sifma
Invested in America

October 21, 2025

Sent via: Regulations.gov
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

RE: Docket No. CFPB-2025-0037; RIN 3170-AB39
Consumer Financial Protection Bureau, Advance Notice of Proposed Rulemaking on Reconsideration of Personal Financial Data Rights Rule

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to submit this comment letter on the above-referenced advance notice of proposed rulemaking ("ANPR") issued by the Consumer Financial Protection Bureau ("CFPB").[2]

The ANPR invites comment and information to assist the CFPB in its consideration of four issues related to Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "CFPA") and its implementing rulemaking (the "Rule"). 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,"[3] "including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data," and further provides that this information "shall be made available in an electronic form usable by consumers."

The ANPR specifically seeks comment on the proper understanding of who can serve as a "representative" making a request on behalf of a consumer; the optimal approach to the assessment of fees to defray the costs incurred by a "covered person" in responding to a customer-driven request; the threat and cost-benefit pictures for data security associated with Section 1033

---

[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 to thank Caitlin Mandel and Dan Chaudoin of Winston & Strawn for their work on this letter.

[2] 90 Fed. Reg. 40986 (Aug. 22, 2025).

[3] A "covered person" is defined in Section 1002(6) of the Dodd-Frank Ac, in part, as an entity engaged in offering or providing consumer financial products or services. 12 U.S.C. § 5481(6).

compliance; and the threat picture for data privacy associated with Section 1033 compliance. SIFMA addresses each of the CFPB's concerns herein.

As stated in its previous comment letters addressing the Rule,[4] SIFMA reiterates its support for 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.[5] Moreover, SIFMA expresses its continued support for the CFPB's initiatives aimed at fostering innovation and competitive practices that benefit consumers in financial markets. But the current Rule's broad definition of "representative" and prohibition on access fees exceed the CFPB's statutory authority and the intent of Congress when it enacted the CFPA. Further, questions remain surrounding the Rule's applicability to entities that are outside the CFPB's jurisdiction as provided in the CFPA or to data providers acting as trustees or with other fiduciary obligations to consumers. Concerns also remain regarding the Rule's potential prohibition of valuable secondary uses of de-identified consumer data.

Executive Summary

In response to the ANPR, SIFMA recommends that the CFPB:

- **Interpret "representative" narrowly**—as limited to individuals or entities with fiduciary duties to the consumer—to ensure accountability and prevent unauthorized third-party access to sensitive data.
- **Define "consumer" as a current customer** to avoid requiring the release of outdated or irrelevant data from former accounts.
- **Respect jurisdictional boundaries** by clarifying that the Rule does not apply to SEC-regulated entities or business lines outside the CFPB's authority.
- **Clarify fiduciary duties** by confirming that data providers acting as trustees or in similar capacities are not required to disclose information in conflict with those obligations.
- **Allow reasonable access caps** to protect data security, preserve system integrity, and balance operational demands.
- **Maintain regulatory harmony with the Gramm-Leach-Bliley Act (GLBA)** as the governing framework for financial data security and privacy.
- **Confirm that secondary uses of de-identified or anonymized data**—which support valuable market research and systemic stability—are not restricted by the Rule.

---

[4] SIFMA has previously provided comments on February 4, 2021, in response to the advance notice of proposed rulemaking published by the CFPB on November 6, 2020; on January 23, 2023, in response to 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; and on December 20, 2023, in response to the notice of proposed rulemaking published by the CFPB on October 19, 2023.

[5] *See* SIFMA Data Aggregation Principles (last accessed Sep. 15, 2025), available here.

- **Permit reasonable access fees** so that data providers may recover the substantial costs of building and maintaining secure interfaces, consistent with long-standing banking principles.
- **Adopt realistic compliance timelines**—specifically, the later of two years after qualified industry standards are issued or two years following final publication—to ensure orderly and secure implementation.

Taken together, these recommendations would realign the Rule with the statutory text and intent of Section 1033, promote responsible data access, safeguard consumer and market stability, and foster innovation without imposing unnecessary risks or costs.

I. Scope of the Rule

The ANPR seeks comment on the proper understanding of who can serve as a "representative" making a request on behalf of a consumer. The current version of Section 1033 allows certain third parties to request covered data as "representatives" with the consent of a consumer in an authorization disclosure.[6] As explained in the CFPB's own May 30, 2025 Motion for Summary Judgment,[7] this interpretation is inconsistent with the CFPA's text, structure, and purpose and exceeds the CFPB's statutory authority. Moreover, SIFMA requests that the CFPB revise the Rule to: (1) limit the definition of "consumer" to current accountholders; (2) clarify that Regulation E accounts held by Securities and Exchange Commission-registered entities are not in scope; and (3) clarify that data providers acting as trustees need not provide data in a manner inconsistent with their fiduciary duties.

A. "Representative" in 12 U.S.C. § 5481(4) Means Individuals or Entities with Fiduciary Duties to the Consumer.

SIFMA supports the interpretation expressed by the CFPB in its own Motion for Summary Judgment that the current rule's interpretation of "representative" exceeds the CFPB's statutory authority. The CFPA mandated that a data provider make available covered financial data upon request "*to a consumer*." 12 U.S.C. § 5533(a). The CFPA defines "consumer" to mean "an individual or an agent, trustee, or representative acting on behalf of an individual." *Id.* § 5481(4). The plain meaning of the CFPA demonstrates that the term "representative" cannot be expanded to mandate open banking to commercial third parties generally.

By its dictionary definition, "representative" means "someone who represents another as agent, deputy, substitute, or delegate usually being invested with the authority of the principal." Representative, Merriam-Webster Dictionary, https://www.merriamwebster.com/dictionary/representative. And in the legal context, "representative" is consistently understood to mean only someone who has a special relationship with or a similar obligation to those he or she represents. *See, e.g.*, *In re Imerys Talc Am., Inc.*, 38 F.4th 361, 376 (3d Cir. 2022) ("'Legal representative' is a term of art, referring to one who owes fiduciary duties to his absent, represented constituents."); *Alcabasa v. Korean Air Lines Co.*, 62 F.3d 404, 408 (D.C. Cir. 1995) ("[A] personal representative

[6] *See* 12 C.F.R. § 1033.401.
[7] ECF No. 58, *Forcht Bank v. Consumer Fin. Prot. Bureau*, No. 5:24-cv-00304-DCR (E.D. Ky. May 30, 2025).

has a fiduciary duty to bargain for the rights of all the decedent's beneficiaries and to turn over to them their appropriate share of any proceeds.").

The statutory context surrounding "representative" further justifies giving the term its limited ordinary meaning. The term "representative" "should read in a similar manner to its companions," the terms "agent" and "trustee." *Dubin v. United States*, 599 U.S. 110, 126 (2023). Both the terms "agent" and "trustee" involve a fiduciary relationship and a duty of loyalty to act for the principal's benefit. *See, e.g.*, Restatement (Third) of Agency § 1.01 (2006); Restatement (Third) of Trusts § 2 (2003). In light of this context, the term "representative" is best understood to mean an individual who has a fiduciary or special obligation to a consumer, not any third party with whom the consumer makes an arm's-length commercial deal. Moreover, such a definition would not improperly render the terms "agent" and "trustee" "misleading surplusage." *See, e.g.*, *Yates v. United States*, 574 U.S. 528, 546 (2015). The term "representative" appropriately encompasses relationships between the representative and individual that are less naturally understood as "agent" or "trustee" relationships, such as executor-decedent and parent-child relationships. *Alcabasa*, 62 F.3d at 408; *Warner v. Sch. Bd. of Hillsborough Cnty., Fla.*, 2024 WL 2053698, at *2 (11th Cir. May 8, 2024) ("[C]ertain representatives, including parents, [are permitted] to sue on behalf of minors.").

Finally, interpreting "representative" to exclude authorized commercial third parties is consistent with the CFPA's statutory scheme and legislative purpose. Under the interpretation of Section 1033 adopted in the Rule, fintechs and data aggregators could be considered "consumers" for purposes of the entire Consumer Financial Protection Act. Such an interpretation would make several provisions nonsensical. For example, 12 U.S.C. § 5511(b)(1)'s requirement that "consumers are provided with timely and understandable information" cannot be understood to mean that fintechs and data aggregators are entitled to such information. Nor can 12 U.S.C. § 5512(c)'s mandate that the CFPB "monitor for risks to consumers in the offering or provision of consumer financial products or services" by considering the "likely risks and costs to consumers associated with buying or using a type of consumer financial product or service" be reconciled with a definition of "consumer" that encompasses commercial third parties. In short, there is no evidence that Congress intended to create an extensive open banking regime when it enacted Section 1033 to "ensure[] that consumers are provided with access to their own financial information."[8] S. Rep. No. 111-176, at 173 (2010). Because Congress "does not hide elephants in mouseholes," the current Rule's expansive definition of "representative" exceeds the CFPB's statutory authority. *Whitman v. Am. Trucking Ass'ns, Inc.*, 531 U.S. 457, 468 (2001).

B. In the Alternative, the Definition of "Representative" Must Be Limited to Third Parties "Acting on Behalf of an Individual."

As noted above, SIFMA strongly supports the CFPB's position that the term "representative" in 12 U.S.C. § 5481(4) is correctly interpreted to mean an entity with fiduciary duties or special relationships to a consumer. However, should the CFPB conclude that a broader interpretation does not exceed its statutory authority, SIFMA notes that 12 U.S.C. § 5481(4) reads

[8] This is further supported by the fact that Section 1033 itself is only about 300 words, none of which speak to the concept of open banking.

in relevant part: "representative *acting on behalf of an individual*." Accordingly, 12 U.S.C. § 5533(a) does not allow the CFPB to regulate the transmission of consumer data between data providers and third parties where the third party is not acting on behalf of an individual. As a result, any iteration of the Rule cannot regulate bilateral negotiations between data providers and third parties for the sharing of consumer data for uses that do not involve the third party acting on behalf of an individual consumer.

C. The Definition of "Consumer" Should Be Limited to Current Customers.

SIFMA also renews its request for the CFPB to amend the definition of "consumer" to specify that a consumer is a natural person "that has at least one current account with the data provider." The financial and other information of former customers of a data provider may not be maintained in the same way that current client information is maintained. The ability of a former customer to access the consumer interface may differ from those methods used by customers with current accounts. Moreover, requiring data providers to furnish information that is outdated and stale to former customers would not appreciably advance the portability objectives underpinning the access right established in Section 1033. Therefore, SIFMA encourages the CFPB to amend the definition of the term "consumer" to clarify that it pertains only to current customers.

D. The CFPB Should Clarify That Regulation E Accounts Held by Securities and Exchange Commission–Registered Entities Are Not in Scope.

In previous rulemaking activities, the CFPB has been silent on Section 1033's applicability to SEC-registered entities that may hold Regulation E accounts.[9] The CFPA clearly states that the CFPB has no authority to "exercise *any power* to enforce" against any "person regulated by the [Securities and Exchange] Commission." 12 U.S.C. §§ 5481(21), 5517(i)(1). But the Rule currently applies to Regulation E accounts and data providers synonymous with Regulation E's definition of financial institutions without regard to the jurisdictional exclusion for SEC-registered persons. And Regulation E generally applies to all financial institutions without reference to the CFPA's jurisdictional exception for SEC-registered entities. *See* 12 C.F.R. § 1005.3(a). Thus, the current Rule sweeps too broadly and impermissibly attempts to expand the CFPB's rulemaking authority to enforce the CFPA against SEC-registered entities. Because "[a]gencies have only those powers given to them by Congress," the Rule currently exceeds the CFPB's statutory authority. *West Virginia v. EPA*, 597 U.S. 697, 723 (2022). Accordingly, the Rule should be revised to create an explicit exclusion for entities consistent with the CFPA's jurisdictional exclusions.

This necessary revision will also require that the CFPB clarify the Rule's applicability to institutions with multiple business lines, some of which are exempt from the CFPB's jurisdiction. For example, a financial institution may operate both a consumer bank and an SEC-registered investment platform. If a consumer has both a consumer deposit account and an investment account, the financial institution may have financial data in its possession, custody, or control relating to both types of accounts. To remain within its statutory authority, the CFPB should clarify

[9] A "Regulation E account" means an account as defined in Regulation E, 12 C.F.R. § 1005.2(b). 12 C.F.R. § 1033.111(b)(1).

that the Rule applies only to client data that is part of those specific business lines that are under CFPB, and not SEC, jurisdiction.

E. The CFPB Should Clarify That the Rule Does Not Conflict with Any Data Provider's Fiduciary Duties.

SIFMA also urges the CFPB to clarify that the Rule does not require certain data providers to provide data inconsistent with their fiduciary duties. Presently, the text of Section 1033 only briefly provides that a data provider can "withhold any information required to be kept confidential by any other provision of law." 12 C.F.R. § 1033.221(c). While the vast majority of financial relationships do not establish fiduciary duties, data providers occasionally operate as trustees, administrators, or conservators. These fiduciary accounts present complex issues regarding data aggregation and confidentiality. For example, information provided to a bank to execute the distribution of funds per the terms of a trust instrument by one beneficiary is restricted from disclosure to the other beneficiaries of the trust. And some financial information requested by one beneficiary may be available only in an aggregated format that contains information required to be kept confidential from the requesting beneficiary. Because the Rule cannot require any data provider to maintain or keep any information about a consumer, *see* 12 U.S.C. § 5533(c), data providers facing requests for such aggregated data cannot comply with both the request and their fiduciary duties. The CFPB should provide clear guidance that data providers facing such requests need not provide any information to a requesting beneficiary that would violate their fiduciary duty to such beneficiary or any other beneficiary.

II. Information Security

The ANPR further seeks comment on the threat and cost-benefit pictures for data security associated with Section 1033 compliance. As the ANPR identifies, the existence of data breaches and other threats to sensitive consumer data is a significant concern with the Rule's open banking regime, and SIFMA supports the CFPB's efforts to ensure that the Rule appropriately addresses information security. To that end, SIFMA supports narrowing the CFPB's interpretation of "representative" to eliminate the requirement that data providers provide sensitive client information to a limitless number of authorized third parties. *See supra* Section I.A. Such a revision would lessen the number of data transmission channels at risk of hacking or breaching.

Moreover, should the CFPB decide not to revise its interpretation of "representative," SIFMA urges the CFPB to allow data providers to impose reasonable access caps to ensure that data providers can appropriately balance meeting performance standards, ensuring consistent consumer service, and maintaining sufficient information security programs. SIFMA also supports the Rule's reliance on the Gramm-Leach-Bliley Act (the "GLBA") for establishing the requisite information security requirements and recommends that the CFPB coordinate with other federal regulators to ensure similar oversight and regulation of fintechs and data aggregators not currently regulated by the GLBA. Any additional security requirements would be overly burdensome, creating patchwork regulation with little security benefit to the consumer.

A. Data Providers Should Be Permitted to Impose Reasonable Data Access Caps.

SIFMA encourages the CFPB to allow data providers to impose reasonable access caps to aid data providers in meeting performance standards, ensuring consistent service for consumers, mitigating initial and ongoing compliance costs associated with compliance, and furthering the CFPB's goal of ensuring that the data being accessed is truly needed to provide the consumers' authorized product or service. While SIFMA appreciates the CFPB allowing for frequency restrictions under limited circumstances, SIFMA encourages the CFPB to permit data providers to prescribe broader limits on both the frequency and the quantity of requests for information needed for the provision of a 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 system outages, impede consumer access through the consumer interface, or slow the production of the requested information, rendering data providers out of compliance with the established performance standards while hindering other regulatory obligations that depend on system 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, or an account's terms and conditions.

B. The Rule's Reliance on the GLBA Is Sufficient to Address Information Security Risks.

The current Rule requires data providers and third parties to adhere to the applicable information security standards under the GLBA and provides that data providers may deny access to data if granting access is inconsistent with policies and procedures reasonably designed to comply with the GLBA's information security standards. 12 C.F.R. § 1033.311(e). SIFMA takes the position that the GLBA sufficiently provides for the secure transmittal and storage of consumer financial data. The GLBA has adequately provided the security framework for the storage and transmittal of consumer data since its passage. Institutions subject to the GLBA have long-standing policies and procedures in place to ensure the security of such data. Any security requirements imposed in addition to the GLBA would increase the compliance burden on data providers for minimal security benefit. Such requirements would also create a scheme of patchwork regulation, arbitrarily subjecting new subsets of data to greater security requirements. Moreover, the current Rule's harmony with the GLBA supports cohesion among regulatory agencies responsible for implementing the GLBA. Finally, SIFMA notes that the CFPB may lack authority to impose additional security regulations under Section 1033, as no provision in Section 1033 expressly authorizes the CFPB to implement such security restrictions. *See generally* 12 U.S.C. § 5533.

If the CFPB concludes that it does have authority to implement security restrictions under this Rule, the CFPB should ensure that any entity handling sensitive consumer financial data adheres to the same information security standards as financial institutions. In addition to the GLBA, financial institutions are subject to oversight under the FFIEC Information Security Handbook. While the GLBA and the FTC's Safeguards Rules establish baseline information security requirements for certain third parties within their purview, the FFIEC IT Examination Handbook provides more comprehensive and detailed standards to which financial institutions must adhere. For example, the FTC Safeguards Rules require covered institutions to conduct a risk assessment "in each relevant area of the company's operations," while the FFIEC Handbook

details extensively the process for developing, performing, reporting, and updating such an assessment.[10] Requiring third parties requesting data to adhere to these same requirements would better align regulatory expectations across entities and help ensure adequate information security. Accordingly, SIFMA recommends that the CFPB coordinate with other federal regulators to ensure similar oversight and regulation of fintechs and data aggregators not currently regulated by the GLBA.

III. Consent and Data Privacy

The ANPR further seeks comment on the threat picture for data privacy associated with Section 1033 compliance. SIFMA supports the CFPB's efforts to amend the Rule to protect the privacy interests of consumers. However, any such revisions to the Rule should recognize that certain data sharing arrangements, such as beneficial research uses or disclosures of data between a covered person's affiliates, should be permitted because of their broader market benefits, and thus should be outside the Rule's scope. We urge the CFPB to adopt a distinction between identifiable data—which implicates consumer privacy—and de-identified or anonymized data, which poses minimal to no risk of re-identification when used for industry-standard market research. The benefits to the economy and markets in terms of more accurate understanding of consumer spending, housing prices, and other economic activity will accrue to all consumers. This distinction is consistent with the GLBA, CCPA, and GDPR, all of which recognize anonymized datasets as outside the scope of restrictive privacy obligations.

A. The CFPB Should Clarify That Certain Uses of Covered Data Are Neither Restricted nor Required by the Rule.

SIFMA encourages the CFPB to clarify that the Rule does not regulate the sharing of consumer data among a data provider's affiliate institutions. The sharing of consumer information among a data provider's affiliate institutions is vital both to the consumer experience across a corporate structure's suite of products and services and to institutional risk controls and fraud prevention. The sharing of consumer information among affiliate institutions is permitted by the GLBA and the Fair Credit Reporting Act and its implementing Regulation V, subject to its disclosure and opt-out requirements.[11] Imposing the Rule's limitations on a data provider's affiliates' access to covered data would disturb these critical functions and introduce regulatory disharmony without benefit.

Further, SIFMA encourages the CFPB to clarify that, while certain secondary uses of information, including de-identified information, shared across institutions may have important benefits, no data provider is required by the Rule to provide data for those uses. Currently, the Rule limits third parties' collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service. *See* 12 C.F.R. § 1033.421(a),

---

[10] *Compare* 16 C.F.R. § 314.3(b) *with* Fed. Fin. Inst. Examination Council, IT Examination Handbook: Information and Security (2016).

[11] *See* 15 U.S.C. § 6802(a) (restricting a financial institution's ability to disclose consumer information "to a nonaffiliated third party"); *id.* § 1681a(d)(2) (excluding from the definition of a "consumer report" any communication of information related "solely as to transactions or experiences" of the consumer and shared "among persons related by common ownership").

(c). If this approach prohibits third parties' access to de-identified data wholesale, this approach ignores the importance of de-identified consumer data to the broader U.S. financial system. For example, financial institutions and research organizations may analyze anonymized transaction data to generate insights that support broader market stability and consumer welfare. Such information has valuable research use cases, including: identifying trends in household savings behavior to understand financial resilience; evaluating small business activity by examining anonymized payment flows; measuring community-level investment and economic development by studying anonymized deposit and withdrawal activity across regions; monitoring regional housing affordability through anonymized mortgage and rental payment patterns; and evaluating the resilience of supply chains by monitoring aggregated retail spending patterns. We emphasize that these beneficial uses rely on anonymized datasets that cannot be traced to any individual consumer and therefore should not be subject to the same restrictions as identifiable data. Far from undermining privacy, these uses safeguard it by removing personal identifiers while still contributing to market stability and economic insight.

The data privacy concerns outlined in the ANPR are inapplicable to these uses of anonymized consumer data. Several statutory regimes recognize the value of such data. Indeed, the GLBA,[12] the California Consumer Privacy Act,[13] and the General Data Protection Regulation of the European Union[14] all exempt anonymized datasets from restrictions on data retention and use.

The CFPB also lacks statutory authority to *require* data providers to provide information to third parties for general market research, as such use cases are not "on behalf of a consumer." *See supra* Section I.B. SIFMA encourages the CFPB to clarify that such beneficial uses may be permitted by private agreements *only*, between data providers and third parties, while emphasizing that data providers are never required to share data for or otherwise facilitate these use cases. Moreover, private agreements can assign liability to the entity where a data breach or data misuse originates. As a matter of policy and statutory authority, such use cases must remain subject to the private negotiations of data providers and third parties.[15]

IV. Compliance Estimates and Allocation of Costs

The ANPR further seeks comment on data providers' estimated compliance costs and whether the CFPB should allow data providers to recover reasonable costs for creating, maintaining, and providing access to covered data through developer interfaces. SIFMA

[12] *See* 15 U.S.C. § 6809(4)(A) (limiting the GLBA's application to types of "personally identifiable financial information").
[13] *See* Cal. Civ. Code § 1789.140(m) (defining "deidentified" consumer data).
[14] Regulation (EU) 2016/679.
[15] Should the CFPB conclude that it does have statutory authority to mandate third-party access to covered data for purposes that are not "on behalf of a consumer," SIFMA recommends that issues of data security and data liability must be addressed through separate opt-in channels that would allow for the sharing of certain data that may not provide any direct product or service to the consumer but which benefit the economy, so long as the use of that data is not otherwise identifiable as to the data provider from which the data originates, and does not contain a consumer's sensitive personal financial information. Such a framework would recognize the value of such uses for de-identified consumer data, while also ensuring that consumers are informed about the uses of their de-identified data.

encourages the CFPB to remove the Rule's prohibition on access fees. As a statutory matter, the CFPB lacks statutory authority to prohibit access fees. As a matter of policy, allowing data providers to recover their considerable compliance costs would acknowledge the substantial expenses associated with compliance, prevent fee disparities between national banks, other banks, and nonbank data providers, and ensure that the Rule does not result in decreased consumer access to covered products and services.

A. Data Providers Should Be Permitted to Charge Fees for Access to Data.

As a textual matter, no provision of Section 1033 authorizes the CFPB to prohibit data providers from charging fees for consumer data. Because "the ability to charge fees" is a "fundamental national bank function," *Monroe Retail, Inc. v. RBS Citizens, N.A.*, 589 F.3d 274, 280, 283 (6th Cir. 2009), the CFPB should require "exceedingly clear language" to support this significant assertion of regulatory power, *Alabama Ass'n of Realtors v. Department of Health & Human Services*, 594 U.S. 758, 764 (2021). Prohibitions on fees are commonly made explicit in the text of statutes themselves. *See, e.g.*, 15 U.S.C. § 1681c-1(a)(2)(B) (requiring consumer reporting agencies to provide disclosures "without charge to the consumer"); *id.* § 1691(e)(4) (requiring creditors to provide certain copies of appraisals "at no additional cost to the applicant"); *id.* § 1639h(c) (requiring creditors to provide appraisal copies "without charge" to applicants for high-risk mortgages). Tellingly, no such language exists in Section 1033. The Rule's fee prohibition is also inconsistent with regulations requiring banks to charge fees "according to sound banking judgment" and taking into consideration "[t]he cost incurred by the bank in providing the service." 12 C.F.R. § 7.4002(b)(2). The Rule's prohibition on fees is thus incompatible with the CFPB's statutory authority and long-standing regulatory principles. Moreover, the Rule's broad scope makes it impossible to confidently estimate compliance costs.[16]

The current fee prohibition requires data providers to incur the indeterminate costs of providing efficient and technical services for the sole benefit of other commercial actors, while also bearing the liability risk for downstream misuses of data over which data providers have no control. Thus, to ensure that costs are allocated efficiently and fairly, the Rule should allow data providers to charge fees associated with building, maintaining, and making data available through secure interfaces. SIFMA also encourages the CFPB to consider establishing an appropriate liability framework to ensure that data providers do not bear the costs of third-party misuse of consumer data accessed through a data provider's secure, compliant API.

V. Compliance Timelines

SIFMA recommends that compliance with any revisions to the Rule should not be required until the later of (1) two years after qualified industry standards are issued or (2) two years after the final Rule's publication.

[16] The Rule presently requires data providers to make an Application Programming Interface ("API") accessible to an indeterminate number of third parties for an indeterminate number of data requests.

VI. Conclusion

SIFMA supports the CFPB's efforts to implement Section 1033 in a manner that enhances consumer access to financial data, promotes competition, and protects data security and privacy. We urge the CFPB to adopt a measured approach that recognizes the limits of the agency's statutory authority and the operational costs and complexities of coming into compliance with the Rule.

We appreciate the opportunity to provide these comments and welcome further engagement with the CFPB as it considers revisions to the Rule. We 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
Managing Director and Associate General Counsel