December 29, 2023

Via electronic submission

Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

Re: **Docket No. CFPB-2023-0052 – Comments on Notice of Proposed Rulemaking on Personal Financial Data Rights**

To whom it may concern:

The Bank Policy Institute ("BPI")[1] and The Clearing House Association, L.L.C. ("TCH" and, collectively with BPI, "Associations")[2] appreciate the opportunity to comment on the Proposed Required Rulemaking on Personal Financial Data Rights ("proposal")[3] issued by the Consumer Financial Protection Bureau pursuant to section 1033 of the Dodd-Frank Act.[4] The Associations support innovation and welcome competition in financial products and services, so long as the innovation is conducted responsibly, consumers are protected, liability is fairly apportioned, and all entities operating in the ecosystem are subject to consistent regulation and examination.

The growth in adoption of digital products and services in recent years has accelerated banks' efforts to leverage market-developed technological solutions to help meet customer demand while ensuring consumers' sensitive financial data is kept private and secure. Unlike other jurisdictions in which consumer financial data sharing has been mandated by government action, this expansion of consumer financial data access in the United States largely has developed through innovation in the marketplace. Under this type of industry-driven approach, participants can innovate and adapt quickly to meet consumer demand and develop safer products and services.

We have asserted in the past that the CFPB's efforts to implement section 1033 of the Dodd-Frank Act should not reverse the significant progress that the industry has made or slow the pace of

---

[1] The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's bank-originated small business loans, and are an engine for financial innovation and economic growth.

[2] The Clearing House Association, L.L.C., the country's oldest banking trade association, is a nonpartisan organization that provides informed advocacy and thought leadership on critical payments-related issues. Its sister company, The Clearing House Payments Company L.L.C. owns and operates core payments system infrastructure in the United States, clearing and settling more than $2 trillion each day. See The Clearing House's website at www.theclearinghouse.org.

[3] *Required Rulemaking on Personal Financial Data Rights*, Consumer Financial Protection Bureau, 88 Fed. Reg. 74796 (October 31, 2023).

[4] 12 U.S.C. § 5533.

continued evolution in this space, which has generally benefited consumers. In this regard, we appreciate the CFPB's recognition in the proposal that industry standard-setting bodies "have a critical role to play in ensuring a safe, secure, reliable, and competitive data access framework."[5] The CFPB rightly acknowledges that "[c]omprehensive and detailed technical standards mandated by Federal regulation could not address the full range of technical issues in the open banking system in a manner that keeps pace with changes in the market and technology. A rule with very granular coding and data requirements risks becoming obsolete almost immediately, which means the CFPB and regulated entities would experience constant regulatory amendment, or worse, the rule would lock in 2023 technology, and associated business practices, potentially for decades."[6] It will be important that the final rule adopt this approach as we have witnessed the challenges that arise in other jurisdictions when technology standards are hard wired into law, such as in the U.K.[7]

In the United States, as consumer demand for digital and interactive financial products and services has increased, an increasing number of financial technology firms and other companies have entered the market for consumer financial products and services. These entities are not generally subject to the same comprehensive regulation and supervision as banks. Increasingly, however, these entities rely on access to sensitive consumer data held at a financial institution to provide their products and services.[8] Our members welcome the competition brought about by innovative financial technology firms and are prepared to support the ability of bank customers to connect their bank accounts to the third-party apps of their choice including where a data aggregator is used to retrieve the customer's information from the customer's financial institution and share it with the app.[9] But such competition cannot come at the expense of data security. It is critical that consumers' personal and financial information remains secure when it is shared between financial institutions and third parties and when it is stored outside of the financial institution. In addition, regulation of the data economy must not create unfair competition by, for example, limiting the imposition of fees by some but not all in the ecosystem.

The Associations support the CFPB's recognition of the critical importance of ensuring that the data access framework is safe, secure, reliable, and competitive, consistent with the CFPB's goal as articulated in the preamble.[10] To help advance those objectives, we make various policy recommendations below, including:

---

[5] 88 Fed. Reg. at 74801.

[6] *Id*.

[7] *See*, *e.g.*, https://standards.openbanking.org.uk/specifications/.

[8] *See* U.S. Department of the Treasury Report to the White House Competition Council "Assessing the Impact of New Entrant Non-bank Firms on Competition in Consumer Finance Markets" (Nov. 2022), *available at* Assessing the Impact of New Entrant Non-bank Firms on Competition in Consumer Finance Markets (treasury.gov).

[9] The CFPB should make it clear that regardless of how third parties use covered data, including in consumer reports, the CFPB does not intend to make data providers furnishers under the Fair Credit Reporting Act (FCRA). The CFPB has stated that it is considering a rulemaking to address a number of consumer reporting topics under the FCRA. Towards this end, on September 15, 2023, the CFPB issued a Small Business Advisory Review Panel for Consumer Reporting Rulemaking – Outline of Proposals and Alternatives under Consideration*, available at* https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-rule-sbrefa_outline-of-proposals.pdf.

[10] 88 Fed. Reg. at 74801.

1. **Consumer Protections**: Many of the requirements in the proposed rule designed to protect consumers and their data, such as the requirements related to consumer authorization and the permissible uses of consumer data, should apply to all third parties and data aggregators in the ecosystem, and to all data.
2. **Credential-Based Access and Screen Scraping**: Credential-based access and screen scraping should be explicitly prohibited with respect to any data made available via a developer interface (not just covered data).[11] This prohibition should apply to all third parties (not just authorized third parties) and data aggregators.
3. **Clear Regulatory Requirements**: The proposed rules largely rely on a web of definitions to articulate its requirements, and private actors as the enforcers of those rules. In the final rule, the CFPB should impose direct requirements on all third parties (as referenced in recommendation 1) and data aggregators and articulate its intent to supervise those entities for compliance.
4. **Data Provider Authorization:** The proposal would require third parties to obtain consumer authorization before accessing their data. It is important that data providers have the right to obtain their own consumer authorizations before sharing consumer data with an authorized third party or data aggregator.
5. **Liability**: The CFPB should ensure that liability is fairly apportioned within the financial data sharing ecosystem. Data providers also should have the right to deny third party and aggregator data access requests based on risk management concerns, including those related to liability.
6. **Data Provider Compensation**: Data providers should be allowed to receive compensation from third parties to recover their commercially reasonable costs and a margin to cover the cost of enabling data sharing. By prohibiting only data providers from charging fees, the proposed rule arbitrarily distorts the marketplace and creates an unfair allocation of benefits to data aggregators and an un-recoupable cost to data providers.
7. **Categories of Covered Data:** Payment initiation by third parties and data aggregators creates unmanageable fraud risks, and payment initiation information should not be a category of covered data. The covered data category of "terms and conditions" should be revised as "account pricing information" with references to existing regulatory disclosures.
8. **Standard Setting Bodies and Data Formats**: The final rule should continue to recognize that a standard setting body is best positioned to develop a standardized format for data sharing and the final rule should extend the CFPB's expectations with respect to use of standard data formats to data aggregators to ensure efficiencies and support competition.
9. **Compliance Dates**: The proposed compliance dates are overly aggressive even for the most sophisticated banks and vague at best with respect to third parties.

We provide an overview of these suggested revisions below, and we make detailed recommendations for amendments to the proposed rule in the Appendix. While we believe we have been comprehensive in our response, the proposal is complex and novel and the CFPB provided less

[11] "Screen scraping" broadly refers to a method of data collection, which uses a computer program to copy data from a website. Credential-based access provides a third party access to a consumer's account information on the website of a financial institution by using the consumer's own authentication credential. Screen scraping can be credential-based or non-credential based. Credential-based screen scraping is prevalent in the market today, as the CFPB recognizes in the preamble. 88 Fed. Reg. at 74797, note 7. Both consumer credential-based access and non-credential-based screen scraping present risks to data providers and consumers.

than the typical 90-day comment period we requested on two occasions.[12] We also note that the proposal leaves many issues unaddressed and likely will require significant amendments to provide further clarity to all relevant stakeholders. While we agree with the urgency of this rulemaking to implement section 1033, given the extensive comments by us below and those expected from other stakeholders, we do not believe the rule is currently ripe for finalization on the basis of this proposal. The CFPB should consider reproposing the rule after reviewing and addressing comments received to ensure that stakeholders have a meaningful opportunity to comment on proposed revisions to the rule. The lengthy amount of time the CFPB has taken to promulgate the proposal illustrates the proposed rule's complexity.

Discussion of the Proposed Rule

1. The consumer protections in the proposed rule should be expanded.

In addition to our general recommendation in section 3 below that the CFPB impose the rule's requirements directly on authorized data providers and data aggregators, rather than relying on those entities to enforce those obligations with one another via private contract, the consumer protections set forth in the proposal should be strengthened by expanding the scope of entities and data to which they apply. As we assert below in section 2, the CFPB should explicitly prohibit screen scraping and credential-based access by all third parties and data aggregators, not just authorized third parties and data aggregators used by those entities, with respect to data that a data provider has made available via a developer interface. This prohibition should extend to all data made available via the interface and not be limited to "covered data."

We also recommend that *all* third parties and data aggregators should be required to abide by all relevant requirements that would apply to authorized third parties (and data aggregators used by authorized third parties) including those set forth in § 1033.421, such as limitations on the collection, use, and retention of data, and requirements to: establish policies and procedures to ensure data accuracy, meet minimum data security standards, obtain reauthorization every 12 months, and provide consumers with a means to revoke authorization. Thus, when a third party or an aggregator acting on the third party's behalf seeks to access data via screen scraping, for example, the relevant consumers should still be provided with an authorization disclosure and have to authorize the entity to access their data via screen scraping.

In addition, the requirements related to data, including limitations on the collection, use, and retention of data, only apply to covered data under the proposed regulation. Thus, if a data provider makes additional data available via a secure interface, or additional data is scraped from the data provider's website, data aggregators and third parties that obtain that data could use it for purposes other than that for which the consumer authorized sharing, which is contrary to the important principles the CFPB has recognized that consumers should have transparency into, and control over, how, why,

[12] *See* "Request for Extension of Comment Period for Notice of Proposed Rulemaking on Personal Financial Data Rights," Correspondence between fifteen trade associations and Director Rohit Chopra, dated October 27, 2023, and "Request for Extension of Comment Period for Notice of Proposed Rulemaking on Personal Financial Data Rights," Correspondence between thirteen trade associations and Director Rohit Chopra, dated December 19, 2023.

and for how long their data is collected, used, and stored.[13] Moreover, this bifurcated framework could cause substantial consumer confusion regarding what data is being accessed, with whom it is being shared, how they can revoke access, and what protections apply to any particular category of data.

Thus, all the requirements designed to protect consumers and their data, such as the requirements related to the collection and use of consumer data, should apply to all third parties and aggregators in the ecosystem, and to all data, not just the limited scope of "covered data" currently contemplated. Again, as we describe in section 3, these requirements should be directly imposed and enforced by the CFPB rather than administered through contracts among the private entities in the ecosystem.

A fragmented approach to consumer and data protection will not provide the appropriate incentives for all third parties and aggregators in the ecosystem to implement sufficient consumer and data protections, undermining the purpose of the proposal to protect consumers and their data. Additional recommendations on these topics are provided in section (3)(c) of the Appendix.

2. <u>Screen scraping and credential-based access should be explicitly prohibited once a data provider has made a developer interface available.</u>

The preamble to the proposed rule appropriately recognizes the dangers of screen scraping and credential-based access by third parties, including "risks to consumers' data privacy and security" and increased "risks of data inaccuracy in the third party's product or service."[14] The proposal also recognizes that screen scraping presents risks to data providers by placing "undue strain on their information systems" and "exacerbates data provider concerns with respect to liability."[15] For these reasons, the CFPB seeks to move the market away from screen scraping because "it is not a viable long-term method of access."[16]

While we appreciate the CFPB's recognition of the dangers of screen scraping and credential-based access generally and agree with the need to transition away from those practices, the proposal does not go far enough. The proposed rule includes a requirement for data providers to make available developer interfaces that do not rely on consumer credentials. It further provides that data providers "must not allow a third party to access the data provider's developer interface by using any credentials that a consumer uses to access the consumer interface."[17] However, the proposal does not require third parties to use the developer interface or prohibit third parties from using consumer credentials (or attempting to use consumer credentials) to access the consumer interface, which is generally the way in which screen scraping occurs. Moreover, while data providers always can block screen scraping

---

[13] Consumer Financial Protection Bureau, "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation" (Oct. 18, 2017) (available at: https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf; Principles 3 and 6.

[14] 88 Fed. Reg. at 74799. The CFPB notes in the preamble that discussion in the proposal about "screen scraping" generally refers to "credential-based" screen scraping. 88 Fed. Reg. at 74797, note 7.

[15] *Id*.

[16] 88 Fed. Reg. at 74800.

[17] Proposed § 1033.311(d).

consistent with prudential risk management practices, blocking is very difficult and costly, even for the largest financial institutions. Even when screen scraping is successfully blocked, consumers will still be exposed to risk because they have already shared their credentials with a third party.

Therefore, the CFPB should explicitly prohibit screen scraping and consumer credential-based access by all third parties, not just authorized third parties, and all data aggregators used by any third party, once a data provider has made a developer interface available with respect to *all data* made available via the interface, not only with respect to "covered data." We submit that the consumer protection benefits of this approach far outweigh any disadvantage to third parties that rely on screen scraping. Appendix section (2)(b) discusses this point further.

3. <u>The CFPB should impose direct requirements on authorized third parties and data aggregators and supervise those entities for compliance</u>.

The proposal does not establish a sufficiently comprehensive or robust framework to ensure that authorized third parties and data aggregators adequately protect consumers and their data.

Authorized third party

Under the proposal, "authorized third parties" would be eligible to access data providers' developer interfaces to obtain consumer data. The third party's status as an "authorized" third party is based on the third party's meeting certain obligations, including providing the consumer with an authorization disclosure, certifying to meet certain obligations, and obtaining the consumer's express informed consent to access their data. However, those obligations operate simply as contractual obligations between consumers and third parties rather than requirements the CFPB intends to enforce to protect consumers. As we discuss further herein, the CFPB should require third parties and aggregators, regardless of how they seek to obtain consumers' data, to abide by the authorization requirements of the rule to protect consumers.

Data providers also would bear responsibility for ensuring that third parties: become authorized third parties, abide by the relevant obligations to obtain such status, and access covered data via developer interfaces and do not use consumer credentials to access consumer interfaces.[18] This puts a substantial oversight burden on data providers, individually and collectively, to monitor compliance by thousands of prospective data recipients.[19] While data providers, particularly those that are regulated financial institutions, conduct appropriate due diligence on third parties and aggregators consistent with their third-party risk management obligations, it is not appropriate or feasible for data providers to bear responsibility for ensuring third party compliance with all relevant obligations. In may also be

[18] Proposed §§ 1033.331(b)(1)(iii) and 1033.311(d).

[19] We further submit that the proposal's delegation of enforcement authority to data providers to enforce the obligations of authorized third parties, and to authorized third parties to enforce the obligations of data aggregators, could be an improper abdication of the CFPB's statutory obligations to protect consumers and could violate the Appointments Clause of Article II of the Constitution and the Constitution-based "private nondelegation doctrine." *See, e.g., Buckley v. Valeo*, 424 U.S. 1, 126 (1976), (holding that agency enforcement authority is executive in nature and constitutes a "significant authority" which only can be executed by an "Officer of the United States"); *National Horsements Benevolent Ass'n v. Black*, 53 F.4th 869, 881-885 (5th Cir. 2022) (holding that Congress violated the private nondelegation doctrine by empowering a private party to exercise federal regulatory power).

impossible for a data provider to determine whether all of the conditions set forth in § 1033.401 were met for a specific consumer, especially within 3,500 milliseconds. More importantly, it would be significantly more effective in ensuring consumers are protected if the CFPB required third parties and aggregators to meet these obligations.

Data Aggregators

The proposal defines a data aggregator as "an entity that is retained by and provides services to the authorized third party to enable access to covered data."[20] It is likely that the vast majority of authorized third parties will use data aggregators in this manner. There are thousands of third parties and data providers in the ecosystem for whom data aggregators likely will facilitate connectivity, resulting in their having access to a substantial volume of sensitive consumer financial data.

Moreover, this definition significantly understates the role that aggregators play, and likely will continue to play, in the consumer-permissioned data sharing ecosystem. Many data aggregators not only enable access to data, but they also collect the data and manipulate the format or other aspects of data to suit the needs of their third-party customers. Data aggregators typically retain the data that is collected, and, in some cases, use it for their own purposes without consumers' express informed consent.

In light of many data aggregators' access to, use, and storage of a substantial volume of sensitive data, the proposal does not impose sufficiently robust requirements on data aggregators that would be enforced by the CFPB. We make recommendations throughout this letter to strengthen the obligations of data aggregators but summarize those points here. For example, while the proposal provides that data aggregators would be bound to comply with certain of the requirements applicable to authorized third parties when acting on behalf of an authorized third party, the proposal contemplates that those authorized third parties would be responsible for the data aggregator's compliance with those obligations, rather than the CFPB.[21] Because data aggregators hold and process an enormous volume of data, the CFPB should hold data aggregators accountable for implementing and maintaining robust data security, privacy, and consumer protections, including limitations on the collection and use of consumer data, including by direct oversight from the CFPB to ensure these obligations are upheld. Moreover, to ensure clarity, these obligations should be set out under the rules as *data aggregator responsibilities and obligations rather than cross-referencing provisions governing third parties*.

To avoid consumer confusion and ensure they have transparency into and control over what data is shared, with whom, and for what purpose, the rule also should prohibit data aggregators acting on behalf of authorized third parties from obtaining an authorization from the consumer to use the

[20] Proposed § 1033.131.

[21] For example, proposed § 1033.431 provides that "a data aggregator is permitted to perform the authorization procedures described in § 1033.401 on behalf of the third party" but "the third party seeking authorization remains responsible for compliance with the authorization procedures described in § 1033.401," and "the data aggregator must certify to the consumer that it agrees to the conditions on accessing the consumer's data in § 1033.421(a) through (f) and the condition in § 1033.421(h)(3) upon receipt of the notice described in § 1033.421(h)(2) before accessing the consumer's data." *See* proposed §§ 1033.431(a) and (c). As noted in footnote 19, this delegation of enforcement authority to authorized third parties to enforce the obligations of data aggregators could be an improper abdication of the CFPB's statutory obligations to protect consumers and could violate the Appointments Clause of Article II of the Constitution and the Constitution-based "private nondelegation doctrine."

consumer's data for its own purposes (i.e., beyond what is needed to enable data sharing with the third party) as part of its interaction with a consumer on behalf of the third party. Data providers should be prohibited from using customer contact information obtained by providing data to an authorized third party for its own use, in any capacity. Data aggregators engage in these practices today and they are not reasonably necessary for the authorized third party to provide the requested product or service. Leveraging the consumer's third-party authorization process in this way takes unreasonable advantage of, and is confusing to, the consumer.

Finally, data providers must be able to impose requirements and obligations on data aggregators and hold them accountable for those obligations before granting them access to their developer interfaces for risk management purposes in the same way data providers may do so with respect to authorized third parties under the proposal. As the primary entity that interfaces directly with the data provider, addressing risk management concerns with data aggregator practices is just as important, if not more important, than doing so with respect to authorized third parties.

CFPB Supervision

To further ensure that third parties and data aggregators used by those third parties abide by the obligations set forth in the proposal, as well as those we recommend the CFPB adopt with respect to all third parties and aggregators, and to help ensure that consumers and their data and the overall consumer data sharing ecosystem are safe and secure, the CFPB should directly supervise third parties and data aggregators.[22] This supervision should include regular examinations, and the CFPB should publish an examination manual to help the market implement appropriate compliance controls and processes in advance of any expected compliance date.[23]

One way in which the CFPB could supervise these entities would be to propose a larger market participant rule to cover those entities; the CFPB also could determine, by order, that such entities are engaging, or have engaged, in conduct that poses risks to consumers, which would then give the Bureau the authority to supervise and examine those entities for compliance with applicable data security standards, federal consumer protection laws, the requirements established in any final rule

[22] The CFPB recently proposed a rule to supervise larger market participants in the market for general-use digital consumer payment apps, many of which would be covered by the proposed rule promulgating section 1033 as third parties and/or data providers. If finalized, approximately 17 entities would become subject to CFPB supervision. The proposal states that those entities would be supervised with respect to "unfair, deceptive, and abusive acts and practices, rights of consumers transferring money, and privacy rights." This rule, however, would only cover a very small subset of the thousands of third parties in the consumer permissioned financial data ecosystem and would not appear to cover the proposed obligations of third parties under the proposed rule implementing section 1033. *See* Consumer Financial Protection Bureau, "Defining Larger Participants of a Market for General-Use Consumer Payment Applications," 88 Fed. Reg. 80197, (Nov. 17, 2023).

[23] The proposal also adds section 1001.2(b) to its regulations that states that a "financial product or service" includes "providing data processing product or services." The CFPB asserts that it added this provision to "ensure that activities involving consumers' potentially sensitive personal financial information are subject to the CFPA and its prohibition on unfair, deceptive, or abusive acts or practices." However, that proposed addition would not ensure that data aggregators and authorized third parties will be held responsible for the obligations proposed in this 1033 rulemaking. Therefore, the CFPB should ensure that it subjects third parties and data aggregators to supervision for compliance with all their obligations under any final rule implementing section 1033.

implementing section 1033, and all other relevant laws and regulations.[24] Only by supervising and examining these entities for compliance with truly equivalent data privacy and security requirements and expectations to which banks are subject, and the requirements established by a rule implementing section 1033, can consumers and their data be sufficiently protected. Pro-active supervision is an important tool in the data security world, as once a system is breached, it is almost impossible to recapture and secure compromised data. Any final rule should also clarify when data aggregators and other third parties receiving covered data may be supervised under the CFPB's FCRA rulemaking.[25]

4. <u>Data providers must have the ability to obtain authorization from the consumer</u>.

The proposal would require third parties to obtain a consumer authorization before accessing their data.[26] Under the proposal, data providers would have the right to "confirm the scope of a third party's authorization," before it is required to make covered data available upon request from an authorized third party.[27] This "confirmation" construction does not fully represent the consumer's authorization to the data provider and does not sufficiently protect data providers from subsequent allegations of impermissible consumer data sharing. It is important that data providers have the right to obtain their own consumer authorizations before sharing consumer data with an authorized third party or data aggregator.

This additional safeguard would help ensure that consumers give informed consent to sharing their data with third parties for a specific purpose and would give data providers more certainty that the consumer has indeed authorized the sharing of their data and understands the key terms of sharing. Moreover, it will help ensure that consumers are not unduly coerced or otherwise subject to unfair, deceptive, or abusive authorization procedures at the third party and that data providers are not later subject to claims for sharing data based on an authorization process that the consumer later alleges was improper for some reason. This topic is addressed further in section (2)(e) of the Appendix.

5. <u>The CFPB should ensure that liability is fairly apportioned within the financial data sharing ecosystem</u>.

The topic of liability within the data sharing ecosystem is of critical importance and has been subject to significant discussion among the relevant stakeholders. Indeed, the Associations have previously encouraged the CFPB to address liability in its rulemaking under section 1033 by making clear

---

[24] 12 U.S.C. § 5514(a)(1)(B) provides that the CFPB has supervisory authority over "larger participant[s] of a market for other consumer financial products or services," as the CFPB defines by rule. 12 U.S.C. § 5514(a)(1)(B) provides that the Bureau can supervise a nonbank covered person that the Bureau "has reasonable cause to determine, by order, after notice to the covered person and a reasonable opportunity for such covered person to respond . . . is engaging, or has engaged, in conduct that poses risks to consumers with regard to the offering or provision of consumer financial products or services." The CFPB also should consult and coordinate with other agencies, such as the Federal Trade Commission, regarding enforcement of relevant laws applicable to third parties and/or aggregators.

[25] *Small Business Advisory Review Panel for Consumer Reporting Rulemaking – Outline of Proposals and Alternatives under Consideration*, Consumer Financial Protection Bureau, *available at* https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-rule-sbrefa_outline-of-proposals.pdf.

[26] Proposed § 1033.401.

[27] Proposed § 1033.331(b)(1)(iii).

that liability of data providers for any incident leading to loss or harm should end when the data leaves the data provider's control. Ideally, to ensure that the consumer permissioned data sharing ecosystem operates as safely as possible, each entity should be liable for, and be required to indemnify other entities in the ecosystem for, losses resulting from unauthorized transactions or other harm arising from a data breach or other compromise of their systems. These requirements will provide for fair apportionment of liability and provide incentives to implement and maintain robust data security programs.

Rather than directly addressing liability in the proposed rule, the preamble to the proposal states that the current system provides sufficient liability protections, primarily through consumer protections in Regulation E and Regulation Z, by application of the GLBA safeguards rule or the FTC safeguards rule, and through bilateral contracts between the data sharing parties. We appreciate that the CFPB recognizes that liability continues to be an important issue in the ecosystem. However, the safeguards articulated by the CFPB do not sufficiently protect consumers and do not sufficiently protect data providers from liability risk.

With respect to Regulation E, the CFPB should clarify that when a consumer initiates an electronic fund transfer using a third-party service, that third party, and any data aggregator used by that third party to enable it to process the payment, is responsible for unauthorized transactions in these circumstances even if the consumer's bank account is used. The CFPB could accomplish this by indicating that a data provider agreement between a financial institution and an authorized third party or data aggregator, is not the type of agreement contemplated in § 205.14(a)(2) of Regulation E. This would help to ensure that the third party or data aggregator would be treated as a service provider under Regulation E and held liable for unauthorized transactions in these circumstances, rather than the financial institution that holds the consumer account. As the entity that receives the consumer's instructions and authenticates the consumer's identity, the third-party service provider is in the best position to control the risk of unauthorized transactions conducted through its system. Therefore, allocation of risk to the third-party service provider makes good policy sense.

We support the CFPB's recognition that all parties in the ecosystem should be subject to minimum data security requirements, pursuant either to the GLBA or the FTC safeguards rule, as applicable. To provide for a higher level of security of consumer data and create a truly level playing field, however, we recommend that the CFPB require that all entities meet the minimum data security standards articulated in the FFIEC information security handbook.[28]

Finally, if the CFPB is going to rely on bilateral agreements as the primary way in which risk is allocated between parties in the ecosystem rather than expressly through regulation, the final rule must expressly acknowledge the right of financial institutions to require entities with whom their customers' data is shared to accept responsibility for harm that is attributable to them. Moreover, even if a liability framework is established by the CFPB, the final rule should permit data providers to deny access to authorized third parties that refuse to agree to the fair apportionment of liability, including, where appropriate, an indemnification obligation. In addition, the current rule, which provides that data providers may deny access to the developer interface or deny a data request based on reasonable risk management concerns about the authorized third party, should be explicitly extended to data

[28] FFIEC Information Technology Examination Handbook Information Security (September 2016), ffiec_itbooklet_informationsecurity.pdf.

aggregators acting on behalf of third parties. The rule should explicitly provide that nothing in the rule shall be interpreted as limiting a data provider's discretion to comply with existing prudential safety and soundness obligations, including third party risk management expectations.[29] These requirements will help incentivize all entities in the ecosystem to establish robust data security and other risk management controls.

6. <u>Data providers should be allowed to receive compensation from third parties to recover their commercially reasonable costs and a margin to cover the cost of enabling data sharing</u>.

Proposed § 1033.301(c) prohibits data providers from receiving compensation from authorized third parties for either establishing and maintaining the developer interface or receiving covered data requests and making covered data available. This prohibition should be removed. We propose instead that a new subsection be added to § 1033.311 permitting data providers to receive compensation from third parties, including data aggregators, to recover their commercially reasonable costs and a margin for establishing, maintaining, receiving requests on, and transmitting covered data on developer interfaces.

In sharp contrast, data aggregators and authorized third parties would be seemingly free to determine the fees, if any, they wish to charge their customers. This provision would only arbitrarily distort a marketplace between sophisticated commercial actors, resulting in nothing but an unfair allocation of benefits to data aggregators and an un-recoupable cost to data providers. The CFPB has an opportunity to benefit from the EU experience where policymakers have recognized the importance of permitting data providers to receive compensation that is "non-discriminatory and reasonable and may include a margin" from third parties for access to data.[30]

In addition to this being bad policy, we have doubts about the legality of this rule. Section 1033 does not contain a prohibition on reasonable fees for access. The CFPB is exceeding its authority by asserting that a reasonable fee would be, as a matter of law, contrary to the statute's text. Further, prohibiting data providers from charging reasonable fees to cover the operational costs of the developer interface may amount to a confiscatory taking of the costs of such services in violation of the Takings Clause of the Fifth Amendment to the United States Constitution. And where data providers are also national banks, proposed § 1033.301(c) does not appropriately consider a national bank's obligations under either the Office of the Comptroller of the Currency's regulations to operate in a safe and sound manner[31] or to set its fees according to cost, deterrence of misuse, or the safety and soundness of the bank.[32] Section (2)(b) of the Appendix discusses this topic further.[33]

---

[29] In addition, the rule should also state that nothing in the rule shall be interpreted as limiting a data provider's discretion to comply with any other relevant law. For example, data providers may have obligations to share covered data unrelated to the consumer-permissioned data sharing ecosystem governed by section 1033.

[30] *Provisional Agreement Resulting from Interinstitutional Negotiations; Proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)*, European Parliament (July 14, 2023), hereinafter "Provisional Agreement," *available at* https://www.europarl.europa.eu/RegData/commissions/itre/inag/2023/07-14/ITRE_AG(2023)751822_EN.pdf.

[31] 12 C.F.R. Part 30.

[32] 12 C.F.R. § 7.4002(b).

[33] There are similar obligations for state insured banks under state law and the Federal Deposit Insurance Act.

7. <u>The covered data categories of "Information to initiate payment to or from a Regulation E account" and "Terms and conditions" need substantial revision</u>.

Information to initiate payment to or from a Regulation E account

The CFPB should withdraw proposed § 1033.211(c) "Information to initiate payment to or from a Regulation E account." Section 1033 is an information production statute. The transitive right to receive a consumer's financial data does not grant a data aggregator or third party the right to initiate a payment from a consumer's Regulation E account and does not require data providers to allow third parties to do so. Open banking schemes in both the E.U. and the U.K. clearly distinguish between "account information services" and "payment initiation services," and require significantly heightened supervision, liability, and security for "payment initiation services" to appropriately protect consumers; none of these protections are present in the proposal.

Regulation E, the foundational consumer protection regulation for electronic fund transfers, was not drafted in consideration of data aggregators and third parties originating transactions from consumer accounts. Important questions remain unaddressed about the application of Regulation E's provisions regarding service providers, access device restrictions, error resolution, and various required consumer notices. Without appropriate consideration of these concerns, consumers will not be sufficiently protected and § 1033.211(c) would expose data providers to reputational and regulatory risks that they cannot measure, mitigate, or control. We urge the CFPB to withdraw this provision and engage with the prudential regulators to address its potential consequences.

Without appropriate consumer identity authentication, payment initiation creates significant risks of fraud and unauthorized transactions for consumers. Many credit-push payment networks appropriately require customer-identity authentication to initiate a credit-push payment from an account. Sharing customer identity authentication information with third parties creates excessive fraud risks, and we strongly oppose a requirement that this information be shared pursuant to section 1033. This information also fits squarely within the § 1033.221(b) exception to "covered data" for information used to prevent fraud. Additional information on this provision is provided in section (1)(d) of the Appendix.

Terms and conditions

Account terms and conditions as found in account opening disclosures and change in terms disclosures are legal contracts, whose prose is simply not compatible with sharing in a standardized format or comparable across account providers. The CFPB should retitle this provision as "Account pricing information" and include an illustrative reference in the example to the list of fees contained in 12 CFR § 1026.6 for credit cards and 12 CFR § 1005.7 and § 1005.8 for Regulation E accounts. These terms are generally included in terms and conditions documents, are well defined to market participants, would ease adoption of this proposed requirement, can be shared as discrete data values, and would permit product comparison. Section (1)(d) of the Appendix addresses this issue in greater detail.

8. <u>A standard setting body is best positioned to develop a standardized format for data sharing</u>.

We appreciate the CFPB's recognition in the proposal of the important role that industry-led standards have played in the successful development of the consumer-permissioned data sharing ecosystem to date. Industry stakeholders across the data-sharing spectrum have done substantial work to create data-sharing standards that are broadly used in the market today and are able to be further refined as use-cases evolve. Specifically, FDX is an example of an industry-led standards organization that has helped advance secure data sharing. FDX is an international, nonprofit organization operating in the United States and Canada. It is dedicated to unifying the financial industry around the FDX API, which is a common, interoperable, royalty-free standard for the secure access of permissioned consumer and business financial data. Through the development, adoption, and constant improvement of the FDX API, FDX and its members have made significant progress transitioning from credential-based screen scraping to the FDX API, with over 65 million consumer accounts using the FDX API as of Fall 2023.[34]

We support the proposal's reliance on industry-led standard-setting bodies ("SSBs") and believe an SSB is well suited to facilitate compliance with certain aspects of section 1033. The proposal contemplates formal recognition by the CFPB of SSBs which would permit them to issue qualified industry standards ("QISs"). We generally agree that CFPB recognition would promote market clarity and regulatory certainty with regard to the regulatory treatment of particular industry standards. As noted above, the industry has invested substantial resources in the FDX API and is concerned that absent designation as a QIS, the industry's investment in the standard – and the consumer protections the standard has provided – will be jeopardized. For this reason, as well as for the reason discussed below, we respectfully request that the CFPB move quickly to consider FDX for SSB status under the final regulation. We understand that FDX is committed to working with the CFPB to become a recognized issuer of a QIS.

The most important reference to a QIS in the proposal is with respect to the standardized format for covered data made available by a developer interface. Data providers would be "deemed to satisfy" the standardized format requirement by making covered data available in a format "set forth in a QIS," granting data providers a safe harbor for compliance with this provision.[35] We support this important reference to a QIS. We encourage the CFPB to recognize an SSB prior to the first compliance date for data providers to allow market participants to use a QIS as to "standardized format" during the initial compliance period.

Elsewhere in the proposal, conformance to a QIS issued by a recognized SSB would generally result in indicia of compliance with a particular provision of the rule. While the "indicia" standard seems designed to permit alternative methods of compliance, we caution that any QIS, even though it carries only indicia of regulatory compliance, could receive extraordinary weight by market participants. For this reason, we believe that the CFPB should remove references to a QIS conferring indicia of

---

[34] *See* FDX Press Release*:* "Financial Data Exchange (FDX) Reports 65 Million Consumer Accounts Use FDX API" (October, 5, 2023), *available at https://financialdataexchange.org/FDX/News/Press-Releases/Financial%20Data%20Exchange%20(FDX)%20Reports%2065%20Million%20Consumers%20Use%20FDX%20API.aspx (last accessed December 24, 2023)*. Almost all FDX Financial Institution (FI) members are using or plan to use the FDX API.

[35] Proposed § 1033.311(b).

compliance or indicia of reasonableness in several cases which are identified in the Appendix in section (1)(f). A more appropriate standard for certain compliance obligations would be one of commercial reasonableness, as we describe further in the Appendix.

Finally, we note that the CFPB must take additional action to ensure that an industry standardized format for covered data is adopted throughout the ecosystem. The proposal only imposes a standardized format requirement on data providers, which will be insufficient to drive these benefits to third parties, including new entrants and small entities. Lacking market power, small third-party recipients of covered data are "format takers" from the market-dominant data aggregators, who provide covered data to them using their own proprietary data formats. The use of these proprietary data formats across different aggregators imposes high switching costs on authorized third parties. One key benefit of encouraging the entire data chain to use a standardized data format is that it would promote competition in the data provisioning market by enabling authorized third parties to more easily switch data aggregators or implement direct relationships with data providers. For these reasons, the CFPB should also require data aggregators to make data available using the standardized format. See our discussion in section (1)(f) of the Appendix for more information standard setting bodies.

9. <u>The compliance date must be extended for data providers and should be explicit for third parties.</u>

Proposed § 1033.121 would stagger the dates by which data providers need to comply with proposed §§ 1033.201 and 1033.301 (the obligations to make data available and establish interfaces), but there is no explicit compliance date in the rule for third parties. Consumers stand to benefit from many provisions of the rule applicable to third parties, including the requirements on third parties to provide consumers a § 1033.411 authorization disclosure, to receive a consumer's express informed consent to access their covered data per § 1033.401(c), and obligations regarding limitations on data use and a maximum duration of an authorization described in § 1033.421.

We recommend that § 1033.121 be amended to expressly state that third parties seeking access to covered data must comply with the rule upon its effective date. This approach is compatible with the structure of the current proposal, but an explicit statement as such would provide significant clarity to market participants. For example, the rule and preamble do not specify whether a third party's obligations are tied to whether the data provider has reached its own compliance date. Further, the rule and preamble do not specify whether these third-party requirements are only applicable in the event of accessing a developer interface or whether they have broader applicability.

As to the time periods of the various compliance dates outlined in § 1033.121, we respectfully state that the proposal vastly underestimates the amount of work that even the largest and most technologically advanced data providers will have to undertake to achieve compliance. The proposed rule requires institutions of all sizes to adapt their current data provisioning practices to account for new covered data types, recordkeeping requirements, and processes to respond to requests for information. It also requires the creation of developer interfaces and compliance with performance specifications for those developer interfaces. For many institutions, the rule will also trigger the need for new or updated risk-management assessments of third parties. The work required likely will take even the most sophisticated data providers significantly more time to complete than is provided in the proposal. We recommend that the first compliance date not occur until 24 months after the final rule's publication in the Federal Register.

We further ask the CFPB to recognize that no data provider should be required to meet the requirement to establish a developer interface until a standard setting body is recognized by the CFPB and that entity has issued a QIS for a developer interface's standardized format.

If the first compliance date of §1033.121(a) is amended to 24 months, and if the subsequently sequenced compliance dates of subsections (b) through (d) are also further extended by 18 months, we generally would support the asset and revenue thresholds outlined. Additional detail about our recommendations regarding the compliance dates is set forth in section (1)(b) of the Appendix.

Conclusion

BPI and TCH appreciate the opportunity to comment on the proposed rule. As discussed throughout our submission, we support consumers' ability to share their account information safely and securely with third parties to enable those entities to provide consumers with a product or service they desire. Our recommendations for amendments to the proposal are intended to ensure that the already competitive and dynamic financial services ecosystem continues to foster responsible innovation while protecting consumers and their sensitive personal data.

/s/
Rodney Abele
Director of Regulatory & Legislative Affairs
The Clearing House Association

/s/
Paige Pidano Paridon
Senior Vice President,
Senior Associate General Counsel
The Bank Policy Institute

Appendix: Section-by-Section Discussion of the Proposed Rule

In this part, our comments are organized as follows:

1) Coverage and Definitions
   a) Coverage of data providers (§ 1033.111(a) through (c))
   b) Compliance dates (§ 1033.121)
   c) Definitions (§ 1033.131)
   d) Covered data (§ 1033.211)
   e) Exceptions (§ 1033.221)
   f) Standard Setting Body and Qualified industry standard (§§ 1033.131 and 1033.141)

2) Data Providers
   a) Obligation to make covered data available (§ 1033.201)
   b) General requirements of data provider interfaces (§ 1033.301)
   c) Requirements applicable to developer interfaces (§ 1033.311)
   d) Interface access (§ 1033.321)
   e) Responding to requests for information (§ 1033.331)
   f) Identifying information (1033.341(b))
   g) Data provider policies and procedures (§ 1033.351)

3) Authorized Third Parties
   a) Third party authorization procedures (§ 1033.401)
   b) Authorization disclosure (§ 1033.411)
   c) Third party obligations (§ 1033.421)
   d) Data Aggregators (§ 1033.431)
   e) Policies and procedures for third party record retention (§ 1033.441)

1) Coverage and Definitions

a) Coverage of data providers (§ 1033.111(a) through (c))

Proposed § 1033.111(a) provides that a "data provider has obligations under this part if it controls or possesses covered data concerning a covered consumer financial product or service, subject to certain exceptions."

With respect to the proposal, the CFPB should clarify or amend certain of the proposed definitions set forth in the proposal. For the avoidance of doubt, the CFPB should confirm that "covered data" shall only be covered with respect to covered financial products and services.

i) Definition of covered consumer financial product or service (§ 1033.111(b)).

Proposed § 1033.111(b) of the proposal defines a covered consumer financial product or service as a consumer financial product or service, as defined in 12 U.S.C. 5481(5), that is:

> (1) A Regulation E account, which means an account, as defined in Regulation E, 12 CFR 1005.2(b);

(2) A Regulation Z credit card, which means a credit card, as defined in Regulation Z, 12 CFR 1026.2(a)(15)(i); and
(3) Facilitation of payments from a Regulation E account or Regulation Z credit card."

The CFPB should clarify the scope of the proposed definitions of covered consumer financial products and services. First, the scope of Regulation Z credit card accounts that would be covered under the proposal would be overly broad and potentially extend beyond consumer credit cards, contrary to the statutory language. Proposed § 1026.2(a)(15)(i) cited in the proposed regulation would capture credit cards, defined as "any card, plate, or other single credit device that may be used from time to time to obtain credit. The term credit card includes a hybrid prepaid-credit card as defined in § 1026.61." In light of the clear statutory language and purpose of section 1033 to enable a *consumer* to obtain 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, the CFPB should clarify that the rule would not apply to corporate, business to business, or business-purpose cards, including business credit cards where a consumer may be personally liable.

In addition, as noted, a covered consumer financial service would include "facilitation of payments from a Regulation E account or Regulation Z credit card." The CFPB should further define this service in the rule text. The preamble to the proposal provides that "products or services that facilitate payments from a Regulation E account or a Regulation Z credit card—would be intended to clarify that the proposed rule would cover all consumer-facing entities involved in facilitating the transactions the CFPB intends to cover." In other words, as described further below, entities that control or possess information concerning a covered consumer financial product or service that the entity did not generate itself in connection with providing a financial product or service to the consumer but instead obtained from another data provider, such as a bank, should not be data that is permitted or obligated to be subsequently shared by that entity. If third parties want to obtain that data, they should seek it from the original data provider to help (i) ensure accuracy of the covered data, (ii) minimize consumer confusion regarding with whom they have authorized their data to be shared, and (iii) ensure that data providers can conduct appropriate due diligence on parties that obtain its data.

ii) Definition of data provider (§ 1033.111(c)

The proposal would define what entities would be considered "data providers." Covered data providers would be limited to:

> (1) A financial institution, as defined in Regulation E, 12 CFR 1005.2(i);
> (2) A card issuer, as defined in Regulation Z, 12 CFR 1026.2(a)(7); or
> (3) Any other person that controls or possesses information concerning a covered consumer financial product or service the consumer obtained from that person."
> "Example 1 to paragraph (c): A digital wallet provider is a data provider."

The CFPB should revise the proposed definitions of data providers in the following ways.

Expand the coverage of data providers

As BPI and TCH have previously asserted, to realize the full benefits of the statute, consumers should have access to their data related to all financial products and services that they obtain from any relevant data provider. The CFPB should expand the universe of data providers to include all entities

that provide any type of consumer credit product shortly after finalization of the final rule**.** Section 1033 provides that consumers may request certain information from "any entity that offers a consumer financial product or service;" thus, all such entities should be "covered entities" for purposes of the rule. We appreciate that the CFPB has stated that it would expand the scope of covered providers and products in the future. We respectfully request that the CFPB issue a proposal to expand the definition of "data provider" to include all entities that provide any type of consumer credit product shortly after finalizing the rule. The prioritization to expand the rule to cover providers of consumer credit products is appropriate given the demand in the market for products and services that require this data.

As we discuss throughout this letter, screen scraping must be eliminated from the ecosystem. Therefore, expanding the universe of covered entities and covered consumer financial products and services that must be offered via the developer interface and not obtained using access credentials should be expanded in very short order after any final rule is issued and screen scraping of that data prohibited. This step would help to achieve the goal of ultimately eliminating screen scraping.

Card issuer

The definition of "card issuer" in 12 CFR 1026.2(a)(7) cited in the proposal provides that a card issuer "means a person that issues a credit card or that person's agent with respect to the card." The official commentary to that regulation specifically provides that "a financial institution may become the agent of the card issuer if an agreement between the institution and the card issuer provides that the cardholder may use a line of credit with the financial institution to pay obligations incurred by use of the credit card." The CFPB should clarify how agents would be captured as data providers under the proposal and subject to any obligation to share covered data where the agent receives notice from an authorized third party.

Controlling or possessing information concerning a covered product or service

As noted above, the proposal defines a "covered consumer financial product or service" as a (1) Regulation E account; (2) Regulation Z credit card; and (3) Facilitation of payments from a Regulation E account or Regulation Z credit card.[36] Proposed § 1033.111(c)(3) includes in the definition of a "data provider" "[a]ny other person that controls or possesses information concerning a covered consumer financial product or service the consumer obtained from that person."

This definition would appear to capture, among other entities, those that "control or possess information concerning" "facilitation of payments from a Regulation E account or Regulation Z credit card" that "the consumer obtained from that person." For example, third parties that provide payment apps that help facilitate payments from Regulation E accounts would appear to be considered to control or possess information concerning facilitation of payments from a Regulation E account, a covered consumer financial product or service the consumer obtained from that third party. It is unclear whether aggregators that facilitate the transfer of information from a data provider to a third-party payment app, for example, may also be captured as possessing information concerning the facilitation of payments, as the connecting entity enabling the data to flow from the provider to the third party. The CFPB should clarify what entities specifically would be captured by the definition of "[a]ny other person

[36] For clarity, § 1033.111(b)(3) should be rephrased as "used to facilitate payments from a Regulation E account or Regulation Z credit card."

that controls or possesses information concerning a covered consumer financial product or service the consumer obtained from that person."[37]

Furthermore, the CFPB should make clear that entities that "control or possess information concerning a covered consumer financial product or service the consumer obtained from that person" may not share information that they possess when that information was obtained from another data provider related to the original data provider's provision of an account or other financial product or service to the consumer. Entities should only be permitted to share data they or their service provider have specifically generated or created in connection with the product or service they have provided to a consumer directly; facilitating entities should not be considered to be in possession of data related to a consumer financial product or service that a consumer obtained from the facilitating entity, as the facilitation is not the desired product or service, but rather is a means to providing the consumer with a desired product or service.

For example, when a consumer obtains a digital wallet app from a third party, that third party as a data provider should not be permitted to share data that it obtained from other companies related to accounts, products, or services offered by those companies to populate the wallet to enable payment functionality. Rather, the third party may only share unique data related to or generated in connection with the product or service *it offers* that it did not obtain from another company. In this example, if the consumer initiated a payment from the digital wallet app, data associated with that payment would fall under the scope of covered data, but data obtained from the consumer's Reg E account provider would not. If the consumer wishes to access or authorize sharing of information that the third party obtained from other entities, the consumer may authorize such sharing by the original data provider. We describe this further below in connection with the definition of a "digital wallet provider."

If the CFPB does not clarify this limitation on the scope of data that may be shared by entities that are considered to be data providers, fintechs and possibly aggregators that obtain information about a covered product from a consumer's bank (e.g., to provide the consumer with a desired product or service, such as a payment application), a consumer could authorize those entities to further share this data as they would be data providers under the proposal. However, the bank would not be able to conduct due diligence on companies that may access the consumer's bank data via those fintechs or aggregators, nor would the bank necessarily be aware of a consumer's revocation of authorization or the flow of data for risk minimization purposes when a data security issue arises. Furthermore, in this scenario, consumers may be confused about how to manage their authorizations related to their bank data and, importantly, how to revoke those authorizations, and the effect of revocation across various entities. This may cause consumers to inadvertently authorize sharing of sensitive bank data given the complicated layers of authorization and data sharing that are contemplated by the proposed rule. In short, only the entity that originated consumer data in connection with the specific product or service provided to the consumer should be permitted to share the relevant data pursuant to a consumer's authorization.

[37] The Clearing House Association, L.L.C. notes that the payment services offered to banks by The Clearing House Payments Company, L.L.C. are not "consumer financial products or services" pursuant to § 1033.111(b). Similarly, The Clearing House Payments Company, L.L.C. is not a data provider pursuant to § 1033.111(b) as a person that controls or possesses information concerning a covered consumer financial product or service that the consumer obtained from The Clearing House Payments Company, L.L.C. The Clearing House Payments Company, L.L.C. is highly regulated as a bank service company under the Bank Service Company Act, 12 U.S.C § 1861, and as the operator of a systemically important financial market utility, 12 U.S.C § 5462.

Digital wallet provider

Consistent with the analysis above, in this section, the CFPB cites a "digital wallet provider" as an example of an entity that would be captured in the third category of "data providers" – "Any other person that controls or possesses information concerning a covered consumer financial product or service the consumer obtained from that person."[38] The preamble states that a "digital wallet can facilitate payments from accounts that the digital wallet provider offers through depository institution partners, or from linked accounts that were originally issued by other institutions (sometimes referred to as pass-through payments).

However, the CFPB should further consider the circumstances in which a digital wallet provider should be considered a covered data provider. For example, the Bureau should consider whether the definition of "covered consumer financial product or service" should exclude digital wallets when the underlying account(s) in the wallet are already covered and the relevant covered data can be obtained from the source of the account(s) that are covered data providers, and the digital wallet generates no unique covered data.

The CFPB should consider whether bank service companies should be excluded from the definition of "data provider" because a consumer does not "obtain" a covered financial product or service from a bank service company; in some cases, digital wallets may be provided by a bank service company.

Moreover, consistent with the principle articulated above, the CFPB should clarify that the obligation of digital wallet providers to share data applies only to sharing covered data on the digital wallet provider's own stored-value accounts, transactions to or from those accounts, and transactions initiated through the digital wallet provider, including those initiated from a pass-through wallet. The consumer should <u>not</u> be able to authorize a digital wallet provider to share the consumer's data contained in or relevant to the digital wallet pertaining to a covered account provided by another company, which may also be displayed to the consumer in that digital wallet. Thus, when a digital wallet is a "pass-through" wallet, account and transaction details pertaining to a linked account (such as data related to a debit or credit card issued by a bank that appear in that wallet) should not be shared by the digital wallet with an authorized third party unless those transactions originated with or through the digital wallet. This limitation is consistent with the more general principle articulated above that entities will only be considered to be in "possession" of information about a product or service they have provided directly to a consumer rather than information obtained from another data provider in connection with the entity's providing a product or service to a consumer.

As referenced previously, the consumer should always be prompted to authorize sharing their data about a covered account or product or service directly from the company that provides that account, product, or service to the consumer. This authorization request should not come from any downstream party, like a wallet, a data aggregator, payment processor, or an authorized third party that has obtained access to that data through a consumer's permission, a digital wallet relationship, or otherwise. This is critical to ensure that consumers, data providers, and third parties and aggregators can manage all relevant risks effectively, ensure appropriate authorization and authentication is

[38] 88 Fed. Reg. at 74803-74804.

conducted, consider liability implications, and understand and ensure accountability for data security and consumer protection obligations and expectations.

b) Compliance Dates (§ 1033.121)

Proposed § 1033.121 would stagger the dates by which data providers need to comply with proposed §§ 1033.201 and 1033.301 (the obligations to make data available and establish interfaces). However, we were surprised not to find an explicit compliance date in the rule for third parties. Consumers stand to benefit from many provisions of the rule beyond the obligations on data providers to make data available and establish compliance consumer and developer interfaces.

We recommend that § 1033.121 be amended to explicitly state that third parties seeking access to covered data must comply with the rule upon the effective date of the final rule. Proposed § 1033.121 only provides staggered compliance dates for data providers, not third parties. The preamble supports this effect when it states:

> "The CFPB proposes that the establishment of part 1033 and the amendment to part 1001 shall take effect 60 days after the date of the final rule's publication in the Federal Register. In the case of part 1033, proposed § 1033.121 provides for staggered compliance dates for data providers. In the case of the amendment to part 1001, the CFPB has preliminarily determined that the activities covered by the amendment are already within the scope of the CFPA's definition of financial product or service, as explained in part IV, and so no compliance date is necessary."[39]

This approach is compatible with the structure of the current proposal but an explicit statement as such would provide significant clarity to market participants. For example, the rule and preamble do not differentiate a third party's obligations to meet its obligations based on whether the data provider has reached its own compliance date or not. Further, the rule and preamble do not specify that these third-party requirements are only applicable when the third party seeks to access a developer interface.

Consistent with our recommendations regarding proposed § 1033.331(c), third parties should be required to become "authorized third parties" pursuant to §1033.401 before they seek to obtain data, whether through a developer interface or a consumer interface via screen scraping

Proposed § 1033.331(c) could contain a new subsection stating that a data provider is not required to make covered data available in response to a request when "the third party is not an authorized third party." While we think this is obviously implied by § 1033.331(b), § 1033.331(c)(4)'s various requirements for an unexpired authorization, and the rule's foundational reliance on a consumer's authorization and a consumer's express informed consent, a clear statement as such would avoid confusion and ensure that third parties meet their obligations to become authorized third parties as soon as the rule becomes effective—to the extent they wish to collect consumer data from data providers.

If this requirement were implemented, even if the consumer's covered data is accessed through a consumer interface through screen scraping, such as in instances when the data provider compliance

[39] 88 Fed. Reg. at 74843.

date has not yet occurred, consumers will benefit significantly from the § 1033.401 requirements on third parties to provide consumers a § 1033.411 authorization disclosure and to receive a consumer's express informed consent to access their covered data per § 1033.401(c). Similarly, consumers will benefit when third parties begin to meet their obligations as described in § 1033.421, including the limitations on use and maximum duration of collection found in subparts (a) and (b) of this section, even if a consumer's covered data is gathered using screen scraping. These examples illustrate how consumers, even at excluded data providers and even with respect to noncovered data, would be provided some of the vital consumer protections of the proposed rule if § 1033.121 were amended to impose specific compliance dates for third parties seeking access to covered data as to §§ 1033.401 and 421.

As to the time periods of the various compliance dates outlined in § 1033.121, we respectfully state that the proposal vastly underestimates the amount of work that even the largest and most technologically advanced data providers will have to do achieve compliance. We do not think this is an overstatement, and we provide extensive comments in this letter to support our position. From new covered data types to the proposed recordkeeping requirements (which we largely object to), to the new processes to respond to requests for information, to completing appropriate risk-management assessments of third parties, to meeting the performance specifications of developer interfaces described in the proposal, the work required will likely take even the most sophisticated data providers much more time to complete than the proposed compliance dates would allow. We recommend that the first compliance date not occur until 24 months after the final rule's publication in the Federal Register. In the event that a data provider meets its compliance obligations before its corresponding compliance date, it should be entitled to enforce its rights and obligations under the rule as to third parties early as well, furthering consumer protection and motivating timely adoption.

We further ask the CFPB to recognize that no data provider should be required to meet the requirement to establish a developer interface until a standard setting body is recognized by the CFPB and has issued a QIS as to a developer interface's standardized format. See our discussion in section (1)(f) of this Appendix. It would also greatly aid uniform compliance if the CFPB would publish an examination manual to help the market implement appropriate compliance controls and processes in advance of any expected compliance data.

If the first compliance date of §1033.121(a) is amended to 24 months, and if the subsequently sequenced compliance dates of subsections (b) through (d) are also further extended by 18 months, we generally would support the asset and revenue thresholds outlined.

c) Definitions (§1033.131)

The CFPB should clarify and amend certain definitions in the proposal, as described further herein.

i) Authorized third party

Proposed § 1033.131 defines an "authorized third party" as "a third party that has complied with the authorization procedures described in § 1033.401." However, the proposal itself does not impose any requirements on authorized third parties to abide by the authorization procedures, but rather simply bases the third party's status as an "authorized" third party on the third party's meeting the obligations set out in § 1033.401. That section of the proposal provides that to become an

authorized third party, "the third party must seek access to covered data from a data provider on behalf of a consumer to provide a product or service the consumer requested and:

> (a) Provide the consumer with an authorization disclosure as described in § 1033.411;
> (b) Provide a statement to the consumer in the authorization disclosure, as provided in § 1033.411(b)(5), certifying that the third party agrees to the obligations described in § 1033.421; and
> (c) Obtain the consumer's express informed consent to access covered data on behalf of the consumer by obtaining an authorization disclosure that is signed by the consumer electronically or in writing."

However, the rule does not impose those obligations as requirements. Rather, those obligations operate simply as conditions the third party must meet to become an authorized third party, as defined, and thereby be able to obtain data from a data provider through its developer interface. The third party's obligations may be enforceable as contractual obligations between consumers and third parties, but those obligations do not appear to be requirements the CFPB intends to enforce to protect consumers. This proposed approach is even more concerning, because, as described herein, there is no incentive for third parties to become authorized third parties. While the compliance obligations set forth in the proposal would require data providers to establish a developer interface by a specific date, there are no requirements that third parties be prepared to use those interfaces by that same date or to use those interfaces at all. This lack of an affirmative obligation on third parties may also further incentivize third parties to use consumer credentials to obtain relevant data since there are no obligations on third parties to become authorized third parties. For this reason, as explained in section 1.b, above, third parties should be required to become authorized third parties and meet all the relevant obligations thereto by the effective date of any final rule.

As discussed in section 2 of the comment letter, the proposal does not explicitly prohibit screen scraping by third parties. We recommend, at a minimum, that the CFPB explicitly prohibit screen scraping by third parties once a data provider has made data—not limited to covered data – available via developer interface.

ii) Consumer

The definition of consumer is defined in § 1033.111(c)(2) as "a natural person" that includes trusts "established for tax or estate planning purposes are considered natural persons." We support the definition of "consumer" as a natural person, as proposed. The CFPB had previously contemplated defining "consumer" to include a consumer's agents within that definition. However, including agents in the definition of "consumer" could substantially complicate the operation of the ecosystem in practice, as there could potentially be numerous parties considered to be acting as agents of a consumer. This could result in confusion regarding authorization, authentication, and data use and retention. It is appropriate that consumers and entities acting on behalf of consumers are subject to different obligations and requirements under the rule to ensure that consumers have control over their data and that they and their data are protected.

On the other hand, the CFPB should consider whether to expand the definition of "consumer" to allow a consumer to designate a natural person acting on their behalf (such as an accountant or attorney) to access the consumer interface on behalf of the consumer in a safe and secure manner (such as using a tokenized version of the consumer's credentials) and not have to access the developer

interface , which could be burdensome and potentially technologically infeasible for an individual acting on a consumer's behalf.

The CFPB should further clarify the treatment of trust accounts. The CFPB proposes to define the term "consumer" to include trusts established for tax or estate planning purposes, but a trust is neither a natural person nor a legal representative of a person; it is a separate legal entity with a separate tax identification number. The CFPB should clarify how tax or estate planning trusts could authorize a third party to access the trust's data and what use cases would support third party access to that data.

The CFPB should further clarify that certain trust accounts are not covered consumer financial products or services within the scope of the rule. We note that the proposed rule defines a "covered consumer financial product or service" as an account defined in Reg E, but accounts held pursuant to a bona fide trust agreement are carved out of the definition of account for Reg E.[40] This exception should be clearly spelled out in the rule to ensure that bona fide trust accounts are not a covered consumer financial product or service under the final rule.

In addition, the CFPB should make clear that any requirements in the final rule will not override a bank fiduciary's duty to keep bank records confidential. Fiduciary accounts involving trusts and estates often involve multiple beneficial interests. Banks have a duty to maintain the confidentiality of beneficiary data and records, not only from third parties, but also from other beneficiaries of the account. That duty may mean that information provided to the bank to make a decision to distribute funds per the terms of the instrument by one beneficiary is restricted from disclosure to the other beneficiaries of the trust. Similarly, there is a risk that aggregating data from trust accounts may not be appropriate where all of the beneficiaries are not the same and could give an incorrect impression of entitlement to certain assets that is not accurate, which could result in consumer harm.

iii) Data aggregator

The proposal defines a data aggregator as "an entity that is retained by and provides services to the authorized third party to enable access to covered data." As we noted in section 3 of the comment letter, data aggregators play a significant role in the consumer-permissioned data sharing ecosystem and likely will continue to do so. The CFPB should amend various aspects of the proposal to ensure that data aggregators are subject to appropriate regulations and requirements to help ensure that consumers and their data are sufficiently protected. The CFPB also should subject data aggregators to the CFPB's supervision. We provide specific recommendations in section 3(d) of the Appendix below.

d) <u>Covered data (§ 1033.211)</u>

Proposed § 1033.211 would define six categories of covered data to include (a) transaction information, (b) account balance, (c) payment initiation information, (d) account terms and conditions, (e) upcoming bill information and (f) basic verification information. In general, we are supportive of the approach taken by the proposal, which takes a high-level approach to defining these categories of data, as opposed to a detailed list in regulation which seeks to enumerate every data element.

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

While we appreciate that §1033.211 defines covered data "as applicable," it would provide greater certainty to market participants if the CFPB were to make clear in the rule text, as it does in the preamble, that these are illustrative examples only.[41] The rule text should clarify that data providers only have an obligation to make available covered data to the extent it is kept, owned, or generated by the data provider for the particular type of account in question. Such a statement would be clearly supported by the text of section 1033(c) which disclaims any separate obligation on data providers "to maintain or keep any information about a consumer."

Finally, the CFPB should clarify that the elements of "covered data" apply only with respect to a "covered consumer financial product or service." Obligations with respect to, e.g., an account balance should not apply to the account balance of investment accounts or other products or services not yet included in the proposed rule.

i) Transaction information (§ 1033.211(a))

We are generally supportive of the category of transaction information, such as information typically found on periodic statements and account disclosures, and believe it is consistent with the statutory language regarding "any transaction" or "series of transactions." Standard setting bodies are well suited to defining an agreed taxonomy for various industries and data sharing use cases. We appreciate the CFPB's recognition that this will "allow flexibility as industry standards develop."[42] Therefore, we do not believe it is necessary for the rule to provide further examples.

In fact, additional examples may prove counterproductive. The proposal includes the example of "rewards credits" without further elaboration. We request the CFPB remove this term or revise this term to include only the disclosure of the rewards balance of the account, which is a data element that is commonly shared today.

Similarly, while we are generally supportive of a historical limit of 24 months of transaction information in § 1033.211(a), the rule should recognize that extensive historical information is not necessary or desirable in every use case. This section should also make clear that if a covered data provider makes all transaction data available, but it is less than 24 months of data, it has similarly complied with the requirements of this section. Sharing such information may put consumer privacy and data security at further risk and be beyond what is necessary for the specific product or service. Additionally, the rule should clarify that once an account is closed, data regarding the account is no longer required to be shared.

We also recommend that the rule further cabin the 24-month safe harbor to this historical transaction information section. The additional five categories of covered data are necessarily "point-in-time" data elements, and providers should only be required to report the "most recently updated covered data that it has in its control or possession at the time of a request" consistent with proposed §1033.201(b).

Lastly, we repeat our prior comments to the CFPB that sharing pending transaction details may unnecessarily introduce unreliable data into the ecosystem. Provisional transaction amounts may

[41] 88 Fed. Reg. at 74810.

[42] *Id*.

significantly differ from the amounts that are ultimately settled, if the transactions are settled at all. Introducing volatile information into the ecosystem is likely to cause significantly more issues and confusion than benefits for data providers, authorized third parties, and most importantly, consumers, alike.

ii) Account Balance (§ 1033.211(b))

The "account balance" category would include available funds in an asset account and any credit card balance. We support the inclusion of this category and note that, consistent with § 1033.201(b), this is a "point-in-time" data point, not historical information. We request that CFPB clarify that Regulation Z credit card accounts should report "total balance owed" on the account, as indicated in the preamble to the rule, and that this also be a current or "point-in-time" data point.

iii) Information to initiate payment to or from a Regulation E account (§ 1033.211(c))

Proposed § 1033.211(c), "Information to initiate payment to or from a Regulation E account," should be withdrawn. Section 1033 is an information production statute, granting consumers a right to receive information. It does not require data providers to allow third parties to initiate payments to or from consumer accounts. The transitive right to receive a consumer's financial data does not grant a data aggregator or a third party the statutory right to initiate a payment from a consumer's Regulation E account using any payment method available to a customer. The statute also grants no statutory authority to the CFPB to issue regulations which would purport to do so. Language in the preamble to the proposal supporting a "payment[s] use case" is not consistent with the text of the statute or legislative intent.[43]

Regulatory concerns

The rule and preamble discussion of this provision are less than one printed page of the proposal's Federal Register notice, and they fail to adequately address the consumer protection implications and payment system risks it embodies. The proposal also fails to appropriately undertake the requisite cost-benefit analysis required of a provision this important. The CFPB should fully recognize the unintended consequences of proposed § 1033.211(c), acknowledge its regulatory responsibilities, and withdraw this provision.

Proposed § 1033.211(c) could result in the wholesale expansion of third-party payment initiation across multiple payment systems in the U.S. Open banking schemes in both the E.U. and the U.K. clearly distinguish between "account information services" and "payment initiation services," and require significantly heightened supervision, liability, and security for "payment initiation services." None of these are present in this proposal to appropriately protect consumers, address the rights and obligations of commercial parties, or protect the integrity of U.S. payment systems.

The proposal recognizes that "many data providers have expressed concern about their Regulation E obligations"[44] if the section 1033 rule were to require the sharing of payment initiation information. These concerns are justified and borne out by experience. The CFPB must consider and

[43] 88 Fed. Reg. at 74811.

[44] *Id.*

address the obligations and liability of data aggregators or third parties that originate transactions from consumer accounts under Regulation E.

It is not clear whether data aggregators and third parties would be considered Regulation E service providers[45] or whether they would be subject to Regulation E's access device restrictions.[46] The CFPB must ensure that these parties also have obligations under Regulation E to investigate, resolve, and provide provisional credit to consumers who allege transaction errors, including unauthorized transactions.[47] Data aggregators and third parties should also have obligations to the consumer to provide Regulation E compliant general, initial, change-in-terms, and error resolution notices.[48]

Without appropriate consideration of these regulatory concerns, this provision would expose data providers to reputational and regulatory risks that they cannot measure, mitigate, or control. If the CFPB proceeds with some version of § 1033.211(c), it should create clear liability and indemnification rules to ensure that financial institutions bear no additional risks or costs as a consequence of a payment initiation by a data aggregator or third party, including costs from performing an investigation as a result of a consumer's notice of error.[49] Consumers will always expect their account-holding institution to address unauthorized transactions from their accounts, and we doubt that even extensive consumer disclosures will entirely mitigate the risk of reputational harm to data providers. The CFPB must also engage with the prudential regulators to address these consequences of its proposed regulatory action.

We agree that tokenized account and routing numbers ("TANs") "may help mitigate fraud risks to consumers and data providers" by allowing data providers "to identify compromised points more easily and revoke payment credentials on a targeted basis," and we support their broader adoption in the marketplace.[50] However, while TANs are useful and effective at stopping ongoing fraudulent transactions, they do not address the Regulation E concerns noted above.

The CFPB may conclude that some additional account identification information would help consumers identify which account data they would like to share. It could include this as an additional data element of § 1033.211(f) addressing "basic account verification information." The CFPB could track the language of Regulation E which references the "number of the account"[51] and should continue to allow the use of tokens or truncated account numbers (as is common in the market today) for this information.

Payment types

As drafted, the language does not specify which payment methods are in or out of scope, instead only providing that this category includes a tokenized account and routing number that can be

[45] 12 C.F.R. § 1005.14(a).

[46] 12 C.F.R. § 1005.5.

[47] 12 C.F.R. § 1005.11.

[48] 12 C.F.R. §§ 1005.4, 7, 8, and 11.

[49] 12 C.F.R. § 1005.11(b).

[50] 88 Fed. Reg. at 74811.

[51] 12 C.F.R. § 1005.9(b)(2).

used to initiate an Automated Clearing House ("ACH") transaction. There are many different payment systems and methods that can be used to initiate payments to or from a consumer's Regulation E account at a bank: ACH, wire, instant payments (RTP, FedNow), Zelle network, card networks, check, remotely created check, cash withdrawals and deposits, as well as potential future means of transfers that are currently unknowable. Additionally, many fintech Regulation E account providers offer their own propriety funds transfer services such as PayPal, Venmo, Cash App, and Apple Cash, among others. These payment types have different initiation methods, risks, consumer liability rules, use cases, interbank liability schemes, and payment features (e.g., irrevocable vs. subject to reversal/return/chargeback).

Not every payment method is available to all consumer accounts or every account providing institution, and some may not be appropriate for the use cases cited. Some payment methods, such as wire transfers and remotely created checks are not considered "electronic fund transfers," and thus not subject to Regulation E's consumer protections.

While an account and routing number can allow third parties to initiate ACH credits to, or ACH debits from, a consumer account, the language that references payments "from" a Regulation E account is ambiguous, as it does not distinguish between credit-push payments (initiated by the consumer through their financial institution) and debit-pull payments (initiated by the third party through their financial institution). In the example of the ACH network, an account and routing number are insufficient to initiate a credit-push payment from a consumer's account. It is only because the ACH network also supports debit pull payments that the account and routing number can initiate a payment "from" an account over the ACH network.[52] As discussed further below, the CFPB must not require a data provider to share information to initiate credit-push payments "from" a consumer's account and it is critical that the CFPB address this point. Proposed § 1033.211(c) should be withdrawn as it is does not give sufficient consideration to the unique characteristics of different payment systems.

Authentication information poses unreasonable fraud risks

Payment initiation creates significant risks of fraud and unauthorized transactions unless it also uses appropriate consumer identity authentication. In many credit-push payment networks, transaction initiation is, by design, more secure and generally requires customer identity authentication information in connection with the consumer's payment instruction to their financial institution to send a credit push payment from their account. Given the fraud risks from sharing customer identity authentication information with third parties, we strongly oppose the sharing of this information as within the scope of section 1033. This information also falls squarely within the exception provided by § 1033.221(b) for information used to prevent fraud. Similarly, the CFPB should not require the sharing of credit card

[52] In such a transaction, the consumer would be the ACH Receiver under the Nacha Operating Rules and may receive ACH debit or credit entries. The consumer's financial institution would be the Receiving Depository Financial Institution or RDFI. The ACH format requires the Originator of the entry to include the Receiver's account number and RTN (or a tokenized version that can be used for ACH transactions). The account number and RTN allows the debit or credit ACH entry to be routed to the RDFI and for the RDFI to post the entry to the consumer's account. The underlying payment mechanics and methods by which a payment may be initiated "from an account" are significant given that financial institutions do not generally offer consumers the ability to originate ACH entries (i.e., in which case the consumer would be the Originator and the consumer's financial institution would be the ODFI).

payment initiation information, such as Visa's card-verification value or MasterCard's card-verification code, which perform similar authentication security functions for "card not present" transactions.

We do not believe that account identification information would (or should) capture secure authentication information. If the CFPB proceeds with requiring additional account identification information under § 1033.211(f), the CFPB should clarify that information that a financial institution uses to authenticate its customer's identity is not required to be shared as covered data under the rule. Requiring a financial institution to share any information it uses to securely authenticate the identity of its customer (e.g., a one-time verification code) as part of a payment initiation process would pose significant risks to the integrity of various payment security standards. Further, it would conflict with the FFIEC's guidance on Authentication and Access to Financial Institution Services and Systems.[53]

Information is not authorization

The CFPB should acknowledge explicitly that even the third party's receipt of payment initiation information does not equate to obtaining the consumer's authorization to initiate a payment from their account under Regulation E, payment network rules, or other applicable law. For example, Nacha Op. Rule Subsection 2.3.2.2 sets forth specific minimum authorization requirements that an Originator must satisfy before originating an ACH debit entry to the consumer's account.[54] Given the complexities and risks noted above, § 1033.211(c) should be withdrawn.

iv) Terms and Conditions (§ 1033.211(d))

Data providers should not be required to provide account terms and conditions as a covered data category. Account opening disclosures and change in terms disclosures are legal contracts, whose prose is simply not subject to ready sharing or comparability as discrete data elements with digital values. Further, as the CFPB is aware, account terms and conditions are already provided directly to the consumer at account opening or upon a change in terms and upon request from most consumer interfaces. As described, the non-exhaustive list of examples provided in the proposed rule would not sufficiently limit all the information described by the phrase "terms and conditions," and could conceivably require the sharing of the entire raw text provided to customers and may include a significant amount of nonrelevant information. We believe this would be inconsistent with the intent of § 1033.311(b) that the developer interface make covered data available in a standardized format and would be excessively burdensome for both data providers and third parties. "Rewards program terms" is another example of terms and conditions that is not reducible to discrete values or readily comparable across products.

In the alternative, a much more limited set of key product pricing fields, such as those that are already required to be shared by Regulation E and Regulation Z would support comparison shopping. CFPB should retitle § 1033.211(d) as "Account pricing information" and include an illustrative reference in the example to the list of fees contained in 12 CFR § 1026.6 for credit cards and 12 CFR §1005.7 and

[53] https://www.ffiec.gov/press/PDF/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf.

[54] A third party acting as an ACH Originator will need to comply with such requirements before debiting the consumer's account and the third party's financial institution (ODFI) will warrant compliance to the consumers financial institution (RDFI) under the Nacha Operating Rules.

§1005.8 for Regulation E accounts. These terms are well defined to market participants, would ease adoption, can be shared as discrete data values, and would permit product comparison.

v) Upcoming bill information (§ 1033.211(e))

Third-party bill pay services, which enable payments from a customer's account to third parties, are a separate financial product and service distinct from a Regulation E account or a Regulation Z credit card. In other words, an entity could offer a Regulation E account without offering bill pay services and an entity could offer a bill pay service without offering a Regulation E account. The CFPB should revise this subsection to only cover payments due from the consumer to the data provider for the covered consumer financial product or service, such as a minimum payment due on a Regulation Z credit card or a preauthorized Regulation E electronic fund transfer under 12 CFR § 1005.10. This provision should also provide a reasonable time limitation on upcoming payments, for example limiting this category of covered data to the next six months.

While many bill pay products are bundled with bank-provided deposit accounts as a benefit to customers, they represent a separate product, often accompanied by their own set of terms and conditions. To the extent these services are captured by proposed §1033.111(b) as a covered consumer financial product or service, it is only because they may meet the definition of a "facilitation [service] of payments from a Regulation E account or Regulation Z credit card" under §1033.111(b)(3), a data category about which we have noted requires further clarification and explanation.

Third-party biller information is highly sensitive, with the potential to reveal intimate details about a consumer's financial relationships. Upcoming bill information is also subject to change as it relates to transactions that have not yet occurred. In addition, third-party biller information is distinct from all other types of covered data in that it is typically generated by the consumer and not verified by the data provider. Data providers do not know whether this information is accurate, and they are not responsible for creating it nor do they have control over resolving errors associated with the request. Requiring providers to share this information with authorized third parties would falsely suggest the data provider created the information and thus stands behind its accuracy, which could risk spreading inaccurate information across the consumer financial system that could be used by third parties to make unauthorized or erroneous transactions.

Consumers should be empowered to elect whether to share this discrete information with a third party just as they would be empowered by this proposed rule to share information about certain accounts, but not others, with third parties. It also creates risk for consumers regarding bills being paid correctly. Some may believe that, by mandating the sharing of upcoming bill information, a consumer could more easily port their scheduled bill payments from one financial institution to the next for account switching purposes. However, unlike in the case of the UK's payment switching service where: (1) there is a guarantee that payments will be redirected seamlessly; and (2) there is a centralized payment rail operator to redirect misdirected payments, such guarantees and functions do not exist in the United States. Accordingly, there is nothing to ensure that all bills at the initial financial institution will be turned off or that double payments will not occur. Lastly, data providers would be required to incur substantial costs to operationalize these new data elements, and, as proposed, would not be permitted to charge fees to third parties and aggregators for the data or operationalizing developer interfaces to transmit the data; to date, we have seen insufficient market demand to justify these costs.

vi) Basic account verification information (§ 1033.211(f))

We agree with the proposal that basic account verification information should be limited to the name, address, email address, and phone number associated with the covered consumer financial product or service. This selection of information would accommodate the vast majority of beneficial consumer use cases today. There are real privacy and security risks from sharing additional information, including consumers' most sensitive personally identifiable information. The release of such data is inherently prone to fraud and misuse. Importantly, the consumer is the true source of this information, and it is not information that is generated by a data provider in connection with the offering of a financial product or service. We support the limited, exhaustive list articulated in § 1033.211(f).

e) Exceptions (§ 1033.221)

The first exception to the definition of covered data would cover any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors. However, the proposal says that information would not qualify for this exception merely because it is an input to, or an output of, an algorithm, risk score, or predictor.

We have concerns that the proposal would frustrate the clear intent of § 1033(b)(1) by requiring the disclosure of algorithm inputs (data elements) and algorithm outputs (reward offerings, APYs, or otherwise). When combined, these can reasonably permit the determination of the algorithm itself, especially when a third party is permitted to evaluate a large data set of consumers specific to a given financial institution.

The CFPB should amend proposed § 1033.421(a)(2) to make clear that using covered data (whether or not that data is deidentified) to reverse engineer confidential commercial information, such as an algorithm used to derive credit scores, is a prohibited secondary activity that is not part of, or reasonably necessary to provide, any other product or service, similar to its prohibitions on targeted advertising and the sale of covered data.

We further suggest that the CFPB use its rule-writing authority to strengthen the language of § 1033.221 by restyling the section as "exemptions" instead of "exceptions" to further make clear that these data types are not covered by the rule.

f) Standard-setting bodies and qualified industry standards (§§ 1033.131 and 1033.141)

We agree with the approach taken by the proposal to recognize the important role that industry-led standards have played in successful development of consumer-permissioned data sharing. Industry stakeholders across the data-sharing spectrum have done substantial work to create data-sharing standards that work well, are broadly used in the market today, and are able to be further refined as use-cases evolve. The CFPB's final rule should not deter or detract from these initiatives and efforts. It should allow participants in the ecosystem to continue to build on these advances and permit the flexibility to develop and amend their specific practices to facilitate data sharing.

i) Industry standards for consumer-permissioned financial data sharing

A standard-setting body ("SSB")[55] is well suited to facilitate compliance with certain aspects of section 1033, which does not direct the Bureau to promulgate standardized formats for the exchange of information itself, but, rather to "prescribe standards applicable to covered persons to promote the development and use of standardized formats for information…."[56] The statute therefore envisions that the Bureau would pursue a principles-based approach that would provide high-level guidance pursuant to which private sector SSBs could develop and maintain detailed market-driven standards to facilitate the information exchange required by section 1033. We believe that a market-driven approach to the development and maintenance of a standardized format is far preferable than a regulatory one and that such standards should be developed through a private sector SSB that includes input from interested stakeholders.

Federal policy has long recognized the benefits of industry SSBs in the development of the kinds of technical standards that will be needed to achieve the Bureau's vision for §1033. Specifically, OMB Circular A-119 notes that agencies must use voluntary consensus standards in lieu of government unique standards except where inconsistent with law or otherwise impractical.[57] "Use" is defined to mean, "inclusion of a standard in whole, in part, or by reference in regulation."[58] The OMB notes that "[m]any voluntary consensus standards are appropriate or adaptable for the government's purposes."[59] The OMB further notes that the use of such standards is intended, among other things, to (1) eliminate the cost to the Government of developing its own standards and decrease the burden of complying with agency regulation, (2) provide incentives and opportunities to develop standards that serve national needs, and (3) encourage long-term growth for U.S. enterprises and promote efficiency and economic competition through harmonization of standards.[60]

The use of voluntary consensus standards, if done appropriately and established prior to any compliance data, would be both consistent with the law and practical, would eliminate the extraordinary cost to the Bureau of developing its own standards, would decrease the industry's burden of complying with the Bureau's anticipated section 1033 rulemaking, would continue to provide

---

[55] We here use the proposed rule's term "standard-setting body" which we believe to be synonymous with the terms "standard setting organization" and "voluntary consensus standards bodies" used in other contexts.

[56] 12 USC § 5533(d).

[57] Office of Management and Budget, OMB Circular A-199 (Rev.) Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities (February 10, 1998). In addition to directing agencies to use voluntary consensus standards wherever possible, the circular provides guidance for agencies participating in voluntary consensus standards bodies and proscribes procedures for satisfying the reporting requirements of the National Technology Transfer and Advancement Act of 1995.

[58] *Id*.

[59] *Id*.

[60] *Id*. Standards are defined broadly in the circular to include "common and repeated use of rules, conditions, guidelines or characteristics for products or related processes and production methods, and related management systems practices" as well as the "definition of terms; classification of components; delineation of procedures; specification of dimensions, materials, performance, designs, or operations, measurement of quality and quantity in describing materials, processes, products, systems, services, or practices, test methods and sampling procedures, or descriptions of fit and measurements of size or strength."

incentives for the industry to develop standards that serve national needs, and would promote efficiency and economic competition through the harmonization of standards.

SSBs already play an important role in facilitating data exchange outside of financial services. In the United States, there are numerous standards bodies that facilitate modern connectivity and data exchange, including the International Standard Organization (ISO), the Consultative Committee for International Telephony and Telegraphy (CCITT), the American National Standards Institute (ANSI), the Institute of Electrical and Electronic Engineering (IEEE), the Electronic Industries Association (EIA), Cellular-3GPP, the Wi-Fi Alliance, and the Bluetooth Special Interest Group (Bluetooth SIG).[61] Indeed, the breadth and ease of data exchange would not be possible without the work of private sector standards setting bodies.

Given federal policy that favors the work of private sector SSBs and the role that SSBs already play in financial services and in the broader economy, it is not surprising that Director Chopra has noted that "fair standards developed by the market to leverage [the Bureau's] rule will be critical to the creation and maintenance of an open banking system[.]"[62] The Director went on to observe that while the Bureau must resolve certain critical issues, much of the work to fully enable consumer-permissioned data sharing will fall on SSOs:

> "Our proposal will recognize that the CFPB must resolve certain core issues because system participants are deadlocked or because existing approaches do not put consumers fully in the driver's seat. But many of the details in open banking will be handled through standard-setting outside the agency."[63]

ii) Financial Data Exchange

Recognizing the need for industry standards in consumer-permissioned financial data sharing, an industry-led SSB has already made significant contributions to the development of consumer-permissioned data sharing in the United States. Financial Data Exchange ("FDX") is an international, nonprofit organization operating in the United States and Canada that is dedicated to unifying the financial industry around the FDX API, which is a common, interoperable, royalty-free standard for the secure access of permissioned consumer and business financial data.

FDX has broad stakeholder representation and is currently comprised of approximately 220 data providers (i.e., financial institutions), data recipients (i.e., third-party financial technology companies and financial institutions[64]), data access platforms (i.e., data aggregators and other ecosystem utilities),

---

[61] "Standards Organizations for Data Communications," *available at*: https://www.geeksforgeeks.org/standard-organizations-for-data-communications/#; *See also*, Qualcomm, "The Essential Role of Technology Standards (September 28, 2020), *available at* https://www.qualcomm.com/news/onq/2020/09/essential-role-technology-standards#:~:text=The%20Bluetooth%20SIG%20(Special%20Interest,products%2C%20and%20promoting%20its%20brand.

[62] Rohit Chopra, "Laying the Foundation for Open Banking in the United States" (June 12, 2023), *available at* Laying the foundation for open banking in the United States | Consumer Financial Protection Bureau (consumerfinance.gov).

[63] *Id*.

[64] Many financial institutions are both data providers and data users.

consumer groups, financial industry groups, and other permissioned parties in the user-permissioned financial data ecosystem.

The work being done by FDX has the benefit of further enhancing competition and innovation in financial services. A common, interoperable, royalty-free, market-led standard that has broad stakeholder support provides foundational requirements for entities seeking to serve the market for user-permissioned data sharing. Further, FDX, as a nonprofit industry standards body, also provides large incumbents and small startups alike with a level playing field on which to compete. By ensuring the interoperability of a wide range of related products, standards "make products less costly for firms to produce and more valuable to consumers."[65] Standards also help fuel dynamic competition by ensuring market-wide acceptance of the most innovative new technologies.[66]

We believe FDX has largely drawn a roadmap for a responsible way to protect personal financial data rights, and we support FDX becoming a CFPB recognized SSB pursuant to this rulemaking.

iii) CFPB recognition

Proposed § 1033.141(b) would provide for formal recognition by the CFPB of the SSB as an issuer of a qualified industry standard ("QIS"). Issuers of a QIS must have been recognized by the CFPB within the last three years under proposed § 1033.141(a)(7). We generally agree that CFPB recognition of an SSB would promote market clarity and regulatory certainty with regard to the regulatory treatment of an industry standard issued by SSBs. In this regard, we believe that FDX is committed to working with the CFPB to become a recognized issuer of a QIS.

The preamble to the rule requests comment on the procedures for recognition. We support the CFPB providing a flexible recognition process, so that participants are allowed to continue to use the data-sharing standards that are broadly used in the market today both before and after the rule's compliance dates. In particular, the CFPB should ensure there is recognition of an SSB prior to the compliance date to allow market participants the opportunity to build out and use an SSB QIS for a standardized format during the initial compliance period. The CFPB's process for recognition of an SSB should also continue to operate after the compliance date of the final rule, to allow for the recognition of new or additional SSBs over the life of the rule.

SSB recognition should also be permissible prior to or after an SSB issues a standard which it intends to become a QIS. We urge the CFPB to also consider the appropriate transition times for market participants, in the event that an SSB is not re-recognized by the CFPB prior to the expiration of a three-year recognition period, such as permitting the continuation of regulatory benefits for at least 12 months after the expiration of any recognition period. In the event that the CFPB recognizes multiple

---

[65] *See* U.S. Dept. of Justice & Fed. Trade Comm'n, Antitrust Enforcement and Intellectual Property Rights." Promoting Innovation and Competition, 33 (2007), *available at* Https://www.justice.gov/sites/default/files/atr/legacy/2007/07/11/222655.pdf.

[66] *See* Makan Delrahim, Ass't Att'y Gen., Antitrust Division, U.S. Dep't of Justice, "Don't Stop Thinking About Tomorrow": Promoting Innovation by Ensuring Market-Based Application of Antitrust to Intellectual Property. Remarks Before the Organization for Economic Co-operation and Development, 4 (June 6, 2019) (discussing the benefits of standard setting), *available at* https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-organisation-economic-co.

SSBs, and there exist potentially multiple QISs regarding the same issue, market participants should be given the option to adopt any QIS and avail themselves of its regulatory benefits.

iv) Characteristics for a recognized SSB

Proposed § 1033.141(a) would define the attributes of an SSB that is "fair, open, and inclusive," and thus able to issue QISs under § 1033.131. This list closely tracks the attributes of a voluntary consensus body outlined in OMB Circular A-199, which cites openness, balance of interest, due process, an appeals process, and consensus. Additionally, proposed § 1033.141 goes further than OMB Circular A-199 by explicitly including the quality of "transparency" in § 1033.141(a)(6). We broadly support these attributes as appropriate for a standard setting body in the personal financial data sharing context the rule. However, the CFPB should clarify that participants in the SSB should not be required to publicly share confidential, proprietary, or competitive information with any other members of the SSB or elsewhere.

Proposed § 1033.141(a) also further illustrates each of these attributes in the context of the section 1033 rulemaking. For example, proposed § 1033.141(a)(2) states that "decision-making power is balanced across all interested parties, including consumer and other public interest groups, at all levels of the standard-setting body."

We are concerned that achieving balanced decision making across all of the articulated interested parties at all levels of an organization may be an impractical standard to achieve in practice, depending on how it is defined. Voluntary standard setting organizations rely on the participation and engagement of their representatives for effective governance and are not able to compel participation or ownership by even critical parties. It is also unclear how the CFPB would interpret this attribute against the subsequent statement that the "ownership structure of entities is considered in achieving balance." We do not believe a necessary precondition of achieving "balance" is that every public interest group, small data provider, and small third party are equal co-owners of the SSB. There are also costs associated with forming and maintaining an SSB that must be considered, usually through the payment of membership fees. In order to achieve balance, it is important that parties contribute to the operation of the SSB to avoid free rider problems. We recommend that the CFPB consider the totality of the governance of an SSB when evaluating whether it meets the attribute of balance. CFPB should recognize that meaningful representation by diverse stakeholders at an SSB may be achieved through consultative governance processes, due process, and transparency in standards development.

v) Regulatory treatment of qualified industry standards

The strongest regulatory benefit from conformance with a QIS in the proposal is contained in proposed § 1033.311(b), which requires data providers to make covered data available in a standardized format. This provision would implement 12 USC § 533(d) which calls for the CFPB to "prescribe standards applicable to covered persons to promote the development and use of standardized formats for information." Data providers would be "deemed to satisfy" the standard format requirement in § 1033.311(b) by making covered data available in a format "set forth in a QIS," granting data providers a safe harbor for compliance.

We support both this regulatory safe harbor and the CFPB's principles-based regulatory approach. We believe these would provide both the regulatory incentives and flexibility so that private-sector standard-setting bodies like FDX could develop and maintain detailed, market-driven, data format

standards to facilitate the efficient and safe information exchange required by section 1033. Industry standards bodies are best positioned to reflect the technological and operational realities of data sharing and adjust to these over time as technological changes occur and consumer demand shifts. This approach would appropriately allow for innovation and development in consumer protections in a manner reflecting the speed with which changes occur in this ecosystem, while still promoting the "fair, open, and inclusive industry standards [that] are a critical element in the maintenance of an effective and efficient data access system" as stated by the preamble to the proposal.

The promotion of industry standards also appropriately encourages the adoption of standardized formats across the market. However, we believe that §1033.311(b) on its own will be insufficient to drive these benefits to the third parties, including new entrants and small entities, as suggested by the proposal's preamble. As a provision which imposes a requirement solely on data providers, the provision fails to address the second half of the two-sided market of consumer data sharing. Data aggregators and other data intermediaries which, especially for new entrants and small third parties, often provide the actual connection to data providers are under no obligation under the proposal to make covered data available in the same, or any, standardized format.

Lacking market power, small third-party recipients of covered data are "format takers" from the market-dominant data aggregators, who frequently provide covered data to small third-party recipients using their own proprietary data formats. The CFPB's rule must recognize the realities of the market that exist, not as it may wish it to be. If the CFPB in fact intends to ensure that covered data is "available in a standardized format that is readily processable by the information systems of third parties across the market, including new entrants and small entities," the rule must impose a corresponding obligation on data aggregators to at least meet a minimum standard of making covered data available in a standardized format. We suggest that this requirement be embodied in a new subsection of § 1033.431.

Elsewhere in the proposal, conformance to a QIS issued by a recognized SSB would generally result in indicia of compliance with a particular rule provision. In these cases, compliance with a QIS is not necessary to demonstrate compliance with a provision of the rule. While this standard seems designed to permit alternative methods of compliance, we caution that any QIS, even though it carries only indicia of regulatory approval, could receive extraordinary weight by market participants. For this reason, we believe that the CFPB should remove references to a QIS conferring indicia of compliance or indicia of reasonableness in several cases.

For example, we do not think any SSB will be well positioned to address the appropriate policies and procedures of either data providers or third parties as in § 1033.351 or § 1033.421. Federally supervised and examined entities are already under extensive requirements as to the sufficiency of their various policies and procedures, and these must necessarily be significantly tailored to the risk and complexity of each organization. These policies and procedures take into account both overlapping regulatory obligations regarding their operation and legal structure and must also be tailored to work within the firm-wide approach to policy and procedure administration and management. We are concerned that generic standards regarding policies and procedures, even when they only confer indicia of compliance, issued by an industry-wide standard setting organization will reduce compliance effectiveness overall, not improve it. Industry standard setting organizations are simply not well positioned to weigh in on the adequacy of policies and procedures, especially over a universe of banks and nonbanks that would be considered data providers under this proposal, and generally have not done so.

In other areas, the CFPB should remove the reference to a QIS conferring indicia and rely on a standard of "commercially reasonable." These include the performance specifications of developer interfaces in § 1033.311(c)(1)(ii) and the total amount of scheduled downtime in § 1033.311(c)(1)(i)(C). In both cases, industry standards are redundant to the general obligation to make covered data available found in § 1033.201(a) and § 1033.311(c)(1) which requires "commercially reasonable" performance of the subject developer interface.

Proposed § 1033.311(c)(2) regarding frequency of access restrictions contains multiple cross-references to otherwise permitted reasons for access denials, including a cross reference to § 1033.321 for denials related to risk management. We appreciate the recognition by the CFPB of the often extensive obligations on federally supervised, examined, and regulated entities which are already required to have effective risk management policies, procedures, assessment, monitoring, and control. Regulatory deference in the section 1033 rule to a generic QIS which overlaps with these existing obligations would invariably cause tensions, if not conflicts, with these existing requirements, even if it were not intended to do so. Reference to a QIS in § 1033.311(c)(2) should therefore be removed.

We are also concerned that a QIS as to the format and form of either a notice of downtime in § 1033.311(1)(i)(B) or a data provider's method for consumer revocation in § 1033.331(e) could improperly conflict with a federally supervised entity's regulatory obligations. In these instances, we believe the greatest risk of consumer harm is presented by un-supervised entities, whose policies and procedures and relevant compliance management systems are not regularly scrutinized.

Guidance from an SSB would be appropriate for these un-supervised entities to help ensure that they are not communicating in a way that unfairly influences a consumer's informed consent to share their data under section 1033, such as through the use of digital dark patterns. "Digital dark patterns are design features used to deceive, steer, or manipulate users into behavior that is profitable for a company, but often harmful to users or contrary to their intent."[67] CFPB's Consumer Financial Protection Circular 2023-01 illustrates how these practices can result in unfair, deceptive, or abusive acts or practices under the Consumer Financial Protection Act. We therefore recommend that the CFPB should consider referring to the "4P's" used by the Federal Trade Commission in determining whether a disclosure is clear and conspicuous.[68]

2) Data Providers

a) Obligation to make covered data available (§ 1033.201)

[67] "CFPB Issues Guidance to Root Out Tactics Which Charge People Fees for Subscriptions They Don't Want" *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-to-root-out-tactics-which-charge-people-fees-for-subscriptions-they-dont-want/#:~:text=Digital%20dark%20patterns%20are%20design,or%20contrary%20to%20their%20intent (*last accessed* December 25, 2023).

[68] The FTC has explained that if "a disclosure is truly clear and conspicuous, consumers don't have to hunt for it. It reaches out and grabs their attention. One mnemonic we use – The 4Ps – can help sharpen advertisers' focus on four key considerations:" *See* FTC "Business Blog: Full Disclosure" *available at* https://www.ftc.gov/business-guidance/blog/2014/09/full-disclosure (*last accessed* December 19, 2023).

Proposed § 1033.201(a) would require a data provider to make available to a consumer and an authorized third party, upon request, covered data in the data provider's control or possession concerning a covered consumer financial product or service that the consumer obtained from the data provider. The CFPB requests comment on whether it would be clearer to interpret CFPA section 1033(a) to set forth certain explicit prohibitions against practices that might make data unavailable or unusable.

We generally support the proposed formulation and do not believe that particular prohibitions are necessary. In addition to its general authority to compel compliance with §1033.201, the CFPB retains its authority against unfair, deceptive, or abusive acts or practices under the Consumer Financial Protection Act. Further, data providers, which are primarily depository institutions as providers of Regulation E accounts and issuer of Regulation Z credit cards, also comprise one of the most highly regulated and supervised sector of the consumer financial data ecosystem. Specific prohibitions designed to prevent evasion are both unnecessary and subject to incompleteness.

Proposed § 1033.201(a) also states that the covered data must be made available "in an electronic form useable by consumers and authorized third parties," due to the CFPB's interpretation that section 1033 should be read in the context of CFPA section 1002 which defines consumer to be inclusive of "an agent, trustee, or representative acting on behalf of an individual." Similar to our comments below regarding § 1033.301(b), we request that the CFPB recognize that the "electronic form" for data provided to consumers and authorized third parties can, and likely should, differ. The proposal acknowledges this distinction in practice by requiring both a consumer interface in § 1033.301 and a developer interface in § 1033.311, but it should be explicitly recognized that the "electronic forms" may differ as between these interfaces.

In addition to the rule text, the preamble states that proposed § 1033.201(a) would mean a data provider would have to make a consumer's data available in any language maintained in records under its control or possession.[69] For example, a data provider would have to make Spanish and English language records available if account records were maintained in Spanish and English. While this requirement might be reasonable in the context of the natural person consumer and the consumer portal, this statement should be clarified as entirely inapplicable as to authorized third parties, developer interfaces, the "electronic form" requirement of § 1033.201(a) as to these parties, and the "standardized format" requirement of § 1033.311(b). While certain consumer disclosures and contracts that potentially fall within the scope of covered data may be made available in languages other than English, we are unaware of any institution that maintains the data itself in any other language. In fact, data is often maintained in code, which isn't a traditional language at all. This statement should be clarified for the avoidance of confusion, particularly as to any QIS promulgated by a standard setting body.

We repeat our prior comments to the CFPB that sharing pending transaction details may unnecessarily introduce unreliable data into the ecosystem. Provisional transaction amounts may significantly differ from the amounts that are ultimately settled, if the transactions are settled at all. Data providers should not be required by regulation to provide this information to third parties, but instead, the market should be permitted to determine if this type of data is necessary and useful to provide consumers with access to desired products and services or alternatively, permit data providers

[69] 88 Fed. Reg. at 74809.

to determine which approach is less burdensome between providing only settled or settled and unsettled transaction information.

b) General requirements of data provider interfaces (§ 1033.301)

i) Consumer and developer interfaces

Proposed § 1033.301(a) requires a data provider to maintain a consumer interface and to establish and maintain a developer interface. Given the CFPB's interpretation that a statutory section 1033 "consumer" should be read inclusive of "an agent, trustee, or representative acting on behalf of an individual," we support the CFPB's recognition that authorized third parties should not be permitted to use consumer portals to retrieve consumer data. To further the goals of reducing screen scraping and to ensure compliance by all third parties with the rule, there should be an explicit provision in § 1033.401 to prohibit third parties from seeking access to covered data from a data provider unless they are an authorized third party in accordance with § 1033.401. In addition, once a developer interface has been established, in the event that a third party or data aggregator acquires covered data directly or incidentally through screen scraping to retrieve non-covered data, the CFPB should require the third party or aggregator to delete the covered data immediately before any use, copying, or further sharing. Screen scraping for non-covered data should not provide a loophole to the general requirement that third parties and data aggregators must access covered data through a developer interface if one is available.

We strongly support the cessation of screen scraping and credential-based access and agree with the preamble to the proposal when it states that "screen scraping as a whole presents risks to consumers and the market and relying on credential-based screen scraping would complicate the mechanics of data access, particularly with respect to authentication and authorization procedures for data providers."[70] We support the CFPB's conclusion that screen scraping should not be an alternative method of access for authorized third parties. The CFPB should consider additional ways to more explicitly forbid screen scraping in order to better protect consumers in the final rule, such as those we suggest in section 2 of the comment letter.

ii) Machine-readable files

Proposed § 1033.301(b) requires that data must be available in "machine-readable file" to both consumers and authorized third parties, upon specific request. Example 1 to paragraph (b) elaborates that this requirement would be satisfied "if the data can be printed or kept in a separate information system that is in the control of the consumer or authorized third party." The preamble suggests that "as a general matter, existing consumer and developer interfaces typically already provide covered data in a form that would comply with this requirement."[71] Furthermore, it states that this provision would ensure that consumers and authorized third parties "can retain electronic files."[72] We request that the CFPB separate this requirement as to natural person consumers and the consumer interface from authorized third parties and the developer interface. In particular, § 1033.301(b) should be limited to

[70] 88 Fed. Reg. at 74813.

[71] 88 Fed. Reg. at 74814.

[72] *Id.*

specify that it is only applicable to consumers and consumer interfaces and continue to make this requirement applicable only upon specific request.

We believe the intent of this provision is to ensure that data providers make data available in a format that consumers can print or keep of their records. Web-based consumer interfaces today allow consumers to print the information displayed on screen to paper or saved as a computer file, when a consumer instructs a web browser to save the page as either a webpage as an HTML file or a PDF. These formats are able to be retained, are machine-readable, can be printed, and display information in a format that is designed for a human reader.

Developer interfaces, covered further below, should be encouraged to use much more sophisticated data formats, such as application programing interfaces or "APIs" to better protect the use of consumer data by third parties. API formats are already data-element delimited to facilitate database functionality. Requiring a parallel computer file format, such as CSV, in addition to an API is excessively burdensome for data providers and not outweighed by any benefit to either authorized third parties or consumers. Importantly, use of APIs does not inhibit an authorized third party from receiving any covered data, so there would be no practical benefit from requiring authorized third parties to provide data in computer file format. Proposed § 1033.301(b) should be amended to remove all references to authorized third parties. To the extent that the CFPB wishes to apply a parallel "machine-readable" requirement to authorized third parties, it could amend § 1033.311(b) to reference a "standardized machine-readable format;" however we believe this would be redundant with the phrase "readily usable by authorized third parties" of § 1033.311(b)(2) and with what we believe would be required in practice by any QIS referenced in § 1033.311(b)(1).

iii) Fees for use

Proposed § 1033.301(c) prohibits data providers from receiving compensation from authorized third parties for either establishing and maintaining the developer interface or receiving covered data requests and making covered data available. This proposed requirement widely misses the mark. Proposed § 1033.301(c) should be removed in its entirety.

We propose instead that a new subsection be added to § 1033.311 permitting data providers to receive compensation from third parties to recover their commercially reasonable costs and a margin for enabling third party data sharing. This approach would ensure that that data providers do not use this right to compensation in a manner to evade compliance with the rule's requirement to generally make data available, while also encouraging competitive markets to determine the value and cost of the services of developer interfaces. This approach would also provide a market incentive for authorized third parties to "limit [their] collection … to what is reasonably necessary to provide the consumer's requested product or service" per the requirement of proposed § 1033.421(a). The proposal currently provides no incentive to authorized third parties (and no means to data providers) to ensure that authorized third parties are reasonably limiting the scope and frequency of their requests to what is truly needed to deliver the product or service.

Policy considerations

The proposed cost recovery prohibition is misguided in addressing only one side of the two-sided consumer data sharing market. If the CFPB's ultimate goal is to provide authorized third parties with free covered data, like consumers, in the hopes that they will then pass on the benefit of this free

good to consumers, the proposal does nothing to address the fees for access that data aggregators impose, or the fees charged by the authorized third parties to consumers. In practice, very few authorized third parties connect directly to data providers today, and data aggregators charge authorized third parties for making covered consumer data available to them. Instead, this provision would only arbitrarily distort a marketplace between sophisticated commercial actors, resulting in nothing but an unfair allocation of benefits to data aggregators and an un-recoupable cost to data providers. As proposed, this provision would artificially tilt the free market in favor of data aggregators and authorized third parties who are free to determine the fees, if any, they wish to charge, especially in instances where those parties are not also covered data providers. Banning fees on only some market participants will reduce competition to the detriment of consumers.

The experience of the European Union ("EU") is particularly instructive on this matter. Having seen anemic growth in its personal financial data sharing ecosystem, the EU is actively working on proposals to advance open finance and the sharing of financial data in the EU through both the Data Act[73] and the Financial Data Access ("FiDA")[74] regulation. In the context of these negotiations, European policymakers have recognized the importance of permitting data providers (called "data holders" in the EU) to receive compensation from third parties (called "data users" in the EU) for access to data shared through APIs. These fees are intended to be "non-discriminatory and reasonable and may include a margin."[75]

FiDA recognizes:

> "To ensure that data holders have an interest in providing high quality interfaces for making data available to data users, data holders should be able to request reasonable compensation from data users for putting in place application programming interfaces. Facilitating data access against compensation would ensure a fair distribution of the related costs between data holders and data users in the data value chain."[76]

These considerations are justified. The CFPB has an opportunity to benefit from the EU experience, and § 1033.301(c) should be removed in its entirety. The final rule should also add a new subsection to § 1033.311 permitting data providers to receive compensation from third parties, including data aggregators, to recover their commercially reasonable costs and a margin for establishing, maintaining, receiving requests on, and transmitting covered data on developer interfaces.

Some have speculated that § 1033.301(c) could similarly bind service providers to data providers. The proposal does not articulate a standard for determining when an intermediary would be

---

[73] *Provisional Agreement Resulting from Interinstitutional Negotiations; Proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)*, European Parliament (July 14, 2023), hereinafter "Provisional Agreement," *available at* https://www.europarl.europa.eu/RegData/commissions/itre/inag/2023/07-14/ITRE_AG(2023)751822_EN.pdf.

[74] *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554. European Commission*, European Commission (June 28, 2023), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0360&secureweb=OUTLOOK.

[75] *Provisional Agreement*, *supra* note 56, Article 9.

[76] FiDA, *supra* note 57, Recital 29.

considered the service provider to a data provider or to an authorized third party. Our proposal to allow commercially reasonable costs and a margin would avoid the need for this distinction.

Legal concerns

We also have concerns that the fee prohibition in proposed § 1033.301(c) is not grounded in the statutory text of section 1033 which contains no prohibition on cost recovery by data providers, and particularly no carveout for authorized third parties and data aggregators, nor in any other authority granted to the CFPB under the CFPA. It is a misreading of the CFPB's authorities to claim that a reasonable fee would be, as a matter of law, contrary to either the statute's text or its objectives.

It must be recognized that proposed § 1033.301(a) would mandate that banks which have consumer interfaces today must "establish and maintain" a developer interface. We are unaware of prior legal precedent by which a financial institution has ever been required by force of regulatory rulemaking alone to engage in offering a new financial product, in this case, the developer interface. For example, financial institutions are not required by regulation to offer Regulation E accounts, issue Regulation Z credit cards, or offer bill pay services. Instead, financial institutions have been permitted to offer products and services based upon fulfilling the needs of their customers and potential customers in a competitive market. New proposed § 1001.2(b) recognizes this developer interface as a new and separate financial product or service which is required to be offered by banks which offer covered products such as Regulation E accounts and Regulation Z credit cards. The CFPB also notes in the preamble that it preliminarily views, among other things, the transmission of financial or banking data, as already within the scope of the CFPA's definition of financial product or service.[77] Such a requirement is clearly beyond the CFPB's statutory authority as described by section 1033. Indeed, section 1033(a) requires only that entities "make available" certain information to consumers "upon request" and in "electronic form."[78] But this mandate does not prescribe a single method or channel by which entities must make information "available." Nor does it compel entities to establish and maintain developer interfaces, much less with all the features prescribed by the proposed rule.

Further, we have substantial concerns that prohibiting data providers from charging reasonable access fees on authorized third parties and data aggregators for the use of the developer interface violates the Takings Clause of the Fifth Amendment to the United States Constitution. Not only is the requirement to establish and offer a developer interface per proposed § 1033.301(a) unjustified, but the operation of § 1033.301(c) prohibiting data providers from charging reasonable fees, including to cover the costs of the operation of such a service, would amount to an uncompensated taking of such services from data providers, even setting aside questions about ownership of the data itself and the inherent value of that data.

In particular, the fee prohibition would constitute a physical taking because the rule is a forced sale or mandate to provide free services to data aggregators and other third parties.[79] The fee prohibition would also be a regulatory taking given the character of the action (effectively commandeering data providers' infrastructure and data services and access for the benefit of third

[77] 88 Fed. Reg. at 74842.

[78] 12 U.S.C. § 5533(a).

[79] *See Garelick v. Sullivan*, 987 F.2d 913, 916 (2d Cir. 1993); *Horne v. Dep't of Agric.*, 576 U.S. 350, 358, 360 (2015) (holding mandate to turn over portion of raisins grown to be a taking).

parties) and the economic impact of the regulation (mandating the creation of infrastructure and provision of services without any compensation, at great cost to data providers).[80]

Proposed § 1033.301(c) also does not appropriately consider a national bank's obligations under either the OCC's 12 CFR Part 30 to operate in a safe and sound manner or the OCC's 12 CFR § 7.4002(b) to set its fees according to:

> "(i) The cost incurred by the bank in providing the service;
> (ii) The deterrence of misuse by customers of banking services;
> (iii) The enhancement of the competitive position of the bank in accordance with the bank's business plan and marketing strategy; and
> (iv) The maintenance of the safety and soundness of the institution."

We strongly object therefore to the simultaneous requirements of § 1033.301(a) which compels data providers to "establish and maintain" a developer interface, a unique product or service under 1001.2(b), and of § 1033.301(c), which prohibits data providers from imposing even reasonable fees on authorized third parties and data aggregators for the costs of establishing, maintaining, receiving requests for covered data, and making covered data available in response to such requests.

In sum, § 1033.301(c) should be removed in its entirety. The rule should encourage market-based competition and instead create a new subsection to § 1033.311 permitting data providers to recover their commercially reasonable costs and a margin for establishing, maintaining, receiving requests on, and transmitting covered data on developer interfaces.

c) Requirements applicable to developer interfaces (§ 1033.311)

Proposed § 1033.311(a) would require that a developer interface "must satisfy the requirements set forth in this section." Proposed § 1033.311(b) would require the use of a standardized format. We broadly support the requirement that a developer interface should be required to make covered data available in a standardized format. We further support the language of § 1033.311(b) and 311(b)(1) that data providers would be "deemed to satisfy" the standard format requirement in § 1033.311(b) by making covered data available in a format "set forth in a QIS," granting data providers a safe harbor for compliance. In the event that multiple QISs exist regarding a "standardized format," a data provider should be granted this presumption of compliance regardless of which QIS it implements.

We also support the fallback language of § 1033.311(b)(2) which provides similar protection for the use of "widely used" formats that are readily useable by authorized third parties. It would be helpful if the CFPB could provide illustrative examples of widely used formats, especially prior to the rule's effective date, to give market participants confidence that they are entitled to the presumption of compliance of § 1033.311(b).

i) Performance specifications

While we agree that an SSB, such as potentially FDX, would be well positioned to address industry standards for standardized formats and for helping to define covered data elements, we do not

[80] *See Penn Central Transp. Co. v. New York City*, 438 U.S. 104, 124 (1978).

support a QIS conferring indicia of compliance as to the performance specifications of developer interfaces in various provisions of § 1033.311(c). References to a QIS should be removed from: § 1033.311(c)(1)(i)(B) regarding a reasonable notice of downtime, § 1033.311(c)(1)(i)(C) regarding the total amount of scheduled downtime, and § 1033.311(c)(1)(ii) regarding the performance of the interface as a whole. The appropriate standard for all of these provisions is already articulated by § 1033.311(c)(1), which requires "commercially reasonable" performance of the subject developer interface. Thus, any reference to a QIS is duplicative, at best, or inconsistent with that requirement, at worst.

We also submit that the regulatory standard in § 1033.311(c)(1)(i) that the "number of proper responses by the interface divided by the total number of queries for covered data to the interface must be equal to or greater than 99.5%" is both unreasonably high and incomplete in that it fails to consider the performance of the requestor in formatting and articulating a request. This "quantitative minimum specification" should be removed from the rule in favor of the "commercially reasonable" standard already articulated in § 1033.311(c)(1). We also reject the assertion in the preamble that, to the extent that the rule retains any quantitative minimum specifications, that a concurrent QIS could become a new more stringent requirement to meet a "commercially reasonable" standard.[81]

In the alternative, if the CFPB insists that some quantitative floor is necessary, the final rule should adopt the more widely used metric of the percentage of developer interface uptime relative to unscheduled downtime discussed below. We suggest, based on the experience of other jurisdictions described below, that a 95% uptime requirement for a developer interface would be both ambitious for the United States market and achieve the goals of the CFPB, while helping to ensure that data continues to be made available to consumers.

The preamble justifies the 99.5% figure by stating that Australia and the United Kingdom "set their thresholds at 99.5 percent" for platform availability.[82] We do not believe these metrics are appropriately comparable to the standard of proposed § 1033.311(c)(1)(i). The Australian government website states that "a period of unavailability is any period of time when any of the API end points defined in the standard is unable to reliably provide a successful response to an appropriately constructed request."[83] It states further that the availability requirement "does not include planned outages." The "platform availability" figures cited in the preamble are therefore closer to a measure of platform uptime relative to unscheduled downtime. It is noteworthy that even using Australia's simple uptime standard, "From December 1, 2021, through September 1, 2023, Australian data holders maintained a platform availability of 96.28 percent," well below the CFPB's proposed 99.5% standard.[84]

Similarly, the metric used by the U.K., which requires quarterly uptime of 99.5% for Account Servicing Payment Service Providers ("ASPSPs"), the equivalent of data providers in the proposal, is

[81] 88 Fed. Reg. at 74817.

[82] 88 Fed. Reg. at 74816.

[83] *See* https://consumerdatastandardsaustralia.github.io/standards/#availability-requirements.

[84] 88 Fed. Reg. at 74816, note 77, *citing* Australian Consumer Data Right, Performance, https://www.cdr.gov.au/performance.

calculated as a "the percentage uptime as 100% minus the percentage downtime."[85] "Downtime" is calculated in the U.K. by an ASPSP "from the moment it has received the first request in the series of five consecutive requests that were not replied to within 30 seconds, provided that there is no successful request in between those five requests to which a reply has been provided."[86] This requirement is therefore also not equivalent to the standard articulated in proposed § 1033.311(c)(1)(i)(D) which does not use any measure of time in its calculation. Instead, under the proposal, every response which is not a "proper response" would count against the 99.5% requirement, whether the platform was generally available or not. The standards for platform availability and uptime in Australia and the U.K. are not comparable to the "proper response" requirement in § 1033.311(c)(1)(i)(D).

Further, these examples are not instructive given the vastly more diverse composition of the United States, where there are many thousands of potential data providers, many of which are smaller than those in other jurisdictions. The concentration of banks in both jurisdictions is vastly higher, where for example the U.K. has only 353 deposit-taking institutions (129 domestically headquartered) and Australia has just over 90 banks (approximately 60 of which are domestically headquartered).[87] In light of the diverse, and already more successful, consumer data sharing ecosystem in the United States than either of these jurisdictions, the CFPB should not attempt to impose a quantitative 99.5% successful return rate threshold.

Conclusions drawn from the CFPB's Provider Collection,[88]such as that "a number of providers' extant consumer interfaces generally meet or exceed" this metric, are similarly inapposite.[89] The Provider Collection surveyed only the largest data providers in the United States, who we suspect field some of the most sophisticated interfaces today.[90] Further, this claim cites to the performance of consumer interfaces alone. Consumer interfaces do not depend on appropriate data request formatting from an authorized third party, they call information natively from the data provider's own website design. The CFPB acknowledges that even large data providers' developer interfaces reported widely varying performance metrics.[91] Further, there are likely to be significant impacts on the performance of the interfaces upon implementation of any final rule, including the likelihood that the number of calls to existing interfaces is going to significantly increase.

It is not clear from the proposal whether a transmission error that is the result of an improperly articulated or formatted data request would result in an improper response by the data provider or not.

---

[85] *See* https://standards.openbanking.org.uk/operational-guidelines/availability-and-performance/key-indicators-for-availability-and-performance-availability/latest/

[86] *Id.*

[87] *See* https://www.statista.com/statistics/870166/number-of-banks-operating-in-the-uk-by-country-of-residence/#:~:text=Monetary%20Financial%20Institutions%20(MFI)%20include,UK%20headquartered%20(parent%20company) *and* https://theaufinance.com/banks.

[88] The CFPB states in the preamble that in January 2023, the CFPB issued two sets of CFPA section 1022(c)(4) market monitoring orders to collect information related to personal financial data rights—one set of orders was sent to a group of data aggregators (Aggregator Collection); the second to a group of large data providers (Provider Collection). 88 Fed. Reg. at 74802.

[89] 88 Fed. Reg. at 74816.

[90] 88 Fed. Reg. at 74802.

[91] 88 Fed. Reg. at 74816.

These failed transmissions would not the fault of the data provider and should not count against the performance standards applicable to the data provider's developer interface. Successful data returns require the appropriate authorizations, customer and account identification, and data element identification which are elements of a proper data request. Australia recognizes the distinction between uptime and communication errors and recognizes that requests can fail as a result of "client-side problems, server-side problems and authentication issues." The Australian government's Consumer Data Right website goes on to state that "Errors typically arise where an [Accredited Data Recipient] uses incorrect syntax to request customer information."

A successful data return is a two-way street which requires the accurate communication performance of both the data requestor (the authorized third party or data aggregator) and the data provider. If proposed § 1033.311(c)(1)(i)(D)(*1*) which defines a "proper response" is retained—and it should not be—it should be revised to explicitly state that failed transmissions which are the result of an improperly formatted request or do not contain the appropriate authorizations, customer and account identification, and data element identification, or where the requests give rise to risk-based denials, do not count against the performance standards applicable to the data provider's developer interface.

We also oppose the quantitative minimum specification for response times articulated in § 1033.311(c)(1)(i)(D)(*3*). Australia's performance standard for response times for data providers is "95% of calls per hour responded to within a nominated threshold."[92] The proposal would have no similarly reasonable percentage for response time performance. It articulates an absolute standard of 3,500 milliseconds in all cases. Australia however further distinguishes response rates by the priority, type, and amount of information requested. For example, a very simple request, such as an inquiry as to the status of a developer interface, is an independent request with a very short response rate. Larger requests, such as "Get Bulk Direct Debits," are allowed 6000 millisecond response times in Australia. The proposal should simply apply the baseline "commercially reasonable" standard in this case and acknowledge the complexity inherent in setting appropriate response rates given the type and amount of information contained in a data request. In the alternative, at most, § 1033.311(c)(1)(i)(D)(*3*) could require the average latency of all response times to be under a certain threshold instead of mandating that every response's latency be under that threshold and permit the SSB to establish reasonable response times. The means and size for the future delivery of data are also unknown and by including an absolute standard for response times, it may unintentionally restrict improved means of complex data delivery.

Further, as currently constructed, it should be recognized that the rule would impose not only a requirement for data providers to create a developer interface, but also that the developer interface they offer must meet this 99.5% successful return rate. We reiterate our prior statement that § 1033.301(a), which would mandate that banks which have consumer interfaces today must "establish and maintain" a developer interface, is beyond the CFPB's statutory authority. The idea that the CFPB may also require such an interface to meet an arbitrary 99.5% successful return rate per § 1033.311(c) is a further illustration of how far the proposal is well beyond the CFPB's regulatory authority to impose on data providers. Our proposed revisions to § 1033.301(a), which would allow for data providers to charge reasonable fees to third parties for the development and maintenance of the consumer and developer interfaces, and our suggested changes to the quantitative minimum performance specifications, are designed to address these concerns.

[92] *See* https://consumerdatastandardsaustralia.github.io/standards/#performance-requirements.

We also recommend that the CFPB remove the requirements of § 1033.311(c)(1)(ii), which provide standards for indicia of compliance as to performance metrics. Specific references to QISs are already present in the individual provisions of § 1033.311 where necessary. Proposed § 1033.311(c)(1)(ii) is therefore duplicative in the appropriate instances, and overly broad as to all other unspecified performance metrics.

Additionally, we particularly reject the second component in § 1033.311(c)(1)(ii)(B), which would require all data providers to meet the performance specifications achieved by "similarly situated data providers." This is an unworkable standard in practice as data providers will not be held to the same universal standard. Even assuming there was some methodology to determine the cohort of "similarly situated data providers" and a further method to establish an average or median performance specification for this cohort, an average or median would, by definition, set a standard that approximately half of the cohort would not meet, essentially making compliance impossible to achieve for 50% of data providers during any regulatory examination. This is an inappropriate standard by which to judge the regulatory compliance of data providers. Baseline QISs must at least be universally achievable by all data providers and the CFPB should encourage a level playing field, rather than create differing, vague, and unworkable regulatory requirements.

ii) Access caps

We are generally supportive of proposed § 1033.311(c)(2) which articulates a "reasonability" standard for data provider restrictions on access frequency and would encourage additional clarity in the final rule that access caps are permitted if the request for covered data is unreasonable for the product or service offered (for example, repeatedly requesting the terms and conditions of an account multiple times a day). We do not believe reference to a QIS is necessary in this instance, as the proposed rule appropriately balances data providers' right to reasonably protect their systems with authorized third parties' ability to access the developer interface only as frequently as needed for the purpose authorized by the consumer.

However, like with response times, we recognize that many complicated factors should be taken into consideration when determining reasonable access restrictions. In the Australian example, traffic thresholds vary depending on whether the end user consumer has initiated the particular request ("customer present" transactions) and whether the call is made during high traffic periods.[93] It should be recognized in the rule that it is reasonable for data providers to give priority to "customer present" or directly customer-initiated requests, over automatic system-generated "robo calls." Further, § 1033.421(a) should specifically recognize that third parties also have an obligation to limit the frequency of requests for information to what is reasonably necessary to provide the consumer's requested product or service.[94] Excessive call requests can slow or even make developer interfaces unavailable, and third parties have no natural incentive to limit their requests unless the data provider is allowed to recover its costs for providing the developer interface. Allowing our recommended cost recovery for data providers will incentivize data providers to ensure that data is readily accessible.

[93] *See* https://consumerdatastandardsaustralia.github.io/standards/#traffic-thresholds.

[94] The proposed limitation in § 1033.421(a) on "collection" should be clarified, in an avoidance of confusion, to encompass both the "frequency of requests" and "scope of data."

iii) Security specifications

Proposed § 1033.311(d)(1) would impose a requirement on data providers to "not allow a third party to access the data provider's developer interface by using any credentials that a consumer uses to access the consumer interface." This provision should be amended to outright prohibit the use of screen scraping for all consumer data made available by a data provider's developer interface. We appreciate the recognition by the CFPB that consumer authentication credentials should never be shared with third parties. We suggest however that the rule should impose a concomitant requirement prohibiting all third parties from "collecting any consumer credentials for the data provider's consumer interface to access covered data." This simple consumer protection is so important and so simple that we suggest the CFPB create a new §1033.151 imposing this prohibition as to all third parties, regardless of whether they are an authorized third party or a defined data aggregator. Similarly, there should be a corresponding prohibition on third parties from seeking access to covered data from a data provider unless they are an authorized third party in accordance with § 1033.401.

Proposed § 1033.311(d)(2) would impose an information security program requirement to its developer interface. We believe this provision is redundant and unnecessary. Financial institutions are examined for compliance with the FFIEC information security handbook[95] and the applicable Gramm-Leach-Bliley Act rules and Federal Trade Commission Standards for Safeguarding Customer Information impose the applicable standards on developer interfaces by their own force.

d) Interface access (§ 1033.321)

The proposal states that a data provider would not violate its obligation to allow consumers and third parties access to an interface if it denied access based on risk management concerns. The proposal further provides that to be reasonable, a denial must, at a minimum, be directly related to a specific risk of which the data provider is aware, such as a failure of a third party to maintain adequate data security, and must be applied in a consistent and non-discriminatory manner.

The rule should explicitly provide data providers with a reasonable period of time to conduct due diligence on any third party or data aggregator seeking access to the third party's developer portal before determining whether to grant access. Where an authorized third party uses a data aggregator to seek access, data providers should be permitted to conduct due diligence on the third party, even in instances where the due diligence has previously been conducted on the data aggregator. Depending on the specific facts and circumstances, where concerns are identified, there may be instances where certain third parties are prohibited from accessing data through a given data aggregator while other third parties may access data through that same data aggregator.

The proposal states that indicia that a denial is reasonable include whether access is denied to adhere to a QIS related to data security or risk management. The proposal also provides that a data provider has a reasonable basis for denying access to a third party if:

- The third party does not present evidence that its data security practices are adequate to safeguard the covered data, provided that the denial of access is not otherwise unreasonable; or

[95] FFIEC Information Technology Examination Handbook Information Security (September 2016), ffiec_itbooklet_informationsecurity.pdf.

- The third party does not make the following information available in both human-readable and machine-readable formats, and readily identifiable to members of the public:
    - Its legal name and, if applicable, any assumed name it is using while doing business with the consumer;
    - A link to its website;
    - Its Legal Entity Identifier; and
    - Contact information a data provider can use to inquire about the third party's data security practices.

We appreciate the CFPB's recognition that data providers should have the right to deny access due to risk management concerns. Banks, which in many cases may be data providers under the proposed rule, are subject to robust and comprehensive risk management obligations to ensure that they maintain safe and sound operations, that their data remains secure, and that consumers are protected. The need to manage risk is of particular importance in the consumer-permissioned data sharing ecosystem given the sensitive nature of consumer data and the lack of regular, direct supervision of larger third parties and data aggregators and the current lack of a comprehensive liability framework to ensure that the entity responsible for harm that occurs is held liable. We recommend throughout this letter that the CFPB should directly supervise third parties and data aggregators to ensure that they meet various obligations to protect consumers and their data and the security of the overall ecosystem. This is especially true for larger entities, given the inherent risks and increased likelihood of being the target of attacks where a significant amount of data is stored. We reemphasize here and otherwise describe the need for a liability framework in section 5 of the comment letter, which is likely to expedite certain due diligence reviews.

While we appreciate the CFPB's recognition of the importance of data providers' ability to deny access when it has risk management concerns, the proposal construes a "reasonable basis" for denial too narrowly. The proposal states that a denial will only be reasonable if it is "directly related to a specific risk of which the data provider is aware." But data providers must anticipate and manage potential risks, not only those that are specifically identifiable and retroactively aware of, across all facets of their operations. Indeed, by the time a risk is specifically identifiable, it may be too late to appropriately manage or effectively contain it. Moreover, given the large number of third parties in the ecosystem, and with further growth expected, it would be virtually impossible for data providers to identify specific risks in all cases and to only deny access in those instances. Risk management requires assessments of the likelihood of various types of risks and managing the possibility of those risks coming to fruition. The recent interagency guidance on third party risk management takes into account these inherent complexities, noting "sound third-party risk management takes into account the level of risk, complexity, and size of the banking organization and the nature of the third-party relationship."[96] To require data providers to only deny access based on a specifically identified risk for each and every third party would not allow data providers to protect consumers' data or their own systems from third parties that may not appropriately manage their own risks.

In addition, the proposal appears to explicitly contemplate that a denial will only be reasonable if it is related to a data provider's concerns about data security. As noted, banks must manage all

[96] The Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC), Treasury, "Interagency Guidance on Third-Party Relationships: Risk Management" 88 Fed. Reg. 37920, (June 9, 2023), *available at* Federal Register :: Interagency Guidance on Third-Party Relationships: Risk Management.

manner of risks, not just those related to data security, and the risks of sharing consumer data with third parties extend beyond protecting the data, as described further herein. The final rule should be clear that other risk-based concerns are inherently reasonable.

The proposal also provides that one indicia of reasonableness is that access is denied in order to adhere to a QIS related to data security or risk management. These indicia of reasonable denial, particularly with respect to risk management generally, are also too limited. Banks manage their risks based on their unique business models and the types of third parties with whom they contract for various services, or, in this case, to whom they consider providing sensitive consumer data. Thus, it would be inappropriate for QISs to establish universal risk management obligations of data providers, as those standards are not amenable to being boiled down to universal terms and may be product or covered data field specific or depend on the nature of the third-party relationship with respect to that specific data provider. Moreover, such a universal standard could result in certain risks going unaddressed or under addressed, leaving the potential for risks to accrue in the ecosystem and ultimately harm financial institutions and consumers alike. If this were to happen, not only would there be significant financial consequences to all involved, but consumers could lose confidence in the data sharing market, or with their specific financial institution, raising reputational risks, even if the financial institution were not at fault. Finally, risks are constantly evolving, depending on the nature of the data provider's activities, the relationship the data provider has with various third parties and those third parties' activities and risk management practices. Some of these risks may be mitigated by bi-lateral contracts and thus the calculation of risk differs among authorized third parties even where a given risk may be potentially identified. Data providers therefore must be able to remain nimble to manage risks that emerge associated with sharing consumer data with various third parties.

Third party risk management obligations impose responsibilities on regulated financial institutions to implement policies and procedures to scrutinize third parties with which they engage, even in instances where that engagement is initiated through the third party. Within the data sharing ecosystem, there are a significant number of third parties and aggregators that may seek to access a data provider's interface to obtain consumer data. This information is highly sensitive, and its mishandling or unauthorized use could cause serious harm to consumers and to financial institutions. Therefore, data providers, and especially financial institutions, must have the ability to impose additional requirements on third parties to enable data providers to appropriately manage the risks of sharing consumer data with third parties, which is consistent with prudential regulatory expectations.

We discuss in section 5 of the comment letter that the rule should establish more explicit liability provisions to help protect data providers by ensuring that parties responsible for harm are held liable and to incentivize robust security and other risk management practices by third parties and data aggregators. However, even if a liability framework is established, the rule should explicitly provide that a data provider should have the ability to require authorized third parties and data aggregators to agree to certain obligations that align with a data provider's established risk-based policies and procedures before granting those entities access to the data provider's developer interface. A failure to agree to those requirements should serve as a reasonable basis to deny access.

The preamble briefly references liability in the ecosystem, stating in relevant part, that:

> Regulation E financial institutions—including digital wallet providers, entities that refer to themselves as neobanks, and traditional depository institutions—have and will continue to have error resolution obligations in the event of a data breach where stolen

> account or ACH credentials are used to initiate an unauthorized transfer from a consumer's account and the consumer provides proper notice . . . Various stakeholders have suggested that consumer-authorized data sharing may create risks to consumers and financial costs to financial institutions arising from an increased risk of unauthorized transactions and other errors, especially when data access relies on screen scraping. In implementing CFPA section 1033, the CFPB is proposing a variety of measures to mitigate unauthorized transfer and privacy risks to data providers and consumers, including allowing data providers to share TANs, not allowing data providers to rely on credential-based screen scraping to satisfy their obligations under CFPA section 1033, clarifying that data providers can engage in reasonable risk management activities, and implementing authorization procedures for third parties that would require they commit to data limitations and compliance with the Gramm-Leach-Bliley Act (GLBA) Safeguards Framework. These provisions are intended to drive market adoption of safer data sharing practices.[97]

We support these provisions intended to reduce risk in the ecosystem. However, these measures are not sufficient to substantially minimize or eliminate risks to the degree necessary under current third-party risk-based policies and procedures. For this reason, data providers must be able to reasonably deny access for a much broader range of risk management considerations, including a failure of a third party to agree to indemnification provisions, in considering whether to allow access to a specific third party because neither the shift to APIs, the application of Regulation E, nor network rules eliminate all the risks or costs. And as discussed earlier, these existing risk considerations go well beyond just data security evaluations. Even with the use of Tokenized Account Numbers in lieu of real deposit account numbers, there is still substantial risk to deposit account providers from being mandated to share data that can be used by third parties to initiate bank payments. While a tokenized account number can be helpful in containing the damage after a breach of account numbers has been definitively identified, it will not eliminate all forms of fraud or resulting losses or harm.

Also, Regulation E and private network rules do not provide for full reimbursement of data provider costs even in the event of credentials being compromised. In the event of fraud or disputes regarding a claim by the consumer against their financial institution under Regulation E, the consumer's financial institution can recover funds under certain circumstances within various networks. However, the data provider may still incur significant expenses in complying with Regulation E, including managing and investigating consumer claims of unauthorized transactions, loss of the use of capital pending resolution, and seeking reimbursement from other parties for those unauthorized transactions. And where the third party is not subject to private network rules, the costs associated with protracted litigation are also significant for all parties involved, further reducing market efficiency and consumer benefits.

Any final rule should be expanded to acknowledge that denials based on risk management considerations beyond those specifically identifiable, related to data security, or included in a QIS would be reasonable. The rule should clearly authorize data providers to require third parties to meet obligations reasonably designed to enable data providers to manage the risks associated with sharing consumer's data with third parties. These requirements could be imposed through bilateral contracts and reasonably designed to protect data providers without unnecessarily restricting the flow of

[97] 88 Fed. Reg. at 74801.

consumer-permissioned data. Alternatively, third parties could enter into collective agreements facilitated through a data aggregator. Requirements that data providers may impose could include those related to minimum risk management standards, accepting liability for unauthorized transfers or data breaches, indemnification for harm resulting from these incidents, obtaining insurance as a backstop to liability, reputational warrantees, and undergoing routine audits.

Requiring third parties to accept liability, indemnify data providers, and obtain insurance as a backstop will not only help ensure that liability is assigned parties responsible for the harm that occurs, but also would help ensure that third parties take their obligations, particularly those related to data security, seriously, given the risk of financial consequences. Without the risk of loss, third parties do not have a financial incentive to prioritize data security or protecting consumers or the overall security of the ecosystem, especially where the loss of compromised credentials only impact accounts held elsewhere. Thus, the refusal of third parties to agree to reasonable terms to help data providers manage their risks and help ensure the overall security of the ecosystem should serve as a reasonable basis on which the data provider may deny access.

While the ability to deny access based on reasonable risk management concerns is of critical importance, it is necessary, but not sufficient, to help ensure that consumers and their data are protected. There are certain market realities that may render a data provider's ability to require third parties or aggregators to agree to certain risk management-related terms very limited in practice. Smaller data providers may not have the ability to hold larger third parties or aggregators to requirements related to risk management, but rather, may be compelled by market forces to provide the information to third parties or aggregators that may not have appropriately robust data security or other risk management standards, which will leave consumers vulnerable to harm. This is yet another reason among many that the CFPB should subject third parties and data aggregators to direct supervision to ensure that they abide by the same data security standards and have greater incentives to proactively protect sensitive data.

Finally, any final rule should address potential conflicts between banks' obligations under the final rule and their legal obligations to operate in a safe and sound manner under other federal law. The rule should therefore include an explicit provision stating that nothing in the rule shall be interpreted as limiting a data provider's discretion to comply with existing prudential safety and soundness obligations, where relevant, or other applicable law. Where those expectations change, so should the applicable risk-based denial expectation. The rule should further provide that if any part of the rule or its application conflicts with a prudential requirement or obligation, the CFPB and the appropriate federal banking regulator(s) shall jointly determine how to resolve the conflict and the data provider shall be under no obligation to share any data with that entity until a resolution is reached.

e) Responding to requests for information (§ 1033.331)

i) Consumer interface

Authentication

Proposed § 1033.331(a) provides that a data provider must make covered data available upon receiving a request from a natural person consumer when it can sufficiently authenticate the consumer's identity and identify the scope of the data requested. We support this clear articulation of the plain language of the statute and agree that proper consumer authentication with the data provider is a

necessary precondition for data transmission. We agree with the preamble statement that these conditions would be satisfied through procedures in use by most consumer interfaces today that authenticate consumers and allow consumers to identify covered data for their retrieval.[98] We encourage the CFPB to recognize that consumer authentication measures such as one-time passcodes are now common security practices.

Consumers should be encouraged to use separate authentication credentials with all the entities with which they authenticate their identity. A consumer's authentication credentials with a data provider should be different than the credentials they might use to log into their account with an authorized third party. We believe this is consistent with proposed § 1033.311(d) and the preamble's language. Separate identity authentication credentials necessarily require that data providers and authorized third parties separately control their own authentication processes. Our recommendations regarding § 1033.311(d) above, calling for a new §1033.151 to prohibit third parties from collecting "any credentials that a consumer uses to access the consumer interface to access covered data," are consistent with this policy goal.

ii) Developer interface

Consumer identity authentication

Proposed § 1033.331(b) sets forth the preconditions necessary before data providers need to respond to requests for covered data by authorized third parties. However, it does not distinguish between an initial or new consumer data request by a third party to a data provider and all subsequent data requests by the third party to update the account data in scope. We suggest that § 1033.331(b) should recognize this distinction, and that the data provider needs more information in the event of a new data request and less in the event of subsequent requests.

For example, proposed § 1033.331(b)(1)(i) requires data provider receipt of information sufficient to authenticate the consumer's identity. We appreciate the recognition that proper consumer authentication is a necessary precondition for data transmission. The preamble recognizes that this is vital to mitigate potentially fraudulent data requests.[99] The preamble further states that, in the market today, before a data provider grants a third party access to covered data, the consumer is typically redirected to the data provider's interface to authenticate the consumer's identity, usually by providing account credentials.[100] This would generally constitute information sufficient to authenticate the consumer's identity for purposes of proposed § 1033.331(b)(1)(i). We agree with this conclusion.

However, this section of the preamble describes the events in the market which usually surround the establishment of a new consumer data sharing request with an authorized third party. Proposed § 1033.331(b) should be clarified to distinguish between the establishment of a new consumer data sharing request with an authorized third party and subsequent data requests by authorized third parties. The redirection of the consumer to the data provider's interface to authenticate the consumer's identity, is true as to the establishment of a new consumer data sharing request, but not always market practice for subsequent requests for information.

---

[98] 88 Fed. Reg. at 74822.

[99] 88 Fed. Reg. at 74823.

[100] *Id*.

Proposed § 1033.331(b) should recognize the right of data providers to directly authenticate consumers upon a new request to share covered data with an authorized third party, including the ability to require one-time passcodes. This right should be structured as a permissive "may" rather than a mandatory "must" or "shall" to allow for the possibility of evolving technologies in the future. The technology for passing consumers directly to the data provider for direct authentication exists today, is common in the market, and provides no unreasonable friction to consumer experiences. As the CFPB has recognized through proposed § 1033.311(d) and the preamble, consumer authentication credentials should never be shared with third parties as they present unreasonable security risks to consumers of fraud and consumer account takeover. Recognizing the data provider's right to directly authenticate consumers upon a new request for information would be consistent with the prohibition in proposed § 1033.311(d) against allowing consumer interface authentication credentials to be used to access the developer portal. Further, it would also be consistent with our recommendation that all third parties should be prohibited from collecting "any credentials that a consumer uses to access the consumer interface" in a new §1033.151.[101]

We appreciate that the CFPB recognizes this prudent practice in the market today as being compliant with its proposed framework, however, the rule should provide that direct consumer authentication is not necessarily required for subsequent data requests by authorized third parties. Once a consumer has properly authenticated their identity directly with a data provider, tokens are typically exchanged between the data provider and the authorized third party which are used for subsequent data calls by the authorized third party. These tokens are frequently used by data providers to identify the consumer account, covered data, and duration of the third party's authorization as applicable.

The use of these tokens makes it unnecessary for data providers to "receive information sufficient to… authenticate the consumer's identity" on subsequent requests. However, the proposal could be read to suggest that consumers should be redirected to the data provider's interface to authenticate the consumer's identity for every data call by an authorized third party. This would not be in keeping with current market practices and would be unduly burdensome for consumers, third parties, and data providers. These tokens also prevent the sharing of consumer interface authentication credentials directly with any third party and represent an industry standard security practice which the CFPB should recognize for subsequent authorized data requests in § 1033.331(b).

The consumer identity authentication process we describe above is analogous to the risk management framework described in the preamble for approving and then providing a third-party authentication token with regard to § 1033.331(b)(1)(ii), discussed further below. Just as the CFPB recognizes that an initial assessment of a new third party will be more extensive than subsequent information requests which rely on a properly issued third-party identity token, so too should the CFPB recognize that subsequent consumer data requests are permitted on the basis of tokens issued once the consumer has been redirected to the data provider's interface to authenticate the consumer's identity. Generally, characterizing the right of data providers to directly authenticate consumers upon a new request as a permissive right instead of a mandatory requirement could also help address the use of tokens for subsequent requests.

[101] *See* section (2)(c)(iii) of this letter.

Third party identity authentication

Under proposed § 1033.331(b)(1)(ii), the data provider would also need to receive information sufficient to authenticate the third party's identity before responding to a request. The preamble recognizes that a token issued by the data provider to a third party could be used to identify the third party and grant access to the data provider's developer interface.[102] It further states that the "CFPB expects that, prior to responding to data requests, most data providers would engage in some reasonable risk management diligence in accordance with proposed § 1033.321(a) as part of approving third parties to access a developer interface."[103] The preamble also acknowledges that data providers would not be required to make data available to third parties that present legitimate risk management concerns.[104] We agree, as we discuss further in section 2(d) of this Appendix.

Confirmation of a third party authorization

Proposed § 1033.331(b)(1)(iii) would require that a data provider receive information sufficient to confirm the third party has followed "the authorization procedures in [proposed] § 1033.401." It is not possible for a data provider to confirm the third party's authorization procedures, which require the provision of a § 1033.411 authorization disclosure, a statement certifying the third party agrees to the obligations of § 1033.421, and that the third party obtain a "consumer's express informed consent" per § 1033.401(c).

Data providers have no ability to control or monitor the conduct of third parties seeking consumer authorizations, nor can they be expected to do so. If a consumer is the victim of an unfair, deceptive, or abusive third-party authorization procedure—a possibility that the CFPB must recognize is both eventually probable and serious—a consumer might allege that the data provider was at fault for making their data available to the third party by virtue of an illegal third-party authorization. The manner and circumstances of <u>how</u> the third party acquired a consumer authorization would be entirely unknown to the data provider, even if the resultant third party authorization is transmitted in full to the data provider, as suggested by the preamble.[105]

Data providers should have no obligation to confirm the third-party's certification as to its § 1033.421 obligations. Further, whether the consumer's signed third-party authorization represents the "consumer's express informed consent" is a facts and circumstances determination, based on how the third party obtained a signed authorization. We propose that § 1033.331(b)(1)(iii) should simply describe "information sufficient to reasonably confirm the consumer's signed third-party authorization." In order to do this, a data provider could seek confirmation with the consumer directly, or institute other controls, such as an automated pre-approval process that consumers can predesignate. This approach would be consistent with the preamble statement that § 1033.331(b)(1)(iii) "would generally be satisfied where the data provider receives a copy of the authorization disclosure the third party provided to the consumer and that the consumer has signed."[106]

---

[102] 88 Fed. Reg. at 74823.

[103] *Id*.

[104] *Id*.

[105] *Id*.

[106] *Id*.

Proposed § 1033.331(b)(1)(iii) should also distinguish between an initial or new consumer data request and subsequent requests. "Information sufficient to confirm the consumer's signed third-party authorization" has utility during an initial or new consumer data request. It also should be provided in the event of a change to an existing third-party authorization or an extension of the duration of an existing third-party authorization. Subsequent data calls relying on existing, unchanged authorization do not need a signed copy of the consumer's third-party authorization and can be executed on the basis of tokens issued in response to an initial or new consumer data request. However, if the data provider has reason to believe there were material changes made by the authorized third party to the product or service or subsequently becomes aware of risks posed by the authorized third party, the data provider should be permitted to conduct appropriate due diligence on the changed (or suspected changed) circumstances prior to making data subsequently available.

Third parties often request updates to the same consumer account multiple times per day, totaling up to 100 billion requests in 2022 alone according to the preamble.[107] Requiring a signed copy of the authorization disclosure, or its equivalent, to be transmitted with every data call would represent a wasteful regulatory obligation on third parties and data providers, in terms of the efficient design of a data sharing network, the bandwidth required to transmit this information, and the computing power and electricity required to send, receive, and process this file upon every data call. This requirement would not be in keeping with current market practices. The rule should recognize this distinction between the information necessary for an initial or new request and subsequent requests as to § 1033.331(b)(1)(iii), as in other areas of § 1033.311(b).

Data provider and third party authorizations

We draw a meaningful distinction between identity authentication and a data sharing authorization. The rule should recognize that consumers give separate authorizations to the data provider and the authorized third party. An authorization represents the instructions and permissions granted by the consumer to the data provider and the authorized third party, independently. Authorizations are like "mini contracts," granting the parties permission to act in accordance with the consumer's instructions. The proposal does not currently sufficiently recognize that consumers should provide an authorization to their data provider in addition to third parties.

In § 1033.331(a), this distinction makes little difference. Once a consumer's identity has been properly authenticated and the scope of relevant data has been defined, the authorization instructions for a consumer interface request are complete. The consumer's instruction is to deliver the requested data directly to the consumer. The consumer is then free to use the data in their possession as he or she deems appropriate.

The facts are more complicated, however, when a consumer is instructing a data provider to make data available to a third party. In this case, a consumer's authorization to a data provider represents the consumer's permission to share their data and instructions regarding what data to transmit to a particular authorized third party. The consumer's authorization to a third party is different; it includes the consumer's instructions and permission to the third party to collect, retain, and use the consumer's specified data in a particular manner. These are two separate sets of instructions and

[107] 88 Fed. Reg. at 74844.

permissions between the consumer and two different parties, the data provider and the authorized third-party.

Proposed § 1033.331(b)(2) attempts to recognize the importance of a consumer's data provider authorization in practice by allowing a data provider to "confirm the scope of a third party's authorization," including the accounts to which the third party is seeking to access in § 1033.331(b)(2)(i) and the categories of covered data that the third party is requesting to access in § 1033.331(b)(2)(ii). We are concerned that this "confirmation" construction does not fully represent the consumer's data provider authorization and does not sufficiently protect data providers from subsequent allegations of impermissible consumer data sharing.

In the event of a new consumer data sharing request, the rule should recognize that the data provider is permitted to receive its own consumer authorization to make available some or all of the consumer's data to a designated third party according to the consumer's express informed consent. The manner and circumstances of the data provider authorization would be within the data provider's control, providing consumers additional protection from unfair, deceptive, or abusive third-party authorization procedures. Data providers would also take significant legal comfort from the fact that they are then transmitting the consumer's data in accordance with a legal, and properly obtained, data provider authorization. Similarly, data providers should be permitted to receive its own consumer authorization in the event of a change to an existing third-party authorization or an extension of the duration of an existing third-party authorization. Data providers should also be permitted to confirm an existing authorization in response to unusual, anomalous, or fraudulent account activity, or based on other reasonable risk management concerns.

Subsequent data requests by authorized third parties relying on an existing, unchanged authorization do not require an additional data provider authorization. Similar to the consumer and third-party identity authentication discussion above, once a consumer has properly authorized a data provider, tokens are typically exchanged between the data provider and the authorized third party which are used for subsequent data calls by the authorized third party.

We believe that recognizing the data provider's right to receive its own authorization and distinguishing between an initial or new request and subsequent requests is appropriate and narrowly tailored to provide consumer protection and align with existing regulatory expectations. Proposed § 1033.331(b)(2) does not currently distinguish between these types of requests and could be read to permit a data provider to "confirm" a third-party authorization for all subsequent data requests. This would not be in keeping with current market practices and would be unduly burdensome for consumers, third parties, and data providers. Our proposal to permit the data provider to receive its own consumer authorization only as part of a new data request strikes the appropriate balance between enhancing consumer protection and reducing the burden on all parties over the life of the permissioned data sharing.

Receipt of a data provider authorization from the consumer in response to a new request would also address the statements in the preamble regarding the benefits of the confirmation step of § 1033.331(b)(2). It would allow the data provider to present the consumer's accounts to the consumer during the initial authorization and identify the data that the data provider would be authorized to share,

giving consumers and data providers greater certainty about what data will be made available.[108] Subsequent requests by authorized third parties could call for only a subset of the authorized information, such as "current account balance," in accordance with what is reasonably necessary at the time.

If the CFPB does not expressly permit data providers to receive their own authorization from the consumer in the rule, and if the rule instead requires data providers to comply with a third party's request regarding accounts and scope of covered data, the rule should expressly absolve data providers from all liability for making such information available according to an authorized third party's request, including a shield from liability in the event of a data breach at the authorized third party or fraudulent payments. Data providers cannot be exposed to any liabilities (uncapped or otherwise) by operation of a regulation which also prevents data providers from taking reasonable steps to mitigate these risks, nor incorporate these clear risks into the economic structure of the specific product or service. Such a liability shift, though, would still not necessarily address the safety and soundness and reputational risks that arise from constraining data providers from collecting authorizations directly.

Response not required

Proposed § 1033.331(c) states specific circumstances when a data provider would not be obligated to make covered information available in response to an authorized third-party request. We appreciate the cross references in § 1033.331(c)(1) and § 1033.331(c)(2) to the provisions of § 1033.221 and § 1033.321(a). We also support the proposal's recognition that a response is not required if the developer interface is not available, in § 1033.331(c)(3). And we agree with the provisions of proposed § 1033.331(c)(4) that a data provider need not make covered data available if a consumer's authorization is no longer valid, through a revocation at either the data provider or authorized third party or because the original authorization has expired consistent with § 1033.421(b)(2).

In an abundance of caution, the final rule should also provide explicitly that data providers have no obligation to make covered data available to third parties that are not "authorized third parties" as defined in accordance with § 1033.401. Correspondingly, the final rule should also contain an explicit provision to prohibit third parties from seeking access to covered data from a data provider unless they are an "authorized third party." While we think this is obviously implied by § 1033.331(b), § 1033.331(c)(4)'s various requirements for an unexpired authorization, and the rule's foundational reliance on a consumer's authorizations and a consumer's express informed consent, a clear statement as such would avoid confusion. Such a provision would be consistent with our recommendations regarding § 1033.331(b)(iii) (requiring "information sufficient to confirm the consumer's signed third-party authorization) and § 1033.331(c)(4) (revocation by consumer or expiry of duration period). Consistent with these recommendations, § 1033.331(c) should contain a new subsection stating that a data provider is not requires to make covered data available in response to a request when "the third party is not an authorized third party."

Jointly held accounts

Proposed § 1033.331(d) would require a data provider that receives a request for covered data from a consumer that jointly holds an account, or from an authorized third party acting on behalf of such

[108] *Id*.

a consumer, to provide covered data to that consumer or authorized third party. The rule should clarify the data provider's obligations in the event of a subsequent revocation by one of the joint account owners, we suggest that data providers should be permitted to consider such a revocation valid, whether the revocation is given to the data provider or the authorized third party. The rule should also clarify that a consumer who is not a joint account holder or owner is not able to authorize the sharing of covered data of an account to third parties through the developer interface. Depositories have differing arrangements allowing additional persons to use or access an account which are less than full ownership of or liability regarding an account.

Similarly, the CFPB should clarify both the authorization rules and revocation rules for trusts, as we discuss above regarding the proposed definition of "consumer" in § 10333.131. In general, accounts held pursuant to a bona fide trust agreement are not considered Regulation E accounts and should be considered outside of the scope of this rule.[109] Further, fiduciary accounts involving trusts and estates often involve multiple beneficial interests. There is a risk that aggregating data from trust accounts could give an incorrect impression of entitlement to certain assets as to a single beneficiary. Additionally, banks have a duty to maintain the confidentiality of beneficiary data and records, not only from third parties, but also from other beneficiaries of the account. For all of these reasons, trust accounts, particularly those with multiple beneficiaries, are not well suited to coverage by the rule and should be explicitly excluded.

Data provider authorization revocation method

Proposed § 1033.331(e) permits data providers to provide consumers with a "reasonable method to revoke any third party's authorization to access all of the consumer's covered data." We appreciate the improvement that § 1033.331(e) represents over the approach of the SBREFA outline. Consumers may not remember the entities with which they have previously authorized sharing of their data, their login credentials to all those entities, or even know whether an intermediary such as a data aggregator was involved. Data providers should be allowed to enable customers to manage all their permissions via the data provider's consumer interface and provide notice to consumers where there are changes to those pre-existing relationships.

However, citing stakeholder concerns about anticompetitive activities, the preamble states that a consumer would not be permitted to revoke an authorization as to one of multiple authorized accounts or one of multiple categories of authorized covered data. In contrast, proposed § 1033.421(h)(1) would allow the consumer to revoke an "authorization to data access for purposes of one product or service but maintain that same third party's data access for purposes of another product or service" if the revocation is provided to the third party. The preamble states that an "all or nothing" revocation mechanism at the third party would effectively constitute a prohibited "cost or penalty on the consumer."[110] We agree with the CFPB's rationale as to § 1033.421(h)(1) and believe that it is similarly applicable to § 1033.331(e). Requiring that a data provider's revocation method must be an "all or nothing" revocation would similarly be "a cost or penalty on the consumer" and frustrate consumer control over their data. Requiring third parties to offer a service which would grant consumers superior control over their data, while prohibiting data providers from offering an equivalent service would unfairly hinder the adoption of data provider revocation methods and unjustly penalize consumers who

[109] *See* 12 C.F.R. § 1005.2(b)(2); Official Interpretation of Paragraph 2(b)(2)-1.

[110] 88 Fed. Reg. at 74840.

revoke at their data provider. Similarly, the proposal would provide inconsistent requirements and may lead to consumer confusion or frustration as to why the consumer cannot make certain elections through their data provider. The proposal should seek to maximize consumers' ability to control access to and use of their data, not restrict or limit the consumer's ability to control their data.

Comments to the CFPB regarding anticompetitive concerns are unfounded and disingenuous. The consumer is the one that initiates a revocation—which represents the withdrawal of the consumer's informed consent—whether it is at the data provider or the third party. Further, the proposal already provides that the revocation method at the data provider must be reasonable and "be unlikely to interfere with, prevent, or materially discourage consumers' access to or use of the data, including access to and use of the data by an authorized third party." These provisions of the proposal are more than sufficient to ensure consumers are not unduly influenced to revoke an authorization.

The preamble states that "consumers who partially revoke access to their data could unintentionally disrupt the utility of data access for certain use cases." We suggest that such a revocation might not be "unintentional" but may be entirely intentional and represent the express informed decision of the consumer. The preamble gives consumers too little credit in this regard. It further states that an account-by-account "revocation method would be inconsistent with proposed § 1033.201(a), which would require data providers to make covered data available upon request based on the terms of the consumer's authorization." Every revocation represents a consumer making a later in time decision to modify a prior authorization, whether they give their revocation to the data provider or the third party, , and the consumer's decision should be given equal consideration, regardless of where they indicate that decision. We disagree that this is any basis upon which to restrict the consumer's ability to revoke their authorization for a third party to access, store, or use their data on an account-by-account basis, whether they give their revocation to the data provider or the third party.

We reiterate our prior comments addressing standard setting bodies and QISs in §§ 1033.131 and 1033.141, that a QIS as to reasonable revocation methods would be inappropriate and could conflict with a federally supervised entity's regulatory obligations.

f) Information about the data provider (§ 1033.341)

Proposed § 1033.341(a) would require data providers to make certain information readily identifiable to the public, which the rule specifies means that "the information must be at least as available as it would be on a public website," and the information must be available "in both human-readable and machine-readable formats." Subsections (b) through (d) specify the information that data providers must make available in these formats.

First, providing the required information about the data provider on a public website should be sufficient to meet this requirement. As we noted with respect to proposed § 1033.301(b), which requires that covered data must be available in "machine-readable file" to both consumers and authorized third parties, upon specific request, example 1 in that section states that such requirement would be satisfied "if the data can be printed or kept in a separate information system that is in the control of the consumer or authorized third party." We therefore believe the intent of that provision is to ensure that data providers make data available in a format that consumers can print or keep. Web-based consumer interfaces today allow consumers to print the information displayed on paper or to retain as a computer file when a consumer instructs a web browser save the page as either a webpage as an HTML file or a PDF. These formats can be retained, are machine-readable, can be printed, and

display information in a format that is designed for a human reader. Therefore, the requirements of this section that certain data provider information be readily identifiable to the public would be met if the required information listed in 1033.341(b) is made available on the data provider's website in a format that can be printed or retained as a computer file.

In addition, this requirement seems redundant with the below requirement regarding "identifying information," which requires data providers to disclose links to their websites if the information was already provided on the website itself.

i) Identifying information (§ 1033.341(b))

The proposal would require a data provider to disclose:

> (1) Its legal name and, if applicable, any assumed name it is using while doing business with the consumer;
> (2) A link to its website;
> (3) Its LEI; and
> (4) Contact information that enables a consumer or third party to receive answers to questions about accessing covered data under this part.

As noted above, providing this information on the data provider's website should meet the requirements for this section.

ii) Developer interface documentation (§ 1033.341(c))

The proposal would require a data provider to disclose documentation, including metadata describing all covered data and their corresponding data fields, and other documentation sufficient for a third party to access and use the interface, that must be at least as available as it would be on a public website. The proposed rule further states that the documentation must:

> (1) Be maintained and updated as the developer interface is updated;
> (2) Include how third parties can get technical support and report issues with the interface; and
> (3) Be easy to understand and use, similar to data providers' documentation for other commercially available products.

We recommend that the proposed rule text be amended to provide that data providers should make available "documentation that informs the third party how to access and use the interface," rather than information that would itself enable the third party to use the developer interface. It would not be appropriate for a public website to contain enough information that a third party could use to access and use the interface, as disclosure of that information raises significant safety and soundness risks given the availability of sensitive consumer information. Additionally, data providers must be able to conduct reasonable due diligence on third parties for risk management purposes *before* those third parties are provided access to the interface. Providing third parties with information that would allow them to access the interface before a data provider may have conducted due diligence on the third party would undermine data provider's risk management obligations and could result in harm to the data provider or consumers. Moreover, the proposed requirement could be construed as requiring data providers to disclose information that should remain confidential for security or other reasons, such as, for example, private API keys.

Proposed § 1033.341(c)(1) would require that developer interface documentation "be maintained and updated as the developer interface is updated." This requirement could be very difficult and resource-intensive for data providers to implement in practice. While some of the largest data providers already comply with some of the developer interface documentation requirements in the proposal, the CFPB should be mindful that these obligations are likely to be costly and onerous to implement, particularly for smaller data providers. Developing a public "developer interface" in and of itself requires significant investment, and it would be overly burdensome and onerous for data providers to have to keep the interface documentation completely up to date regarding changes that may be made to the API. This could require nearly constant updating. A more achievable alternative would be to require data providers to make available developer interface documentation in a timely manner that enables connectivity as required by any final rule and to update the interface documentation within a reasonable time period after a change is made to the developer interface.

iii) Performance specification (§ 1033.341(d))

Proposed § 1033.341(d) would require data providers to disclose on or before the tenth calendar day of each calendar month the quantitative minimum performance specification that the rule would require in § 1033.311(c)(1)(i) that the data provider's developer interface achieved in the previous calendar month. The disclosure would be required to include at least a rolling 13 months of the required monthly figure. The data provider would be required to disclose the performance specification as a percentage rounded to four decimal places, such as "99.9999 percent."

The proposed regulatory standard in § 1033.311(c)(1)(i) provides that the "number of proper responses by the interface divided by the total number of queries for covered data to the interface must be equal to or greater than 99.5%." As we described previously, this proposed performance specification is unreasonably high and fails to consider the performance of the requestor in formatting and articulating a request. Therefore, we recommend that the CFPB should replace the "quantitative minimum specification" with the "commercially reasonable" standard already articulated in § 1033.311(c)(1) of the proposal. We also do not support the assertion in the preamble that, to the extent that the rule retains any quantitative minimum specifications, a concurrent QIS could become a new higher requirement to meet a "commercially reasonable" standard.

However, if the CFPB proceeds with implementing a required quantitative minimum performance specification for developer interfaces, the final rule should adopt the more widely used and accepted metric that measures the percentage of developer interface uptime relative to unscheduled downtime. Based on the experience of other jurisdictions, we believe that a 95% uptime requirement for developer interfaces would achieve the goals of the CFPB that developer interfaces are almost always available. Our specific recommendations regarding the proposed requirements that would apply to developer interfaces are laid out in greater detail in section 3(c) of this Appendix.

Regarding the specific requirements of 1033.341(d), we recommend that the CFPB require publication on a quarterly basis, rather than monthly, to account for the fact that data providers may have certain key staff responsible for compiling these statistics that may have other assignments or take personal time off in any given month that would make it more difficult for the institution to meet the monthly requirement. Quarterly reporting, which is the required reporting cadence in other jurisdictions, such as the UK, also provides a greater volume of data, which generally will better reflect overall trends rather than potentially give undue weight to unanticipated one-off events. Finally,

rounding to no less than two but no more than four decimal places provides a more easily understood and flexible reporting structure and aligns with the CFPB's requirements in the Remittance Rule related to the presentation of exchange rates.[111]

In addition, data providers should have more time before they are required to publish developer portal performance statistics on a public website after the requisite publication deadline. For example, 45 calendar days beyond the end of the elapsed calendar month (or quarter, if the rule is amended as we recommend), would be more appropriate for the following three reasons:

(1) In some instances, it may take internal databases over a week to populate underlying data needed for the proposed reporting.
(2) Once automated reports are generated, some data providers may need time to perform manual work to create the specific reporting statistics that meet the CFPB's definition of a "proper response" if that requirement is included in the final rule, or other reporting metrics that the CFPB may require, including by combining data from multiple sources.
(3) Whatever metrics are ultimately required to be reported may have to be reviewed and approved by multiple parties at the data providers to ensure accuracy before being reported externally (e.g., to investigate potential reporting anomalies that can arise due to problems involving error codes, temporary reporting database failures, or other issues that have to be addressed).

Publishing the data on a 45-day lagging basis is a more realistic timeframe to allow data providers to ensure that data is collected and reported accurately and does not materially degrade the benefit of holding data providers accountable for being transparent about their interfaces, compared with 10 days. At a minimum, the 10 days should be extended to 10 business days to ensure a consistent reporting schedule; a requirement of 10 days could result in a varying reporting schedule and could in reality give data providers even less time to publish, depending on how many weekends and/or holidays may occur at the beginning of any given month. There is no inherent reason to rush reporting at the risk of publishing accurate data. There may be a greater risk of misreporting metrics if data providers do not have sufficient time to ensure the data's accuracy.

Additionally, we encourage the CFPB to provide flexibility in how developer interface performance statistics are made publicly visible. The proposal would require that each data provider make such information *readily identifiable to members of the public*. In the future it may be efficient for an industry body to collect and publish this information in a single place for multiple data providers, rather than for each data provider to publish this data separately (e.g., on their own disparate websites). It may be more cost-effective for the industry, more useful for interested parties, and more consumer-friendly if an industry body were to publish the data from multiple data providers. The CFPB should clarify that, if such an industry solution were to be built, making performance statistics available in this way would satisfy the requirements in the rule to make such data readily identifiable to the public.

[111] 12 CFR 1005.31(b)(1)(iv).

g) Data provider policies and procedures (§ 1033.351)

Proposed § 1033.351(a) would set forth the general obligation that data providers establish and maintain written policies and procedures that are reasonably designed to achieve the objectives set forth in proposed subparts B and C, including proposed § 1033.351(b) through (d). It also states that these must be appropriate to the size, nature, and complexity of the data provider's activities. Federally supervised and examined financial institutions are already under extensive requirements as to the sufficiency of their various policies and procedures, and these must necessarily be tailored to the risk and complexity of each organization.

Proposed § 1033.351(a) would require financial institutions to create, maintain, and keep extensive new amounts of information and records and would be inconsistent with the plain statutory language of section 1033(c) which specifically prohibits interpretations of section 1033 which may "impose any duty on a covered person to maintain or keep any information about a consumer."[112] The preamble protests that § 1033.351 does not require a covered person "to maintain or keep additional information *on a consumer* and is silent as to record retention relating to compliance with CFPA section 1033 itself" (emphasis added).[113] We disagree.

The very title of the subsection 1033(c) is "NO DUTY TO MAINTAIN RECORDS."[114] This is an information production statute; it contains no recordkeeping requirements and specifically prohibits implementing regulations which purport to do so.

It is an unjustified and overly narrow reading of this provision to argue that the extensive new records and information which it requires data providers to maintain and keep are not "about a consumer." Data providers are only covered by this proposal by virtue of the covered consumer financial product or service they offer to individual consumers. Further, the express exception in section 1033(b)(4) which excludes "any information that the covered person cannot retrieve in the ordinary course of its business" supports our plain reading of the statute that section 1033 may not require data providers to create, maintain, or keep new information by virtue of its implementing regulations alone.

Congress flatly rejected imposing new recordkeeping obligations on data providers and instead imposed a straightforward obligation on these institutions to make the information that they already keep in the normal course of their business available to consumers in an electronic form. Citations to the CFPB's general authority under CFPA section 1022(b)(1) to prevent evasion and carry out the purposes of section 1033 are insufficient to overrule the clear prohibitions on information collection and retention explicitly provided regarding personal financial data rights in subsections 1033(b)(4) and (c). It is a well-recognized principle of statutory interpretation that, if statues are in conflict, the more specific statute (here one which imposes specific limitations of agency authority) must prevail over the general statute (here the general authority of the CFPB to write rules to give effect to other statutes and prevent evasions thereof).

The preamble presents no evidence that data providers have attempted to evade the requirements of section 1033. To the contrary, data providers have facilitated up to 100 billion consumer

[112] 12 USC 5533(c).

[113] 88 Fed. Reg. at 74829.

[114] 12 USC 5533(c).

data access requests in 2022 according the CFPB's own estimates. Not only is evasion not a problem, but the proposed solution is in no way appropriately calibrated between its costs and potential benefits. Rule provisions to "discourage evasion"[115] or make potential evasion "more difficult"[116] must still be calibrated to an extant problem to avoid being seen as an arbitrary and capricious abuse of regulatory authority. Proposed § 1033.351 is not reasonably calibrated. We describe below further reasons why the proposed specific recordkeeping requirements below, in addition to being ultra vires, are unnecessary, inappropriate, and overly burdensome.

i) Available data

Proposed § 1033.351(b)(1) would specifically require the data provider to have policies and procedures reasonably designed to create a "record of the data fields that are covered data in the data provider's control or possession" and "record what covered data are not made available through a consumer or developer interface pursuant to an exception in § 1033.221, and the reason(s) the exception applies." While well intentioned, this provision vastly underestimates the burden it would place on data providers and should be removed. New types of information are constantly being created and deleted regarding consumers, their accounts, and their transactions. Requiring the creation and maintenance of a database which catalogues all of these attributes against those which might be covered data and those which might be eligible for an exception would result in a new and monumental compliance cost for every data provider and result in no benefit to consumers.

The preamble observes that this database "could help the CFPB identify compliance gaps in what the data provider makes available, streamline negotiations between data providers and third parties by establishing the available data fields, and encourage the market to adopt more consistent data sharing practices." Further, it states that documentation of the "use of the exceptions can help identify noncompliant use of the statutory exceptions." Respectfully, federally supervised, examined, and regulated data providers already have extensive obligations to comply with supervisory requests for information from the CFPB and other enforcement agencies, and the proposal cites to no evidence of a current deficiency in the agency's current authorities to request information related to the current data fields and those made available. Neither the statutory text nor the Congressional intent of section 1033 calls for data providers to create and constantly maintain such a record specific to the requirements under a 1033 rulemaking.

Further, this record would not and should not be made public as it represents confidential commercial information about how data providers serve their customers and the proprietary data fields they may use to do so. We appreciate that the proposed regulatory text refrains from calling for public disclosure of the proposed § 1033.351(b)(1) record. As such, we can see no way in which it would "streamline negotiations between data providers and third parties by establishing the available data fields." Additionally, even if it were to streamline negotiations, which it does not, there is no statute which establishes "streamlining the negotiations" of private commercial actors as an appropriate mission of the CFPB (much less the purpose of section 1033) or which grants the CFPB the authority to write regulations to effectuate this.

[115] 88 Fed. Reg. at 74829.

[116] *Id*.

Lastly, the recognition of a QIS as to a standardized format, issued by a CFPB-recognized standard setting body, will itself "encourage the market to adopt more consistent data sharing practices." We appreciate that the preamble believes that "allowing a data provider to cite data fields defined by a qualified industry standard … could ease the compliance burden on data providers and promote market standardization." [preamble page 121] However, any compliance reduction would be completely undone by the last sentence of § 1033.351(b)(1), which states that "exclusive reliance on data fields defined by a qualified industry standard would not be appropriate if such data fields failed to identify all the covered data in the data provider's control or possession." Every data provider would have to customize their § 1033.351(b)(1) record on this basis. QISs as to data format are necessarily limited to only those data fields which are appropriate for data sharing. Every institution maintains additional data fields which are inappropriate to share regarding a customer, their account, and their transactions. This provision would do nothing to encourage consistent data sharing practices beyond what a QIS would itself do and would only increase the burden on data providers without any associated consumer benefit.

ii) Denials of access to a developer interface and denials of information requests

Proposed § 1033.351(b)(2) would require a data provider to have policies and procedures reasonably designed to create a record explaining the basis for denying a third party access to its developer interface pursuant to § 1033.321 and communicate to the third party as quickly as is practicable the reason or reasons for the denial.

Proposed § 1033.351(b)(3) would similarly require a data provider to have policies and procedures reasonably designed to create a record explaining its basis for any decision to deny a request for information pursuant to § 1033.331 and communicate to the consumer or authorized third party the type(s) of information denied and the basis for the denial. This too would have to be communicated as quickly as is practicable. Proposed §1033.331(b)(3)(ii) should be clarified to state that the data provider should communicate to the consumer, in the case of a consumer request through the consumer interface, or to the third party, in the case of a third party request through the developer interface. We believe this is the intention of proposed §1033.331(b)(3)(ii) which states "consumer or third party."

A simultaneous requirement to contact the consumer and the third party would be excessively burdensome to the consumer—and may be impossible for the data provider—in the event that the request does not allow for the identification of the consumer, does not authenticate the third party, lacks information sufficient to confirm a consumer's signed third-party authorization, or the denial is based on a malformed data request. If a data provider does not receive the information specified in § 1033.331(b) or is not required to respond to a request under § 1033.331(c), the third party requestor is in the best position to rectify the request, which may be the result of a system error at the third party.

We address elsewhere in this letter the proposal's permissible bases for a denial of access to a developer interface and a denial of an information request.[117] We appreciate the language in the preamble that the proposed rule attempts to give data providers flexibility to design policies and procedures to reasonably account for the limited cases in which the disclosure of the specific reason for a denial might present additional risk management concerns.[118]

[117] *See* section (2)(d) and section (2)(e)(ii), respectively.

[118] 88 Fed. Reg. at 74827.

iii) Accurate data transmission

Proposed § 1033.351(c) would require data providers to establish and maintain policies and procedures reasonably designed to ensure that "covered data are accurately made available through the data provider's developer interface." The preamble clarifies that this provision refers to "the accuracy of transmission rather than the underlying accuracy of the information in the data provider's systems. That is, the policies and procedures should be designed to ensure that the covered data that a data provider makes available through its developer interface matches the information that it possesses in its systems."[119] We appreciate the CFPB's recognition that the statute generally requires covered data providers to make available information in their control or possession concerning the consumer financial product or service that the consumer obtained from the data provider. The statute does not reference data accuracy. In fact, subsections 1033(b)(4) and (c) display Congress's intent to expressly cabin the scope of section 1033 to information already kept in the ordinary course of business.[120] By contrast, for example, the Fair Credit Reporting Act and Regulation V impose accuracy requirements on the information furnished to and provided by consumer reporting agencies. Congress could have included data accuracy responsibilities for data providers but did not do so.

We also agree that the information stored in data providers' existing systems is already subject to several legal requirements regarding accuracy. As the preamble states, "Regulation E protects consumers against errors, and Regulation Z protects consumers against billing errors. In addition, the Interagency Guidelines Establishing Standards for Safety and Soundness require operational and managerial standards for information systems."[121] Therefore the rights provided through existing regulation are the appropriate means for addressing any potential errors associated with a consumer's data.

As stated above where we address the role of a standard setting body, we do not support proposed § 1033.351(c)(3), which would grant a QIS indicia of compliance as to the reasonableness of the policies and procedures of a data provider required by § 1033.351(c). Federally supervised and examined entities are already under extensive requirements as to the sufficiency of their various policies and procedures, and these must necessarily be tailored to the risk and complexity of each organization and regularly reviewed and updated, as appropriate. Financial institution policies and procedures take into account overlapping regulatory obligations regarding their operation and must be tailored to be consistent with the firm-wide approach to policy and procedure administration and management. We are concerned that generic standards regarding policies and procedures, even when they only confer indicia of compliance, issued by an industry-wide standard setting organization will reduce compliance effectiveness overall and potentially conflict with the prudential expectations specific to a financial institution.

Industry standard setting organizations are simply not well positioned to weigh in on the adequacy of policies and procedures, and generally have not done so to date. Insofar as this provision attempts to address a standard for data transmission fidelity, or acceptable error rates for these transmissions, we believe that this is already addressed by proposed § 1033.311(b) which incentivizes

[119] 88 Fed. Reg. at 74828.

[120] 12 USC 5533(b)(4) and (c).

[121] 88 Fed. Reg. at 74828 (citations omitted).

accurate data mapping to a QIS as to a standardized format and § 1033.311(c) which requires that a developer interface must meet commercially reasonable performance specifications.

v) Policies and procedures for record retention

Proposed § 1033.351(d) would require that data providers establish and maintain policies and procedures reasonably designed to ensure retention of records that are "evidence of compliance" with a data provider's obligations. These would "ensure the CFPB and other enforcers can verify compliance with the proposed rule" according to the preamble.[122] We repeat our position that CFPA section 1022(b)(1) does not trump the explicit prohibitions found in subsections 1033(b)(4) and (c), which display Congress's intent to expressly cabin the scope of section 1033 to information already kept in the ordinary course of business.[123] Respectfully, federally supervised, examined, and regulated data providers already have extensive obligations to comply with supervisory requests for information. Neither the statutory text nor the Congressional intent of section 1033 calls for data providers to create and constantly maintain such additional records specific to the requirements under the final rule.

Proposed § 1033.351(d)(1) would specifically require the creation and retention of records "related to a data provider's response to a consumer's or third party's request for information or a third party's request to access a developer interface" and these "must be retained for at least three years after a data provider has responded to the request." Proposed § 1033.351(d)(2) further specifies that these records must include "without limitation:

> (i) Records of requests for a third party's access to an interface, actions taken in response to such requests, and reasons for denying access, if applicable;
> (ii) Records of requests for information, actions taken in response to such requests, and reasons for not making the information available, if applicable;
> (iii) Copies of a third party's authorization to access data on behalf of a consumer; and
> (iv) Records of actions taken by a consumer and a data provider to revoke a third party's access pursuant to any revocation mechanism made available by a data provider.

In addition to these proposed requirements being beyond the CFPB's authority to impose, we further observe that, as drafted, they are unnecessarily broad and burdensome. Records of every request for information, regardless of whether it is an initial or new request or a subsequent request, would have to be maintained, including potentially records of all the data transmitted in response to a request and a copy of the third party authorization transmitted with every request, as currently required by proposed § 1033.331(b)(iii).

The data storage demands of this requirement, based on CFPB's own estimate of up to 100 billion access requests in 2022, would be astronomical, not to mention the concomitant costs to data providers of maintaining these records. Should the CFPB proceed with implementing this requirement, despite it being beyond its authority to do so, the CFPB should undertake a detailed cost analysis of this provision and publish it for public inspection. It is unreasonable and not useful to require this information to be retained for every data request. Additionally, data providers and authorized third parties are already incentivized to retain a single copy of an authorization request, whether it is the third

[122] 88 Fed. Reg. at 74828.

[123] 12 USC 5533(b)(4) and (c).

party's authorization or the data provider authorization we recommend, as a legal defense to allegations of unauthorized access. Similar incentives exist as to consumer revocations provided to data providers. These provisions are not necessary or appropriate.

3) Authorized Third Parties

a) Third party authorization procedures (§ 1033.401)

The CFPB's proposed rule includes authorization procedures for third parties seeking to access covered data on consumers' behalf. The proposed authorization procedures "include requirements to provide an authorization disclosure to inform the consumer of key terms of access, certify to the consumer that the third party will abide by certain obligations regarding the consumer's data, and obtain the consumer's express informed consent to the key terms of access contained in the authorization disclosure." As discussed in section 2(e)(ii)(4) of this Appendix, while third parties may obtain authorization from consumers to access, use, and retain a consumer's data for a specific purpose, data providers should have the right to obtain authorization from the consumer regarding the scope of data the consumer wishes to share and with what third party.

We note that the rule does not address third party obligations when material terms in the original authorization change. For example, if the third party changes certain aspects of the originally desired product, determines it needs additional or different data from what was originally contemplated as being "reasonably necessary," changes vendors that help it provide the product, or the aggregator it uses changes, new disclosures to consumers and new authorization obligations should be triggered. This should be made explicit in the rule. Similarly, data providers would have the same rights to obtain authorization from the consumer regarding the scope of data to be shared with that third party and to withhold making data available in order to conduct due diligence on any new downstream entities that may get access to the consumer's data. This would help ensure consumer data is not compromised due to an authorized third party's decision to change service providers. The CFPB should make appropriate clarifications in the rule to address all such scenarios.

Consistent with our recommendation in section (2)(b)(i), there should be an explicit provision in § 1033.401 to prohibit third parties from seeking access to covered data from a data provider unless they are an authorized third party in accordance with § 1033.401. The rule should further provide that if a developer interface is established by a data provider, prior to or after the data provider's official compliance date, authorized third parties and data aggregators are prohibited from accessing a data provider's consumer interface to access data made available via the developer interface as a new subsection to § 1033.421. A prohibition against authorized third parties and data aggregators accessing consumer interfaces would be a significant and meaningful benefit to consumers and data providers, and a strong, market-based incentive for them to adopt a compliant developer interface. This would also further effectuate the CFPB's policy goal of reducing the practice of screen scraping as a method of data collection.

b) Authorization disclosure (§ 1033.411)

Proposed § 1033.411 would require a third party to provide the consumer whose data the third party is seeking permission to access with an authorization that "must be clear, conspicuous, and segregated from other material" and must include:

- The name of the third party seeking access;
- The name of the data provider that controls or possesses the data the third party is seeking to access;
- A brief description of the product or service that the consumer is seeking from the third party that requires use of the relevant data; and
- A statement that the third party will collect, use, and retain the consumer's data only for the purpose of providing that product or service to the consumer.

Thus, the proposal would require third parties to provide consumers with clear, conspicuous, and segregated authorization disclosures containing numerous pieces of important information. We support the CFPB's proposed requirement that all this information must be presented clearly to the consumer as part of the authorization process. The CFPB should provide additional guidance regarding the standard that must be met for disclosures to be considered "clear and conspicuous." For example, the rule could include a reference to the "4P's" used by the FTC in determining whether a disclosure is clear and conspicuous.[124] To help ensure that consumers actually review the disclosures, the CFPB should require authorizations to be scrolled through in their entirety by consumers prior to agreeing. The CFPB also should consider including a prohibition on "misleading and inaccurate" statements such as that found in Regulation DD, to ensure by regulation that the disclosure language is not misleading or inaccurate.[125] As a practical matter, the CFPB could cite violations of this standard through its supervisory and enforcement authorities; as we have recommended throughout this letter, third parties and aggregators should be subject to CFPB supervision and examination.

The authorization disclosure also should contain a consumer-controlled duration (anywhere from a one-time data collection authorization up to, but not exceeding, 12 months) unless subsequently revoked or reauthorized to extend and should contain the authorized third party's contact information (address, website, email, telephone number) for consumers to reach to ask questions, resolve issues, or revoke authorization.

While it is important that consumers are provided with critical information in the authorization process regarding with whom, for how long, and for what purpose their data will be shared, it is important that the disclosure is not so long that it is unlikely that most people will review it. As such, striving for more disclosure may have the unintended effect of making consumers *less aware* of how their data is being accessed and used. Accordingly, we recommend that the CFPB consider which components are most important to be presented in the primary authorization disclosure and which components could be referenced in a separate document, which could be made accessible via a hyperlink. This may be similar to the short-form and long-form disclosure regime used as part of the Prepaid Accounts rule.[126] For example, the CFPB could provide an option for the certification statement required to be presented as described in § 1033.401(b) to be accessible via a link or otherwise provided

[124] The FTC has explained that if "a disclosure is truly clear and conspicuous, consumers don't have to hunt for it. It reaches out and grabs their attention. One mnemonic we use – The 4Ps – can help sharpen advertisers' focus on four key considerations:" Prominence, Presentation, Placement, and Proximity. Full Disclosure | Federal Trade Commission (ftc.gov).

[125] 12 C.F.R. § 1030.8(a).

[126] *See* 12 CFR § 1005.18. The CFPB should amend proposed § 1033.421(a)(2) to make clear that using covered data to reverse engineer confidential commercial information, such as an algorithm used to derive credit scores, is a prohibited secondary activity that is not part of, or reasonably necessary to provide, any other product or service.

in a separate document. Similarly, the list of entities with whom the third party reasonably anticipates further sharing the consumer's data could be available via link or separate document.

c) Third party obligations (§ 1033.421)

Proposed § 1033.421 describes the obligations to which third parties must certify to be authorized to access covered data. As discussed further in section (3)(d), aggregators used by third parties to conduct the authorization process and assist with accessing covered data for the third party should have to comply with all of the requirements set forth in this section; as proposed, data aggregators would only have to comply with 1033.421(a)-(f) and § 1033.421(h)(3) upon receipt of the notice described in § 1033.421(h)(2) regarding consumer revocation of authorization. To ensure that consumers have the ability to revoke authorization with any entity involved in the data sharing transaction, aggregators should have to provide consumers with a means to revoke authorization. In addition, 1033.421(g) requires require third parties to provide the consumer with a copy of the authorization disclosure and to provide contact information that enables a consumer to receive answers to questions about the third party's access to the consumer's covered data. Third parties also would be required to establish and maintain reasonable written policies and procedures designed to ensure that the third party provides to the consumer, upon request, the following information:

- Categories of covered data collected;
- Reasons for collecting the covered data;
- Names of parties with which the covered data was shared;
- Reasons for sharing the covered data;
- Status of the third party's authorization; and
- How the consumer can revoke the third party's authorization to access the consumer's covered data and verification the third party has adhered to requests for revocation.

Data aggregators used by third parties should be subject to these same requirements given their involvement in the handling of consumer data.

i) General standard to limit collection, use, and retention (1033.421(a))

Under proposed § 1033.421(a)(1), third parties would be required to limit collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service, and proposed § 1033.421(a)(2) provides that the following activities are not part of, or reasonably necessary to provide, any other product or service:

(i) Targeted advertising;
(ii) Cross-selling of other products or services; or
(iii) The sale of covered data.

We support what we believe to be the intent behind this proposed limitation on the secondary use of data: that if an entity wishes to use a consumer's data for any of these purposes, that entity must follow all the requirements set forth in the proposed rule to obtain the consumer's authorization to do so as the primary purpose of the third party's data access. The proposal appears to take this position in

footnote 130.[127] As discussed previously with respect to aggregators, consumer authorization for any activity other than the primary activity that the consumer desires cannot be obtained in connection with the primary authorization process. The process to obtain the consumer's authorization for any of the aforementioned activities must be separate from the authorization process for a different product.

Finally, reverse engineering should also be expressly prohibited. The CFPB should amend proposed § 1033.421(a)(2) to make clear that using covered data to reverse engineer confidential commercial information, such as an algorithm used to derive credit scores, is a prohibited secondary activity that is not part of, or reasonably necessary to provide, any product or service, as the benefit of using data to reverse engineer inures to the third party, not the consumer. This prohibition should expressly extend to de-identified data, because removing identification information does not mitigate the ability to reverse engineer or the resulting harms.

ii) Collection of covered data (1033.421(b)(1))

Proposed § 1033.421(b)(2) provides that a third party's collection of covered data is limited to a maximum period of one year after the consumer's most recent authorization. BPI and TCH support these limitations on duration and frequency of access, which helps ensure that consumers have continuing knowledge and control over with whom, for what purpose, and for how long their data is shared. As noted above, the authorization disclosure should make this maximum duration clear. The proposal would require the authorization disclosure to include a description of the revocation mechanism that the third party would be required to provide to the consumer, which we agree is an important right of which the consumer should be aware.

iii) Reauthorization after maximum duration (1033.421(b)(3))

To collect covered data beyond the one-year maximum period, the proposal would require a third party to obtain a new authorization from the consumer pursuant to § 1033.401 no later than the anniversary of the most recent authorization from the consumer. The proposed rule also provides that a third party is permitted to ask the consumer for a new authorization in a "reasonable manner." The CFPB should consider establishing more specific requirements regarding how requests for reauthorization may be made. For example, the CFPB should consider limiting the number of times a third party can request reauthorization, including reasonable limitations on pop-ups and notices, and prohibiting requests that could be considered threatening, misleading, or otherwise negatively impact consumers. Prohibited threats would include conditioning providing a consumer one product or service on the consumer's authorizing the third party to capture data for another product or service or use. In particular, consumers should not be coerced into agreeing to allow third parties or data aggregators to use their data for sale, direct marketing, or cross selling in order to obtain a desired product or service.

[127] Footnote 130 provides that "the proposed rule would not prevent third parties from engaging in an activity described in proposed § 1033.421(a)(2) as a stand-alone product. To the extent that the core function that the consumer seeks out in the market is such an activity, a third party could potentially provide that core function to the consumer consistent with, and subject to, the terms of the proposed rule. Any such offering, of course, would also be subject to all other applicable laws, including the CFPA's prohibition on unfair, deceptive and abusive practices." 88 Fed. Reg. at 74833-74834.

The CFPB should also prohibit retaliatory behavior by third parties (and aggregators if acting on behalf of a third party) if a consumer does not reauthorize. This would be consistent with § 1033.421(h)) that provides that in connection with a consumer's revocation of a third party's access, the third party "will also ensure the consumer is not subject to costs or penalties for revoking the third party's authorization." As described below, the CFPB should clarify that "penalties" include retaliatory behavior towards the consumer. In addition, all of the requirements applicable to the initial authorization should apply to any reauthorization and downstream data users and holders, where relevant. As noted throughout this comment letter, third parties and data aggregators should be subject to direct CFPB supervision to ensure that those entities are complying with all the requirements set forth herein as well as all Federal consumer protection and data security laws, as applicable.

iv) Effect of maximum duration (1033.421(b)(4))

The proposed rule provides that if a consumer does not provide the third party with a new authorization, the third party will no longer collect covered data or use or retain covered data that was previously collected unless use or retention of that covered data remains reasonably necessary to provide the consumer's requested product or service. This provision could present risks to consumers if appropriate guardrails are not established and enforced. Consumers should be provided with clear disclosures regarding how their data will continue to be used or retained and the terms of any such continued use or retention after an authorization has lapsed, to the extent data is required to continue to be used to provide the specific product or service, and consumers must agree to such continued use or retention. This transparency and consumer consent is important to ensure that consumers retain control over the collection, use, and retention of their data. The standard in the proposed rule is too vague to meaningfully inform consumers about the actual uses or to provide them with any meaningful ability to understand what data would be used or retained and for how long, undermining the fundamental principle that consumers should retain ultimate control over their data. If the consumer does not agree, the continued use or retention must be ceased by the third party on expiration of the authorization.

While we agree with the requirement that after the maximum duration lapses the third party may no longer collect, use, or retain covered data, the CFPB should make clear that the third party itself must no longer retain the data, nor may the third party transfer the data to another party to retain, for example. It should be made explicit that this provision requires third parties to purge and delete the data.

v) Use of covered data (1033.421(c))

The proposal provides that the general standard to limit collection, use, and retention of covered data pursuant to § 1033.421(a) includes both the third party's own use of covered data and provision of covered data by that third party to other third parties. The proposal states that "[p]roposed § 1033.421(c) specifies that, in addition to limiting the third party's own use of covered data, third parties would not be able to provide covered data to other third parties unless doing so is reasonably necessary to provide the consumer's requested product or service."[128] The proposal provides the following examples of uses of covered data that are permitted under that section of the proposal:

[128] 88 Fed. Reg. at 74836.

(1) Uses that are specifically required under other provisions of law, including to comply with a properly authorized subpoena or summons or to respond to a judicial process or government regulatory authority;
(2) Uses that are reasonably necessary to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; and
(3) Servicing or processing the product or service the consumer requested

First, this section, and the related section, 1033.421(f), do not provide adequate details regarding the circumstances under which an authorized third party would be permitted to provide covered data to another third party, including unaffiliated third parties. The proposal contemplates just one example of when an authorized third party may share a consumer's data outside of sharing required by law or reasonably necessary to prevent fraud: sharing in connection with "servicing or processing the product or service the consumer requested." However, the CFPB should establish a more stringent limiting principle as to when secondary sharing would be permitted. For example, it may be permissible for third parties to share data with subcontractors that enable an authorized third party to provide its products or services. However, this secondary sharing should be expressly limited to such instances and be properly disclosed to consumers.

Second, this section and proposed § 1033.421(f) would require only that the third party hold other third parties with whom it shares a consumer's data contractually liable for meeting a subset of the obligations that the third party itself must meet, including the limitation on collection, use, and retention of consumer data and data security requirements. This framework is inadequate to ensure that consumers and their data and data providers are protected from harm that may occur when sensitive data leaves the safety of a prudentially regulated and supervised bank. The CFPB must establish robust requirements regarding the protection of consumer data that are enforceable by the CFPB rather than merely by third party contract. Additionally, the CFPB should supervise third parties that provide financial products and services to consumers to ensure that consumers and their data are protected regardless of whether they obtain products and services from a bank or nonbank. At a minimum, the CFPB should raise the standard to which the third party is held for ensuring other third parties comply with the requirements in the proposal by providing that a third party must "require and ensure" that other third parties abide by the relevant obligations.

As noted previously, the CFPB proposes as part of the rulemaking to define "service provider," which is generally defined in section 1002(26) of the Dodd-Frank Act as "any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service."[129] A service provider may or may not be affiliated with the person to which it provides services. The CFPB should subject third parties to direct supervision and oversee service providers to ensure that those third parties and their service providers are meeting their obligations to protect consumers and their data, including by ensuring that other third parties abide by those same obligations.

vi) Accuracy (1033.421(d))

The proposal provides that third parties will establish and maintain written policies and procedures that are reasonably designed to ensure that covered data are accurately received from a

[129] 12 U.S.C. 5481(26).

data provider and accurately provided to another third party, if applicable. In developing their policies and procedures, third parties must consider, for example:

- Accepting covered data in a format required by § 1033.311(b); and
- Addressing information provided by a consumer, data provider, or another third party regarding inaccuracies in the covered data.

The proposal would require third parties, in developing their policies and procedures, to consider accepting covered data in a format required by § 1033.311(b), which provides that data providers must make data available via the developer interface in a standardized format. However, consideration must be given to the format in which third parties may ultimately digest the data. Currently, many data aggregators provide data to third parties in a proprietary format unique to each aggregator. Therefore, to the extent that it is the intention of the CFPB that the industry align around a standardized format, the role of aggregators as intermediaries in the transmission of data must be considered. The CFPB should require data aggregators to, at a minimum, offer covered data in a standardized format.

1033.421(d)(4) provides that indicia "that a third party's policies and procedures are reasonable include whether the policies and procedures conform to a QIS regarding accuracy." However, the establishment of an industry standard regarding accuracy of the receipt or downstream transmission of data may not be a metric that is able to be readily tested and standardized across the universe of third parties. Rather, policies and procedures that are reasonably designed to achieve a high degree of accuracy in acceptance and transmission and that provide for comprehensive monitoring and swift correction of any inaccuracies should be adequate to ensure that accuracy is monitored closely in the ecosystem. Moreover, the CFPB should ensure that third parties uphold these obligations through supervision and examination of those entities.

vii) Data security (1033.421(e))

1033.421(e)(1) provides that a third party will apply an information security program that satisfies the applicable rules issued pursuant to section 501 of the Gramm-Leach-Bliley Act to its systems for the collection, use, and retention of covered data.[130] If the third party is not subject to section 501 of the GLBA, the rule provides that the third party will apply to its systems the information security program required by the Federal Trade Commission's Standards for Safeguarding Customer Information.[131]

We appreciate and support the CFPB's recognition of the importance of ensuring that third parties have robust data security practices. However, rather than requiring third parties to meet the standards under section 501 of GLBA or the FTC Safeguards rule, we recommend that all third parties should be required to apply to their systems for the collection, use, and retention of covered data an information security program that satisfies the standards set forth in the FFIEC Information Technology Examination Handbook on Information Security.[132] While the CFPB may seek to enforce the FFIEC

[130] *See* 15 U.S.C. § 6801.

[131] 16 CFR part 314.

[132] FFIEC Information Technology Examination Handbook Information Security (September 2016), ffiec_itbooklet_informationsecurity.pdf.

standards through its UDAAP authority, explicitly requiring adherence to those standards will create additional clarity as to the CFPB's expectations. By not requiring adherence, it may weaken the CFPB's authority to cite a UDAAP violation where an entity otherwise complied with the lowest applicable standard. The GLBA and FTC Safeguards rule are neither specific nor comprehensive enough to address the stringent security protocols that should be followed to protect shared consumer financial data. The FFIEC Information Security Handbook standards are more comprehensive and detailed. These are the standards by which banks must abide to protect consumer information, in addition to the prudential regulatory expectations to which they are subject. Nonbanks will be in possession of the same sensitive data that banks are, and every entity to which that data is provided should be held to no less stringent standards to ensure that consumers and their data are adequately protected.

viii) Provision of covered data to other third parties (1033.421(f))

Proposed § 1033.421(f) provides that before providing covered data to another third party, third parties will "require the other third party by contract to comply with the third-party obligations in paragraphs (a) through (g)" of 1033.421 and the condition in paragraph 1033.421(h)(3).

As noted previously, the proposal provides that the general standard to limit collection, use, and retention of covered data pursuant to § 1033.421(a) includes both the third party's own use of covered data and provision of covered data by that third party to other third parties. The proposal provides the following examples of uses of covered data that are permitted under that section of the proposal:

- Uses that are specifically required under other provisions of law, including to comply with a properly authorized subpoena or summons or to respond to a judicial process or government regulatory authority;
- Uses that are reasonably necessary to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; and
- Servicing or processing the product or service the consumer requested.

As stated previously, the CFPB should establish a more restrictive standard as to when secondary sharing by third parties would be permissible. For example, it may be permissible for third parties to share data with subcontractors that enable an authorized third party to provide its products or services. However, this secondary sharing should be expressly limited to such instances, and additional protections should be added to the rule, as described further herein.

In addition, the proposed rule does not contemplate that a third party would be required to disclose to a consumer as part of the authorization process the other third parties with whom the third party may share the data for purposes such as servicing or processing the product or service the consumer requested. While the third party would be required to provide the consumer with the names of entities with whom the third party has shared the consumer's data pursuant to § 1033.421(g) on the consumer's request and after the sharing has transpired, consumers would not have the ability to authorize the third party's proposed sharing of the consumer's data with other entities with whom the third party intends to share in the first instance. At a minimum, consumers should have transparency and control over other entities with whom their data is shared to the extent third parties know other entities with whom they intend to share the consumer's data, such as third-party processors or other vendors. We understand that third parties cannot not represent with certainty that a consumer's data would be shared with law enforcement or to prevent fraud with any specificity, but the authorization or

an additional or linked disclosure could contain a general disclosure that the consumer's data would be so shared as required by law or to prevent fraud.

As noted previously, data providers must be able to conduct robust third-party risk management assessments when its data is being shared with other entities, but the proposal does not provide for any disclosure to data providers of third parties with whom a third party intends to share or has shared consumer's data from that data provider. One could imagine creative legal structures to obscure from data providers and consumers the full uses of consumer data as it relates to downstream uses and agreements, especially as it relates to the movement of funds.

Finally, the proposal would require only that a third party holds other third parties with whom the third party shares a consumer's data contractually liable for meeting a subset of the obligations that the third party itself must meet, including the limitation on collection, use, and retention of consumer data, data security requirements, and ensuring that consumers are informed as required under 1033.421(g), discussed further below. The requirements applicable to third parties with whom the initial third party shares a consumer's data should be directly applicable to those entities and enforceable by the CFPB rather than merely by third party contract, and the CFPB should supervise third parties that provide financial products and services to consumers to ensure that those third parties are appropriately monitoring entities with whom they share consumers' data for compliance with all of the obligations by which the third party must abide. Any requirement that is left to contract between parties could leave inconsistent consumer protections. In some cases, it may be appropriate for the CFPB to directly supervise entities with whom the third-party shares consumer data, in addition to aggregators, which we have described previously. Consumers and their data must be protected regardless of whether consumers obtain products and services from a bank or nonbank. At a minimum, the CFPB should raise the standard to which the third party is held for ensuring other third parties comply with the requirements in the proposal by providing that a third party must "*require* and ensure" that other third parties abide by the relevant obligations.

ix) Ensuring consumers are informed (1033.421(g))

Proposed § 1033.421(g) would require third parties to provide the consumer with a copy of the authorization disclosure and to provide contact information that enables a consumer to receive answers to questions about the third party's access to the consumer's covered data. Third parties also would be required to establish and maintain reasonable written policies and procedures designed to ensure that the third party provides to the consumer, upon request, the following information:

- Categories of covered data collected;
- Reasons for collecting the covered data;
- Names of parties with which the covered data was shared;
- Reasons for sharing the covered data;
- Status of the third party's authorization; and
- How the consumer can revoke the third party's authorization to access the consumer's covered data and verification the third party has adhered to requests for revocation.

In addition to this information that would be required to be provided to the consumer upon request, the aggregator authorization may be obtained separately from the third-party authorization disclosure process. Any separate aggregator authorization should be available to the consumer on

request from either the third party or the aggregator. Additionally, as noted, third parties should have to disclose other third parties with whom the third party reasonably expects to share the consumer's data as part of the authorization process, which would give consumers greater transparency into and control over with whom their data may be shared.

x) Revocation of authorization (1033.421(h))

Proposed § 1033.421(h) provides that third parties will provide the consumer with a mechanism to revoke the third party's authorization to access the consumer's covered data that is as easy to access and operate as the initial authorization. The third party also "will also ensure the consumer is not subject to costs or penalties for revoking the third party's authorization." As noted previously, the CFPB should clarify that "penalties" include retaliatory behavior towards the consumer. The third party also must notify the data provider, any data aggregator, and other third parties to whom it has provided the consumer's covered data when the third party receives a revocation request from the consumer. When a third party receives a consumer's revocation request or notice of a revocation request from a data provider as described in § 1033.331(e), a third party will:

- No longer collect covered data pursuant to the most recent authorization; and
- No longer use or retain covered data that was previously collected pursuant to the most recent authorization unless use or retention of that covered data remains reasonably necessary to provide the consumer's requested product or service.

The proposed rule provides that if a consumer revokes authorization, the third party will no longer collect covered data or use or retain covered data that was previously collected "unless use or retention of that covered data remains reasonably necessary to provide the consumer's requested product or service." This provision could present risks to consumers if appropriate guardrails are not established and enforced. Consumers should be provided with clear disclosures regarding how covered data will continue to be used or retained and the terms of any such continued use or retention after an authorization has been revoked and must agree to such continued use or retention as part of the initial data sharing authorization. If the consumer does not agree, the continued use or retention must be ceased by the third party, regardless of the impacts on the delivery of the specific product or service.

d) Data aggregators (§ 1033.431)

The rule contemplates that authorized third parties may use data aggregators to "enable access to covered data." It likely will continue to be too expensive and administratively onerous for each third party to directly connect with thousands of data providers, aggregators are likely to continue to facilitate connectivity for thousands of data providers and data recipients, thereby giving them access to a substantial volume of sensitive consumer financial data. Therefore, it is essential that the rule clearly requires data aggregators to abide by appropriately robust requirements to ensure that consumers and their data remain safe and secure.

As noted previously, to ensure that consumers and their data are protected, the proposal should ensure that *all* third parties (not just authorized third parties) and aggregators used by those third parties will be held accountable for implementing and maintaining robust data security, privacy, and consumer protections, including limitations on the collection, use, and retention of consumer data, and all of the requirements in any final rule implementing section 1033. Third parties and aggregators should be subject to direct supervisory oversight and CFPB enforcement to ensure these obligations are met.

Currently, the proposal does not impose sufficiently robust requirements on data aggregators. For example, the proposal provides that data aggregators would be bound to comply with the certification obligations in 1033.421 when acting on behalf of an authorized third party, which include important limitations on the collection, retention, and use of consumer data. However, *those authorized third parties would be responsible for the data aggregator's compliance with those obligations*, rather than the CFPB.[133] In turn, under the proposal, data providers would be responsible for ensuring that authorized third parties have complied with their own data authorization obligations, which we previously discussed as also being insufficient as a means of overseeing third parties.[134] Because data aggregators hold and process the largest volumes of data, they must be subject to explicit requirements in the rule enforceable by the CFPB as well as direct supervision by the agency.

Proposed § 1033.431 provides that "a data aggregator is permitted to perform the authorization procedures described in § 1033.401 on behalf of the third party."[135]

The proposal also provides that when a third party intends to use an aggregator to "assist with accessing covered data on behalf of a consumer, the data aggregator must certify to the consumer that it agrees to the conditions on accessing the consumer's data, in § 1033.421(a) through (f) and the condition in § 1033.421(h)(3) upon receipt of the notice described in § 1033.421(h)(2), before accessing the consumer's data." These conditions are those to which authorized third parties must agree.

In both instances, the responsibilities and obligations of the aggregator are defined by reference to provisions of the rule addressing the third party's obligations directly rather than the aggregator's. In general, *it would be clearer if the CFPB established separate requirements setting forth the aggregator's responsibilities and obligations rather than cross-referencing provisions governing third parties*. For example, the certifications that both the aggregator and third parties provide set forth in 1033.421 include provisions related to maximum duration of the collection of data and the requirement to obtain consumer reauthorization every year. It appears that an aggregator could perform the reauthorization function on behalf of a third party, but this could be made explicit in the rule.

Substantively, it is not clear why aggregators are not required to certify to the conditions set forth in 1033.421(g), which list requirements for third parties to ensure "consumers are informed," including by providing a copy of the authorization to the consumer and providing contact information to the consumer to ensure the consumer can receive answers to questions about the third party's access to the consumer's covered data. These same requirements should similarly apply to data aggregators so that the aggregator must ensure that the consumer receives the aggregator's certification (either separately from the third party certification or with the third party certification, each of which is a permissible option under the proposal), and the consumer is able to contact the aggregator about the

[133] Proposed § 1033.431(a).

[134] Proposed § 1033.331(b)(iii).

[135] The authorization procedures in § 1033.401 provide that to "become an authorized third party, the third party must seek access to covered data" and: (a) Provide the consumer with an authorization disclosure as described in § 1033.411; (b) Provide a statement to the consumer in the authorization disclosure, as provided in § 1033.411(b)(5), certifying that the third party agrees to the obligations described in § 1033.421; and (c) Obtain the consumer's express informed consent to access covered data on behalf of the consumer by obtaining an authorization disclosure that is signed by the consumer electronically or in writing."

services it provides on behalf of the third party in helping to facilitate the consumer's access to the desired product or service provided by the third party. Establishing separate and distinct responsibilities and requirements applicable to third parties and data aggregators would help ensure that those entities, and all entities in the ecosystem, understand their obligations and responsibilities.

The rule also should prohibit data aggregators acting on behalf of authorized third parties from capturing an authorization from the consumer to use data for its own purposes (i.e., beyond what is needed to enable data sharing with the third party) as part of its interaction with a consumer on behalf of the third party. This would prevent the aggregator from obtaining consumer authorization for the aggregator to use the consumer's data for a separate use beyond the third party's product or service that the consumer originally sought.

Prohibiting this activity is consistent with the CFPB's goal of ensuring that consumers have control over the use of their data and that data is collected and used solely for the purpose the consumer intended it to be used. Consumers should never have new accounts or customer relationships established for them without their full knowledge and consent; an aggregator must not do so in fine print, when the consumer likely has no prior relationship and often no knowledge of the aggregator's existence. If data aggregators wish to use consumer data for their own purposes, they must offer those products and services and obtain separate consumer authorization to obtain that data for the use for which they intend to use it just as any other third party must do under the proposed rule.

Finally, data providers must be able to impose requirements and obligations on data aggregators and hold them accountable for risk management purposes in the same way data providers should be able to hold authorized third parties accountable. We provide further comments on data providers' right to deny access in section 2(d) of this Appendix. Nothing in the rule should restrict data providers' ability to enter bilateral agreements with data aggregators to provide additional consumer protections and protections to ensure the data provider's safety and soundness.

Data Aggregator authentication

Data providers should be able to require information sufficient to authenticate an aggregator. Proposed § 1033.331 provides that upon request from an authorized third party, a data provider must make available covered data when it receives information sufficient to: (i) Authenticate the consumer's identity; (ii) Authenticate the third party's identity; (iii) Confirm the third party has followed the authorization procedures in § 1033.401; and (iv) Identify the scope of the data requested. In addition, the data provider is permitted to confirm the scope of a third party's authorization to access the consumer's data by asking the consumer to confirm the account(s) to which the third party is seeking access and the categories of covered data the third party is requesting to access.

The CFPB also should clarify that when a third party uses a data aggregator, the data provider should have all of the rights herein with respect to the aggregator. For example, the data provider should only have to make available data when it receives information sufficient to: authenticate the consumer's identity, the third party's identity, the aggregator's identity, confirm that the aggregator has followed the authorization procedures in § 1033.401, and identify the scope of the data requested. In addition, the data provider should be permitted to obtain its own authorization from the consumer regarding the scope of the consumer's authorization to allow the aggregator, on behalf of the third party, to collect the consumer's data from the data provider. In short, all of the provisions in § 1033.331 regarding responding to requests for information that refer to a third party should apply when a third party uses a

data aggregator, as well as the additional recommendations we make herein regarding the data provider's right to conduct their own consumer authorization process,

This clarification would help data providers ensure that consumers' data remains safe and is only shared when the consumer has authorized such sharing. Extending these provisions to data aggregators also would help ensure that data providers are able to conduct appropriate risk management due diligence and help ensure consumers understand and authorize the access they are granting to what entities and for what purpose. For example, data providers could provide consumers a security dashboard listing the entities with whom consumers' data has been shared and for what purpose.

e) Policies and procedures for third party record retention (§ 1033.441)

The proposal provides that a third party that is a covered person or service provider must establish and maintain written policies and procedures that are reasonably designed to ensure retention of records that are evidence of compliance with the requirements of subpart D, which provides the obligations of third parties that would access covered data on behalf of a consumer.

Third parties would have to retain records for a reasonable period, not less than three years after a third party obtains the consumer's most recent authorization. Records retained would have to include a copy of the authorization disclosure that is signed or otherwise agreed to by the consumer and a record of actions taken by the consumer to revoke the third party's authorization. Data aggregators would have to retain a copy of any data aggregator certification statement provided to the consumer separate from the authorization disclosure, as would be permitted under the proposal.

The requirement to retain only the authorization disclosure and any revocation is too limited to ensure that consumers may obtain information about with whom their data has been shared for reasonable period of time after its last authorization. For example, the proposal would require data aggregators to retain a copy of the data aggregator certification if it is obtained separately from the authorization process and would require third parties to retain the authorization disclosure. However, the third party should have to maintain the record of data aggregator authorization if separate from the third party authorization, or, at a minimum, obtain the aggregator authorization from the aggregator on consumer request. The record retention period should follow industry standards, but should not exceed two years to be consistent and align with existing record retention periods for credit card and Regulation E accounts.

The rule also provides that third parties must ensure that consumers can obtain the names of parties with which the covered data was shared. Contact information for these parties should also be provided to consumers so that they can address any concerns they may have upon learning of the name of the third party. To ensure that consumers may obtain this information for a reasonable period of time after final authorization, these records should be maintained for the minimum period. Consumers may wish to access this information even after authorization has not been renewed or has been revoked, and two years is a reasonable period of time to provide consumers to obtain that information. Finally, the CFPB should closely monitor consumer complaints and ensure that third parties uphold these obligations through risk-based supervision and examination of those entities.