

16 12 CFR § 7.4002.

17 CFPB, Consumer Information Requests to Large Banks and Credit Unions (Oct. 2023), https://files.consumerfinance.gov/f/documents/cfpb-1034c-advisory-opinion-2023_10.pdf.

18 As of the date of this letter, the Financial Data Exchange ("FDX"), a nonprofit industry standards body that is dedicated to unifying the financial services ecosystem around common, interoperable and royalty-free technical standards for use-permissioned data financial data sharing, is the entity operating in the United States that comes closest to the proposed rule's criteria for recognition by the CFPB.

not otherwise accounted for by the CFPB, leading to a significantly higher burden or reduction in products or services offered given that, as proposed, the rule would not permit entities to recoup their costs.

SIFMA encourages the CFPB to comply with the required standards for CFPB rulemaking in 12 U.S.C. § 5512(b)(2) and reduce the impact on covered persons while increasing consumer benefits, in contrast to the NPRM's approach that risks significantly reducing access to consumer financial products or services while also increasing the compliance burden on covered persons.

Furthermore, even advanced institutions will have to build out programs, appoint personnel for monitoring requests, tag updates to identify requests and update processes to include and retain data as required by the rule. Building out that capability will be more complicated and costly in the absence of a standard-setting body and associated qualified industry standards. Moreover, smaller firms likely will need to limit access requests in connection with secondary uses to instead devote resources to building disclosure and reauthorization systems to come into compliance with the proposed six-month timeline, which will have the undesirable consequence of reducing consumers' access to data from current levels. SIFMA encourages the CFPB to provide that compliance with the final rule should not be required until two years after a standard-setting body is recognized or one year after qualified industry standards for applicable provisions are issued.

I. The CFPB Should Amend the Definition of Qualified Industry Standards and Implement Guidelines on the Promulgation of Qualified Industry Standards.

SIFMA encourages the CFPB to include a more prescriptive definition of what may be considered a "qualified industry standard" and to implement guidelines for standard-setting bodies to issue such standards. In the SBREFA Comment Letter, SIFMA encouraged the CFPB to support industry efforts to create standards that accelerate innovation and adapt to future technological advances. Accordingly, SIFMA commends the CFPB for including the issuance of qualified industry standards by standard-setting bodies. As currently contemplated, the term "qualified industry standard" is defined as "a standard issued by a standard-setting body that is fair, open and inclusive in accordance with Section 1033.141(a)." As drafted, the definition in proposed Section 1033.141(a) is vague and duplicative. For example, the CFPB proposes that an indicia that performance of the interface is commercially reasonable includes that, among other things, it "meets the applicable performance specifications" set forth in qualified industry standards or achieved by the developer interfaces. As contemplated, the meaning behind these terms is unclear, especially when the qualified industry standards are not already established. SIFMA encourages the CFPB to provide clarification around these points while retaining flexibility for recognized standard-setting bodies to meet consumer and industry needs to deliver covered data to the consumer in a secure and efficient manner.

In addition, SIFMA encourages the CFPB to clarify that any qualified industry standards must be specific and measurable. Specifically, the CFPB should specify guidelines by which qualified industry standards must be promulgated. For example, the CFPB should require that qualified industry standards (1) address what a customer can direct their financial institution to share with a third party electronically and (2) ensure that a customer's credentials must not be exposed to any third party during the fulfillment of the request. At the same time, compliance with such standards should not be mandatory, nor should a recognized standard-setting body be granted

the power to enforce such standards. The final rule should permit data providers flexibility to otherwise comply in ways that align with the substantive requirements, including recognizing that, on occasion, denying access to data may be required to comply with prudential regulators' risk management expectations.

J. The CFPB Should Allow a Safe Harbor for Compliance with Qualified Industry Standards.

SIFMA encourages the CFPB to implement a safe harbor so there is a rebuttable presumption of compliance when operating pursuant to the substantive provisions of the rule and qualified industry standards. As currently contemplated, the CFPB proposes an indicia of compliance that a data provider's data accuracy policies and procedures are reasonable if they conform to a qualified industry standard. As the CFPB is strictly defining the requirements to become a standard-setting body while also placing considerable power in standard-setting bodies, SIFMA strongly encourages the final rule to provide that data providers will not be subject to enforcement or supervisory actions or penalties if they are conducting business in compliance with qualified industry standards. Where questions of compliance with qualified industry standards arise, the standard-setting body should be tasked with determining an answer to those technical questions, as it is best positioned to do so.

Alternatively, the CFPB could reduce the number of required attributes to become a standard-setting body while also providing an indicia of compliance where an entity complies with applicable qualified industry standards. The CFPB could also establish a process through which qualified industry standards are submitted for non-objection; when an objection is not made within a reasonably short timeframe (*e.g.*, 30 calendar days), it is deemed to be a safe harbor for at least two years (or an equivalent period to the record retention requirements within the final rule). This higher level of assurance will incentivize data providers to participate in standard-setting processes that will facilitate industry buy-in, create efficiencies, reduce the likelihood that consumer data will be misused and signal to the market that in addition to the substantive provisions of the rule, these standards may be relied upon.

K. The CFPB Should Clarify that Regulation E Accounts Held by Securities and Exchange Commission-Registered Entities Are Not in Scope.

The CFPB has no authority to "exercise any power to enforce" Title X of the Dodd-Frank Wall Street Reform and CFPA against any "person regulated by the [Securities and Exchange] Commission" ("SEC"),[19] defined by the CFPA to include certain persons that are required to be registered either under certain federal securities laws or with the SEC itself, and certain of their employees, agents or contractors.[20] The proposed rule, however, applies to Regulation E accounts and data providers that are synonymous with Regulation E's definition of financial institutions without regard to the jurisdictional exclusion for SEC-registered persons.

By its terms, Regulation E generally applies to all financial institutions, with certain exceptions made for "person[s] excluded from coverage of this part by section 1029" of the

[19] 12 U.S.C. § 5517(i)(1).

[20] 12 U.S.C. § 5481(21).

CFPA.[21] Section 1029 in turn is the CFPA's jurisdictional exemption for auto dealers. Thus, by failing to make express allowances for the CFPA's jurisdictional exemption, the proposed rule sweeps too broadly to potentially encompass accounts that may meet Regulation E's definition but that are offered by SEC-registered persons over which the CFPB cannot exercise authority. The CFPB's final rule must make clear that accounts held by financial institutions within the scope of Regulation E are nonetheless exempt from the final Section 1033 rule if those accounts are held by SEC-registered persons within the meaning of 12 U.S.C. § 5481(21).

L. The CFPB Should Clarify the Treatment of Trust Accounts and Ensure that the Final Rule Will Not Conflict with a Data Provider's Fiduciary Duties.

SIFMA encourages the CFPB to further clarify the treatment of trust accounts. As proposed, the final rule would define the term "consumer" as a natural person, including a trust established for tax or estate planning purposes. However, a trust is neither a natural person nor a legal representative of a person. Rather, it is a separate legal entity with a separate tax identification number. Further, the proposed rule defines a "covered consumer financial product or service" as an account defined in Regulation E, but accounts held pursuant to a bona fide trust agreement are carved out of the definition of account for Regulation E.[22] Therefore, the CFPB should clarify whether the final rule will apply to fiduciary accounts where a national bank acts as trustee and/or executor of a trust or estate that distributes fiduciary funds, electronically or otherwise, to an individual.

In addition, SIFMA encourages the CFPB to further clarify that a final rule will not require certain information and associated commentary related to trust accounts to be disclosed to third parties in violation of a data provider's fiduciary duties. Fiduciary accounts involving trust and estates often involve multiple beneficial interests for which banks have a duty to maintain the confidentiality of beneficiary data and records among various beneficiaries of the account. Indeed, this may mean that information provided to the bank to execute the distribution of funds per the terms of the instrument by one beneficiary is restricted from disclosure to the other beneficiaries of the trust. Moreover, aggregated trust account data is not appropriate where beneficiaries' entitlements may vary, and thus aggregation of amounts would convey an inaccurate impression as to the amounts each beneficiary may be entitled to receive. Therefore, SIFMA encourages the CFPB to ensure that a final rule will not put data providers with fiduciary duties at risk of either not complying with the requirements under the final rule or providing potentially unclear information.

M. The CFPB Should Clarify that Certain Data Uses Are Permissible.

SIFMA encourages the CFPB to clarify that certain information shared across institutions or within an institution among affiliates is not prohibited within the scope of the rule. For example, some firms utilize aggregating software to provide financial providers with access to information on accounts from multiple different data providers. In addition, information may be shared among affiliated entities in their daily operations. As such, SIFMA encourages the CFPB to clarify that such sharing of information is outside the scope of the rule. Alternatively, the CFPB could make

---

[21] 12 CFR 1005.3(a).

[22] 12 C.F.R. 1005.2(b)(2); Official Interpretation of Paragraph 2(b)(2)-1.

reference to the Gramm-Leach-Bliley Act ("GLBA") and its implementing Regulation P in its final rule and provide either that entities subject to and in compliance with their GLBA obligations are deemed compliant with the final rule or are exempt from prohibitions on sharing of covered data with their affiliates. Doing so will allow use of covered data to be dictated by consumer choice rather than the mechanism of transfer and prevent consumers from having to share data from one entity to another multiple times via multiple channels to obtain the products and services they desire.

In addition, SIFMA encourages the CFPB to clarify that certain financial research that is conducted in the ordinary course of business may be a permissible use of covered data. As currently contemplated, third parties would be required to limit their collection, use and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service. This limitation would impinge on standard research that financial institutions routinely conduct. For example, consumer information is often used to, among other things, evaluate economic growth by analyzing consumer consumption; assess the economic health of the loan market by understanding loan repayments, such as home or student loans; analyze inflation-related metrics through interest rate and consumption-related data; and examine the health of financial markets by understanding consumer transactions, such as deposits and withdrawals.

Therefore, SIFMA encourages the CFPB to clarify that such reasonable uses are permitted within the meaning of the rule as they benefit both consumers and the economy at large. Furthermore, the CFPB should ensure any requirements with respect to anonymized data are consistent with current federal, state and international data privacy regimes that allow for third-party use of anonymized datasets.[23] In addition, consumers should be able to opt-in through segregated means to allow certain data uses that may not provide any direct product or service to the consumer but benefit the economy, so long as the use of that data is not otherwise identifiable as to the data provider from which that data originates and does not contain a consumer's sensitive personal financial information. Further, if the consumer fails to reauthorize or otherwise revokes authorization, that data must similarly be deleted from the research data set or any other subsequent uses.

Nevertheless, SIFMA supports the CFPB's efforts to curtail the use of data beyond what is necessary to meet consumers' expectations to deliver the specific product or service. In order to effectuate this, the final rule should explicitly prohibit the use of permissioned data for targeted advertising and cross-selling, sale of data, marketing and reverse engineering by data aggregators and third parties, except where an entity providing services to the consumer uses data to offer its own products to the consumer. As the proposed rule acknowledges, none of these activities are reasonably necessary to deliver a specific product or service to a consumer. To avoid confusion, the word "other" in 1033.421(a)(2) should be deleted to make clear that no product or service offered in connection with Section 1033 can involve these activities.

[23] At present, the GLBA, the California Consumer Privacy Act, and the General Data Protection Regulation of the European Union, among others, allow for third-party use of anonymized datasets.

N. The CFPB Should Allow Data Providers to Confirm the Scope of Authorization.

SIFMA encourages the CFPB to allow data providers to confirm the scope of their authorization with consumers regarding accounts and duration of sharing prior to making data available to third parties. Financial institutions regulated by prudential regulators must operate in a safe and sound manner and align their policies and procedures to ensure that they handle consumer information appropriately. It is therefore imperative that the final rule include a provision, as the NPRM does, that a data provider is permitted to confirm the scope of the third party's authorization.[24] In addition to what is permitted under the NPRM, a data provider should be permitted to confirm the duration of such authorization, provided that in no event should it be greater than one year. This will help further effectuate the CFPB's 2017 Data Principles and reduce the risk that consumers' data is misused or made available for a period greater than the consumer authorizes or intends.

O. The CFPB Should Clarify and Expand the Obligations of Authorized Third Parties and Data Aggregators, Set an Appropriate Framework for Diligence of Them and Their Supervision and Impose Obligations on Data Aggregators to Oversee These Market Participants.

SIFMA encourages the CFPB to clarify and expand the obligations of authorized third parties and data aggregators and set an appropriate framework for both data aggregators and third-party data recipients to (1) comply with data authorization, security and usage requirements of the final rule and (2) perform due diligence and ensure oversight of the entities with which they share consumer information to ensure compliance. In addition, the CFPB should include a framework by which it will supervise data aggregators.

The proposed rule requires data providers to ensure that authorized third parties have complied with the third parties' data authorization requirements (after the authorized third parties have ensured that data aggregators have complied with their certification requirements). The proposed oversight mechanism set forth in the NPRM essentially places oversight obligations on data providers and third parties, many of whom are much smaller and less sophisticated than data aggregators.

Large data aggregators are arguably the parties in the ecosystem that are most in need of direct supervision by the CFPB in these areas because they hold and process the largest volumes of data and often also have the most resources and leverage in their relationships with data providers and third parties. However, the NPRM's mechanism places oversight obligations on smaller and less sophisticated third parties. Therefore, SIFMA asks the CFPB to directly obligate data aggregators to comply with all of the same obligations placed on third parties in its final Section 1033 rule and place them under supervision.

* * *

[24] 1033.331(b)(2).

SIFMA appreciates the opportunity to provide feedback on the CFPB's NPRM 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.com.

Sincerely,

Melissa MacGregor

Melissa MacGregor
Deputy General Counsel and Corporate Secretary

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