Submitted electronically

December 21, 2023

Comment Intake—FINANCIAL DATA RIGHTS
c/o Legal Division Docket Manager
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Notice of Proposed Rulemaking - Required Rulemaking on Personal Financial Data Rights
(Docket No. CFPB-2023-0052; RIN 3170-AA78)

The Financial Technology Association (FTA) appreciates the opportunity to provide feedback on the CFPB's "Notice of Proposed Rulemaking - Required Rulemaking on Personal Financial Data Rights," which will implement Section 1033 of the Dodd-Frank Act (the "Proposal"). FTA believes that a robust personal financial data right can empower consumers, drive greater financial health and opportunity, and advance consumer-centric financial services competition.[1] We accordingly applaud the Bureau's Proposal and offer this comment letter in support of the thoughtful and consumer-centric final implementation of the rule.

FTA champions the transformative role of financial technology for American consumers, businesses, and the economy. A core pillar of FTA's effort to advance consumer-centric financial services development in the U.S. is ensuring modern regulatory frameworks that recognize and foster the benefits of financial technology-driven innovation, including with respect to new models that rely on responsible use of financial data. Fintech innovators are leveraging internet and mobile technologies to offer consumers access to credit, new payment options, and financial advisory services that can significantly reduce costs, accelerate access to funds, improve transparency and convenience, and enhance financial inclusion.

[1] We agree with the Bureau that "[d]igitization and decentralization in consumer finance create new possibilities for more seamless consumer switching and greater competitive intensity." *See* Consumer Financial Protection Bureau, *Required Rulemaking on Personal Financial Data Rights* (Docket No. CFPB-2023-0052), available at https://files.consumerfinance.gov/f/documents/cfpb-1033-nprm-fr-notice_2023-10.pdf. Examples of open banking include when consumers seamlessly connect their bank account to a payment app, use personalized financial dashboards to better understand their financial health, provide access to non-traditional financial data in order to receive credit, and aggregate investments with robo-advisors. Open banking further provides opportunities to stimulate payments innovation by permitting direct integrations with banks and offering consumers faster and lower-cost payments services.

Much of this innovation is the result of consumers being increasingly able to expand their access to tailored financial products by unlocking and sharing their financial data with new providers. The ability to control and share financial data allows consumers more convenient and efficient ways to view and manage their money and shop for new, more tailored, and lower-cost financial services products and providers. This facilitates competition by allowing new entrants in the marketplace and ensuring information is no longer trapped with incumbent providers; consumers are empowered to use their data for their own benefit.

Notably, today, open banking technology allows access to important tools for unbanked and underbanked consumers, including increased access to credit through identity verification, increased data sources, such as rental, utility, or tax payment history, and no-fee salary advances. This technology further helps to safeguard the financial system, including through enhanced fraud mitigation tools facilitated by robust identity verification capabilities.[2]

I. The Bureau Should Anchor to Core Guiding Principles and Make Important Amendments to the Proposal in Finalizing Section 1033 Implementation.

FTA welcomed the earlier opportunity to comment on the CFPB's "Outline of Proposals and Alternatives Under Consideration Related to the Rulemaking on Personal Financial Data Rights." In that letter, we noted the importance of the Bureau anchoring the ultimate implementation of the 1033 rulemaking to three core principles, which remain equally relevant here. More specifically, we urged then and reiterate now that in finalizing the rule, the Bureau should:

1. *Focus on consumer-centric implementation*: The touchstone of the final rule should be fostering competition and responsible innovation in financial services that permits more informed comparison shopping and product selection, better holistic understanding of financial health and wellness, and ultimately greater financial choice and opportunity. As discussed in greater detail below, this means allowing for consumer-centric secondary use of such data, subject to clear disclosure, as well as robust privacy and security safeguards.

2. *Avoid anti-competitive behavior*: Traditional financial institutions (FIs) have commonly held a consumer's financial data captive in order to prevent the consumer from switching to a different service provider or shopping for alternative products and services.[3] Consistent

[2] *See, e.g.*, MX, *What Is Instant Account Verification? What to Know and Key Benefits*, available at https://www.mx.com/blog/what-is-instant-account-verification/; Plaid, *Plaid Identity Verification* (last visited Dec. 14, 2023), available at https://plaid.com/products/identity-verification/.

[3] *See* Dan Murphy and Jennifer Tescher, *Policymakers must enable consumer data rights and protections in financial services*, Brookings (Oct. 20, 2021) ("Already there are reports of some financial institutions restricting access to consumer data. Such restrictions can serve to entrench incumbent institutions and limit competition to the detriment of consumers. These restrictions also are out of step with consumer preferences."), available at

with the U.S. Treasury Department's recent white paper on competition in financial services, the Bureau should monitor and prevent industry attempts to craft, interpret, and apply certain Section 1033 requirements in a manner that would block the sharing of financial data, restrict data parity, and advance anti-competitive objectives.

3. *Leverage Existing Legal Frameworks, Technologies, and Standards Setting Organizations (SSOs)*: Given the potential complexity of implementing Section 1033, FTA supports the Bureau's proposed reliance on existing legal and regulatory frameworks, and available technologies, to avoid creating new, untested requirements that may delay implementation, increase uncertainty, or complicate compliance. FTA further supports reliance on SSOs, but encourages the Bureau to work promptly to provide more specificity around the proper development and approval of an SSO given its centrality to the successful implementation of open banking in the United States.

With these core principles underpinning our feedback, FTA will detail below the following recommendations and suggested amendments to final implementation of the open banking rule:

A. Broader use of data, including for secondary use and when data is de-identified, benefits consumers and should be permitted, subject to appropriate disclosures and additional safeguards.
B. Given the importance of SSOs and related standards and certifications, the final rule should provide greater clarity regarding the composition, operations, and role of SSOs, as well as more time to ensure an SSO is properly developed.
C. Given the time, cost, and complexity of operationalizing Section 1033 requirements, the final rule should create a more realistic timeframe for implementation—a failure to do so could result in confusion, undermine security and trust, and lead to service interruptions that harm consumers.
D. The concept of digital wallets is vague and undefined—the final rule should provide greater clarity regarding definitions and responsibilities, as well as provide for an extended implementation timeframe.
E. The Bureau should further ensure that the final rule:
    i. Clarifies the interplay of Section 1033 with the proposed FCRA rulemaking and confirms that data aggregators are not de facto credit bureaus.

https://www.brookings.edu/research/policymakers-must-enable-consumer-data-rights-and-protections-in-financial-services/; *see also* Director Rohit Chopra, *Prepared Remarks of CFPB Director Rohit Chopra on the Overdraft Press Call* (Dec. 1, 2021) ("If America can shift to an open banking infrastructure, it will be harder for banks to trap customers into an account for the purpose of fee harvesting."), available at https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-rohit-chopra-overdraft-press-call/.

ii. Avoids overly prescriptive disclosure requirements and ensures such disclosures are not used by data providers to dissuade or discourage a consumer from seeking a personal data transfer.

iii. Establishes clear standards around the use of Tokenized Account Numbers to avoid anticompetitive behavior, undermining fraud models, and chilling further innovation in business models.

II. Broader use of data, including for secondary use and when data is de-identified, benefits consumers and should be permitted, subject to appropriate disclosures and additional safeguards.

As a threshold matter, FTA understands and agrees with the Bureau on the importance of safeguarding how consumer data is collected and used by intermediaries and financial services providers. FTA members are among the world's leading financial technology firms focused on improving consumer financial services, outcomes, and opportunities. Financial data is often at the center of financial services innovation, and its fair, transparent, and permissioned use is critical to building consumer trust and driving consumer-centric competition and product development.[4] To this end, FTA members take seriously their responsibilities and obligations to customers, and view such commitments as essential to building this long-term trust.

As part of these commitments, FTA has published data privacy principles that reflect FTA's values of promoting consumer trust and transparency, along with financial inclusion and robust competition to lower costs and improve financial services.[5] These principles for engaging with consumers include: (i) full transparency regarding how data is collected and used, (ii) consumer control of personal data, (iii) provider use of data for stated and transparent purposes, (iv) plain language disclosures, and (v) non-discrimination.

We note these principles as consistent with the overarching goals and intent of Section 1033 and consistent with unlocking the full value of open banking for consumers. When presented with clear information on data collection, use, and practices, consumers are best positioned to authorize the

[4] It is important to emphasize that this rulemaking should mark only the beginning of a broader push in the U.S. to an "open finance" system, whereby all individuals and entities have the ability to share their permissioned financial data with chosen third-parties. To this end, broader categories of data should be incorporated into an open finance system and no data providers should be allowed to engage in anti-competitive behaviors in order to block or dissuade the sharing of such data. FTA welcomes the Proposal's requirements regarding the obligations of data providers for categories of data not explicitly covered by the final rule and the push for wider adoption of APIs that will underpin an expanded open finance system in this country.

[5] Financial Technology Association, *FTA Privacy Principles for the Future of Finance* (last visited Dec. 14, 2023), available at https://www.ftassociation.org/fta-privacy-principles-for-the-future-of-finance/.

sharing and use of their financial data. A broad right to such authorization ensures that consumers can benefit from increased financial services competition and improved product offerings.

On the other hand—and of particular concern given the Proposal's current approach to data collection and use—unnecessarily prescriptive regulatory limitations and restrictions on data collection, retention, and use will undermine consumer interests by reducing the ability of third parties to develop new products and services and offer consumers additional products that compete with their legacy providers. An approach that seeks to preclude providers from collecting and using data for consumer-centric product innovation will have negative consequences on competition, innovation, and the health of financial services in the United States. As detailed below, this approach is also not necessary to satisfy legitimate consumer and regulatory privacy concerns. To this end, reasonable safeguards can empower consumers to understand and authorize how their data is used, while preventing harms referenced by the Bureau in its Proposal.

A. Consumers should have the right to permission their data that is "reasonably related" to the products or services being offered by a third party.

The Bureau's Proposal limits a provider's access only to a consumer's data that is "reasonably necessary" to provide the product or service requested by the consumer. This standard creates the opportunity for misinterpretation that is unnecessarily restrictive, could impede consumer-centric product offerings, and places third-parties receiving data through Section 1033 at an unfair disadvantage relative to those receiving data under well-established regimes, including the Gramm-Leach-Bliley Act (GLBA).

More specifically, in offering a particular product or service—and further improving or tailoring such product or service—a provider may reasonably collect a range of data and data elements. Each such data element alone may not be explicitly "necessary" for the provision of a particular product or service, but taken together such elements become necessary to offering the product or service. Additionally, certain data elements may be important to improving aspects of the product or service, including the associated customer experience and overall product performance, rather than being critical in offering the original product or service. Allowing space for improving products is critical to avoid locking in the status quo. The improvement of products may require access to various data elements, some of which will prove to be essential to that new product or offering.

For this reason, the Bureau should allow an authorized third-party to collect data that is "reasonably related" to the product or service, especially because the data is already subject to appropriate

safeguards.[6] To this end, the Bureau should consider how the requirement of clear disclosure regarding data use and informed consent can help to minimize regulatory concerns.

Additionally, GLBA allows financial institutions to collect data that goes beyond a "reasonable necessity" standard, subject to disclosure and consent safeguards. Consistent with our north star principle of leveraging existing regulatory frameworks to help ensure consistency and certainty, GLBA should inform Section 1033 implementation to be sure that all providers are on a level playing field when it comes to collection, use, and retention of permissioned consumer financial data. And, indeed, the Bureau does appropriately rely on GLBA in the Proposal as the framework for data security, which it should similarly do in the context of data use and privacy.[7]

If the Bureau maintains a reasonable necessity standard, however, it should clarify that in determining whether data is reasonably necessary for a particular product or service, it will look holistically at the data being collected and used rather than assess necessity at the individual data element level. The Bureau should further make clear that data elements used to improve, develop, personalize, or innovate from an initial product or service offering are properly considered to be reasonably necessary.

As noted above, an overly restrictive view will serve to lock in the status quo and prevent product improvements that benefit consumers, including with respect to consumer underwriting that has long been constrained by singular reliance on credit scores. Importantly, data is also essential to other business operational improvements, including fraud detection and prevention, as well as enhanced user engagement and experience. Given these business and design realities, absent such clarification in the final rule, including through the provision of examples, the term "reasonably necessary" will create uncertainty amongst providers and limit their confidence in using data to offer or improve a product offering or business operation.

B. Secondary use of consumer data is in the consumer's best interest and should be broadly permitted.

The Bureau's Proposal currently prohibits "secondary use" of financial data, except in limited cases, such as countering fraud. While the Bureau properly notes concerns with certain practices, including opaque sales of consumer data to other entities and providers, it takes an overbroad approach to mitigating such concerns rather than a tailored solution that avoids unintended

[6] Adopting the "reasonably related" standard is supported by the fact that this standard is understood and used for various purposes in state data privacy laws. *See, e.g.*, California Consumer Privacy Act of 2018 (CCPA).
[7] *See* Consumer Financial Protection Bureau Proposal, *Required Rulemaking on Personal Financial Data Rights* (Docket No. CFPB-2023-0052), available at https://files.consumerfinance.gov/f/documents/cfpb-1033-nprm-fr-notice_2023-10.pdf.

consequences. The Bureau should consider the many consumer benefits of secondary data use and whether other tailored safeguards can better satisfy important regulatory objectives, including prohibitions of specific business activities known to cause consumer harm, clear disclosure, and informed consent.

With respect to consumer benefits, secondary uses of financial data may include holistic consideration of the consumer's financial health and tailored recommendations for more appropriate products and services that better meet the consumer's financial goals and which may not be within the scope of services initially requested or may not be known to the consumer to exist as an alternative. Some of these tailored offerings may be part of cross-selling efforts, which are commonly desired by consumers.

Indeed, a recent survey of consumers found that 77% would value having their financial institution offer them personalized financial advice based on open banking financial data; and 94% would want their financial institution to use financial data to advise them about a better deal on a product.[8] Both of these scenarios may be considered a "secondary use" of data. Restricting these types of secondary uses would be inconsistent with the overarching principle that Section 1033 implementation should be in the consumer's best interest. It would also be counter to the inclusion of existing regulatory frameworks that permit secondary use of data, including GLBA and state data privacy regimes. A failure to ensure parity in treatment of secondary use under Section 1033 with other data privacy frameworks will arbitrarily place third-parties in this regime at an unfair competitive disadvantage relative to most other firms in the broader economy.

It is further a bedrock of the American rule of law that consumers should be permitted to make their own informed decisions when provided with proper information.[9] For this reason, it is appropriate for the Bureau to focus on the quality and clarity of disclosures, including when a third-party seeks to use data for secondary purposes. A consumer provided with appropriate disclosures that he or she can reasonably understand should accordingly be able to provide informed consent to secondary use. This approach would be the most consumer-centric and foster consumer choice and agency.

To the extent that there are potential secondary uses objectively deemed so harmful to consumers that it should override informed consent, only those specific uses the Bureau so identifies after careful review and sufficient public comment should be precluded. For example, FTA believes

[8] MX, *The Ultimate Guide to Open Banking*, available at https://www.mx.com/assets/resources/ult-guides/ultimate-guide-to-open-banking.pdf.

[9] Jacqueline M. Nolan-Haley, *Informed Consent in Mediation: A Guiding Principle for Truly Educated Decisionmaking*, 74 Notre Dame L. Rev. 775, 827 (1999) ("Informed consent is an ethical, moral, and legal concept that is deeply ingrained in American culture.").

that consumer financial data should not be secondarily used by providers to enhance collections efforts. There may be other such uses that objectively are not in the consumer's best interest. Beyond these scenarios, however, proper disclosures, informed consent, and data privacy and security practices are the appropriate way to address other risks highlighted by the Bureau in the Proposal, including with respect to the protection of sensitive data.

C. *In line with the SBREFA panel recommendation, de-identified data should be allowed for a broad range of research & development, model development, and product innovation purposes—a failure to so permit will impede financial services and technology development in the U.S.*

The Bureau's Proposal currently includes a blanket prohibition on secondary data use, including when data is de-identified. As the Bureau notes, however, the SBREFA small business panel recommended that the Bureau "consider options that would permit uses of data (including de-identified or anonymized data . . .)." The Bureau goes on to note the existence of a straightforward standard for defining de-identified data that should mitigate outstanding privacy concerns.[10] Given the importance of permitting use of de-identified data and the ready availability of standards to mitigate risks, it would be against the consumer's interest to preclude such use, especially when the use does not harm the consumer. Moreover, a failure to allow for use of de-identified data would cause substantial harm to industry and overall U.S. competitiveness, which require access to high-quality data.[11]

First, smaller financial services providers would find themselves facing an insurmountable competitive disadvantage relative to larger organizations, including banks. Larger FIs collect vast amounts of data on consumers, including under GLBA. These FIs are permitted to pursue research & development, product innovation, and development of new business models, including those leveraging AI technology, using such data. Smaller entities or startups, on the other hand, lack access to large pools of quality data. Section 1033 was intended to help promote consumer choice and market competition, but as proposed by the Bureau, the rule will in effect undermine these objectives if entities receiving data under the rule are not able to use the data, even in a de-identified format, to innovate and compete.

Second, a blanket prohibition on use of de-identified data will impede and undermine U.S. global competitiveness in developing responsible AI/ML technologies, which hold promise across the

[10] *See* Consumer Financial Protection Bureau Proposal, *Required Rulemaking on Personal Financial Data Rights* (Docket No. CFPB-2023-0052), n. 144, available at https://files.consumerfinance.gov/f/documents/cfpb-1033-nprm-fr-notice_2023-10.pdf.

[11] It is important to underscore that once data is properly de-identified it would no longer be subject to the third-party obligations contained within Section 1033.421(h)(3)(ii).

financial services landscape from improving the fairness of consumer underwriting to enhancing compliance and fraud detection. The FSOC recently published its 2023 Annual Report where it noted that "AI offers potential benefits, such as reducing costs and improving efficiencies, identifying more complex relationships, and improving performance and accuracy."[12] FSOC further noted potential risks, including around access to and use of quality data that is subject to appropriate data controls.[13] To this end, Section 1033 holds promise in creating a transparent and regulated pipeline of high-quality data, subject to appropriate safeguards, that can advance responsible model development. The Proposal, however, would undermine such development by limiting access to quality data—likely resulting in less innovation and model development that relies on lower quality data more likely to include inaccuracies, bias, and other harms.

Finally, as noted above—and in contravention of the principle that the Bureau should incorporate existing regulatory requirements and expectations, where appropriate—the current Proposal would place entities receiving data via Section 1033 on an unlevel playing field relative to those receiving data under GLBA or other regulatory frameworks and contractual relationships. Many entities collect and have access to broad pools of de-identified consumer data and rarely have limitations on secondary use. Especially when Section 1033 includes many additional consumer safeguards, it is not necessary to treat these data recipients punitively relative to other data recipients. This approach will also drive nonsensical scenarios where a small bank that receives data directly from customers can use such data, including when it is de-identified, for secondary purposes, while it cannot do the same with respect to data received under Section 1033.

For the reasons noted here, we strongly encourage the Bureau to adhere to the SBREFA small business panel recommendation of allowing use of de-identified data. We further encourage the Bureau to adopt the standard it flagged in the Proposal with respect to defining what "de-identified" data means. More specifically, the Proposal noted that "one standard suggested by SBREFA commenters, articulated in a 2012 FTC privacy report, and codified in several State laws describes de-identified information as data for which a business has (1) taken reasonable measures to ensure that the information cannot be linked to an individual; (2) publicly committed not to attempt to re-identify the information; and (3) contractually obligated any recipients not to attempt to re-identify the information."[14] This standard is a reasonable way to safeguard consumers, while

[12] U.S. Financial Stability Oversight Council, *2023 Annual Report* (December 2023), available at https://home.treasury.gov/system/files/261/FSOC2023AnnualReport.pdf?ftag=YHFa5b931b.
[13] *Id.* FTA and its members believe in the importance of responsibly developing AI technologies, including through collaboration with governmental and regulatory stakeholders. To this end, we look forward to working with the Bureau and the broader government to address risks and ensure responsible AI development in the U.S.
[14] The Proposal (*citing* Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, at 20-21 (2012), available at https://www.ftc.gov/reports/protecting-consumer-privacy-erarapid-change-recommendations-businesses-policymakers; Cal. Civ. Code section 1798.140(m); Colo. Rev. Stat. section 6-1-1303(11); Va. Code sections 59.1-575, 59.1-581; Utah Code Ann. 13-61-101(14)).

allowing for critical, consumer-centric research and development, competition, and product innovation.

III. Given the importance of SSOs and related qualified industry standards and certifications, the final rule should provide greater clarity regarding the composition, operations, and role of SSOs, as well as more time to ensure an SSO is properly developed.

FTA supports the Bureau's proposed incorporation of, and reliance on, a recognized standards setting organization (SSO) that will issue qualified industry standards. As the Bureau notes, prescriptive technical requirements issued by the regulator will fail to keep pace with technological change and the development of related best practices. Beyond such standards, FTA further believes that an empowered SSO is necessary to ensure the sound and efficient operation of an open banking regime in the U.S.

Given the centrality of the SSO to the Bureau's Proposal, as well as the need to further clarify, define, and potentially expand its role, we believe more work needs to be done by the Bureau in its final rulemaking and subsequently by a future SSO before Section 1033 can be safely effectuated. The following recommendations are aimed at increasing clarity and certainty regarding an SSO—which is a lynchpin of the open banking framework—and allowing proper time for SSO development and operationalization.

A. Clarify the process for official SSO "recognition" and ensure diverse representation and governance.

The Proposal suggests that the Bureau will provide further communications regarding the process for official recognition of an SSO and related requirements. Given the centrality of an SSO to the proposed open banking framework, however, we believe that clarity needs to be provided as soon as possible and in advance of the final rulemaking in order to avoid subsequent delays. As a threshold matter, the CFPB should develop a clear application process and timeline to recognize a standard-setting body. Decisions regarding such applications should be made public and explain why an application was approved or denied.

Additional critical areas for clarification include detailed discussion of the criteria the Bureau will use to assess an SSO, as well as confirmation that the Bureau expects that only one such SSO is necessary to accomplish the rulemaking's objectives. While the Bureau notes that diverse stakeholder participation in the governance of the SSO will be necessary, we also believe the Bureau should be more specific in its expectations. For example, the Bureau should require that the SSO leadership include a number of both small and large non-bank financial technology

companies and providers—offering products across the financial services landscape—to avoid the organization being controlled by a few traditional "dominant firms." The Bureau should also express that diversity in SSO representation should also include representative trade organizations, such as FTA, to help expand the range of viewpoints in establishing qualified industry standards.

Beyond membership and governance, the Bureau should also establish which key categories of standards should be largely finalized in order for the SSO to receive official recognition. Put differently, an SSO should not be eligible for formal recognition unless and until it has promulgated standards central to the safe and efficient implementation of the open banking framework, including around security, authorization, disclosures, and risk management. The lack of such standards would severely undermine the framework and risk security and other operational disruptions.

We recognize that there is a bit of a "chicken and egg" dynamic to how the Bureau will be able to review and recognize an SSO and the pace of its work in promulgating standards. More specifically, it is likely an SSO will need to know it is "on the right track" to receiving recognition before it can garner broader stakeholder buy-in and finalize this important work. For this reason, we believe the Bureau should implement a phased approach to full SSO recognition, whereby it meets periodically with an SSO to review its governance and standards-setting efforts and offers feedback on steps to final recognition. To this end, the Bureau might consider providing an SSO with an earlier "conditional approval" predicated on successful completion of key categories of standards that are central to the open banking framework.

B. Provide appropriate time for SSO development and link industry implementation timelines to such development.

As recognized by the Bureau, the key operational, technological, and security details of the U.S. open banking system should appropriately be placed with an SSO. Given the effective delegation of central aspects of the rulemaking to an SSO, it is imperative that the Bureau provide an appropriate and realistic timeframe for SSO development and formal recognition. As further discussed below, the Bureau should also link the commencement of broader industry implementation timelines to the formal recognition of an SSO both to ensure the safe, smooth, and consumer-centric implementation of the open banking framework, as well as to incentivize all stakeholders to complete the work and authorization of an SSO expeditiously.

With respect to an appropriate timeframe for SSO development, as noted above, the Bureau needs to communicate clear guidance and expectations well in advance of a final rulemaking. The Bureau should also engage in ongoing communication with a potential SSO organization, including through use of a "conditional approval" designation process, to allow SSO development to occur

pending a final rule. In order to ensure that all stakeholders are incentivized to form an SSO, promulgate critical standards, and receive formal Bureau recognition, FTA recommends that the Bureau grant an SSO a conditional approval by the time the final rule is issued and make explicit in a final rule that, barring unexpected challenges, an SSO will be fully approved no later than 6 months following the issuance of a final rule. This approach assumes the Bureau works with the industry in the time leading up to a final rule to ensure such a deadline can be satisfied and that a conditional approval is granted by the time the final rule is issued.

Alternatively, if the Bureau is unable to provide additional clarity around SSO requirements and the formal recognition process in advance of the final rulemaking, then the 6 month timeframe may need to be extended. It is advisable that the Bureau not rush implementation without formal qualified standards being in place in order to avoid uneven implementation of the open banking framework. Without accepted standards in place, there are significant risks of operational failures, all of which will undermine consumer trust in open banking—this would be the worst of all outcomes, even relative to the status quo.

Finally, given the centrality and importance of security, authorization, disclosures, and risk management standards, as discussed in greater detail below, we encourage the Bureau to commence broader industry implementation timelines only once an SSO has been recognized by the Bureau, along with its promulgation of key qualified industry standards. A final rule that requires the final approval of an SSO within 6 months of rule publication can prevent unnecessary delay, and render it appropriate to anchor broader implementation deadlines to such approval.

C. Clarify and expand SSO capabilities and responsibilities in order to ensure safe, reliable and consumer-centric operation of the open banking regime in the U.S.

As noted above, it is critical that the Bureau specify core standards that must be promulgated by an SSO prior to formal recognition. These standards should, at a baseline, cover security,[15] authorizations, disclosures, and risk management. A failure to develop qualified industry standards within these categories will result in uneven and potentially defective implementation of the open banking framework. It will further undermine consumer trust and adoption.

Beyond these central categories requiring standards, FTA further encourages the Bureau to specify and expand an SSO's functions in order to foster an orderly, efficient, and trusted open banking system in the U.S. An SSO could be delegated certain regulatory authorities as a Bureau

[15] It is important to note that we do not believe an SSO should promulgate a new data security standard, but rather should adopt existing standards in order to avoid further standards fragmentation.

recognized self-regulatory organization (SRO)[16] or could replicate the organizational features of entities like Nacha. Consistent with our comments above, the development of a robust SSO will require appropriate time but can also ensure safe and seamless implementation of the open banking system.

To this end, we encourage the Bureau to specify and delegate additional key functions to an SSO, including:

- Development of risk management standards that permit objective review and potential denial of access to a third party;
- The collection and maintenance of lists of third parties that are rejected by data providers based on risk management considerations;
- Identification of existing certifications, audits and other processes that confirm compliance with industry standards and/or requirements in the Bureau's final rule; and
- Maintenance of a white list of entities that meet security and other relevant standards based on appropriate certifications.

Notwithstanding the above, FTA recognizes the possibility that an SSO may not be formally recognized within the 6 month timeframe we recommended above due to unexpected circumstances. This scenario would undoubtedly generate ambiguity regarding Section 1033 implementation and operationalization, as well as create security and user-experience risks. The Bureau should accordingly take all steps to facilitate the development and recognition of an SSO, including through further guidance and regular engagement with potential SSO candidates. The Bureau may further have to consider subsequent extensions of implementation timeframes if unforeseen delays arise given the importance of an SSO to the safe and trusted launch of a formal open banking system in the U.S.

IV. Given the time, cost, and complexity of operationalizing 1033 requirements, the final rule should create a more realistic timeframe for implementation—a failure to do so could result in confusion, undermine security and trust, and lead to service interruptions that harm consumers.

As detailed in the Bureau Proposal, data providers are expected to take numerous steps to implement Section 1033 requirements, including technological integrations, the development of internal policies and procedures, the creation of consumer disclosures and engagement interfaces, and ramp-up of operational capabilities. Notably, these implementation steps can increase in

[16] Well known and established SROs with delegated regulatory authority include FINRA from the SEC and NFA from the CFTC.

complexity for larger companies that in some cases will serve as data providers and in others will be data recipients. Under both scenarios, companies will be required to dedicate substantial resources to implementation and to cover all related financial costs. Proper implementation is, of course, critical given the importance of safeguarding consumer data and ensuring a positive consumer experience necessary for building ecosystem trust.

Against this backdrop, FTA remains a steadfast champion of open banking but also recognizes the importance of avoiding hasty and unsuccessful implementation. The long-term success of open banking will begin through a successful launch—a process that will require care, compliance and operational excellence.

FTA accordingly urges the Bureau to ensure realistic implementation timeframes that focus on getting open banking "right" rather than simply out the door. To this end, we believe it is prudent to add an additional 6 months of time to each category of the Proposal's suggested implementation timeframe. As noted above, we further suggest that the Bureau begin these implementation schedules (which will now be 12 months for the largest data providers) at the time the Bureau formally recognizes an SSO, which should be no later than 6 months after the final rule is issued. Under this construct, the latest that Section 1033 implementation will begin in the marketplace is 18 months after the final rule (and potentially earlier if an SSO is recognized prior to the 6 month post-rule deadline).

We believe that the above formula best balances expediency with care and prudence. It would further incentivize the Bureau and market participants to promulgate SSO standards and recognize an SSO sooner than the 6-month post-rule deadline in order to expedite the implementation timeframes. In the event that an SSO is not recognized by the 6-month deadline, the Bureau and market participants will be negatively impacted by the potential for ambiguity and uneven implementation—a powerful incentive to get the SSO authorized and operational. This construct also aligns the Bureau and market participants in monitoring SSO development and further helps them react if there are unexpected implementation developments.

V. The concept of digital wallets is vague and undefined—the final rule should provide greater clarity regarding definitions and responsibilities, as well as provide for an extended implementation timeframe.

The Bureau's proposed coverage of "digital wallet providers" is incongruous with the Proposal's approach to facilitating the sharing of covered Reg E and Reg Z accounts and may create confusion and data integrity problems for data providers, data users, and consumers alike. The Proposed Rule enables consumers to wield their own data in a way that empowers them to obtain new or better consumer financial products or services. As discussed below, however, capturing consumer data

held by a digital wallet provider may create inefficiencies and inaccuracies that conflict with a consumer's ability to achieve these goals.

First, the Proposal covers certain Reg E and Reg Z accounts and the issuers of those accounts. This approach ensures that consumer account data is available to be shared with third parties for any variety of purposes. The Proposal goes on, however, to include "other payment facilitation providers" based on the preliminary determination "that the marginal burden of including other payment facilitation products and services would be minimal given how these providers would generally already be covered as Regulation E financial institutions."[17] The Proposal further suggests that such an approach will avoid loopholes.

We respectfully submit, however, that this analysis does not consider the confusion, unnecessary duplication, and data accuracy challenges that inclusion of other payment facilitators will introduce when such entities interact with Reg E and Reg Z accounts. In these situations, digital wallet providers do not "control or possess" Reg E or Reg Z account data; but rather, they "control or possess" limited account data only for those transactions that were conducted through the digital wallet. Pulling in digital wallet transactions is not consistent with the Proposed Rule's goal of enabling the sharing of consumer account data because digital wallet providers do not have account data to share. Put differently, except for stored value, pass-through digital wallets are merely a record of the underlying data provider's account, and that record is not related to the product being provided to the consumer. The CFPB should be laser-focused on enabling the sharing of account data and not creating multiple, potentially conflicting sources of truth in the consumer's data ecosystem. Accordingly, we suggest excluding pass-through digital wallet features from the scope of the final rule.

Second, including digital wallet providers has the potential to create confusion for consumers and data integrity challenges for users. The data in the control or possession of digital wallet providers is generally only a portion of the data associated with any covered Reg E or Reg Z account and thus the sharing of that data is necessarily incomplete, potentially misleading to any user of that data, and potentially inaccurate due to latency. A consumer who chooses to share data from a digital wallet provider as opposed to the issuer of the covered Reg E or Reg Z account may end up sharing incomplete data, which may not assist the consumer in obtaining the products or services sought. Moreover, having the same data available in multiple places presents the risk of inaccuracies due to latency. For example, a digital wallet provider may have data showing an ACH debit transaction from a covered Reg E account that has not yet processed the received ACH debit instruction.

[17] Proposal at 31.

There are accordingly a few potential definitional changes that may address the challenges described above:

- Exclude "[f]acilitation of payments from a Regulation E account or Regulation Z credit card" from the definition of covered consumer financial product or service.
    - Entities that facilitate payments have consumer data, but as discussed *infra*, the data is incomplete, confusing, and potentially inconsistent with the data that exists with the provider of the covered Reg E or Reg Z accounts and
    - Pulling in digital wallet providers does not add to the universe of data available to users and consumers-–it is all inherently redundant of data that exists elsewhere, and it will add confusion to the data ecosystem.
- Clarify that a digital wallet provider "controls or possesses" the data only when the data relates to the product that the digital wallet provider or neobank offers to the consumer. Pass-through wallets are merely a record of the underlying data provider's account, and that record is not related to the product being provided to the consumer.

Beyond these definitional clarifications, the Bureau should further consider extending the implementation timeframe for digital wallet providers to ensure final definitions for open banking purposes align with other rulemakings involving this category of providers, including through the payments company larger participant rule and FCRA amendments. Similar to our suggestions above, while FTA champions the benefits of open banking in the U.S., we think it is most important that we collectively get this "right," including by ensuring clear and consistent coverage, definitions, and regulatory expectations. Given the ill-defined and fast-evolving concept of digital wallet in financial services, we believe that definitional clarity is paramount.

VI. The Bureau should implement a number of additional amendments and clarifications to the final rule to ensure successful and consumer-centric implementation of open banking in the U.S.

A. Clarify the interplay of Section 1033 with the Bureau's proposed FCRA rulemaking and confirm that data aggregators are not de facto credit bureaus.

The Proposal raises whether certain FCRA requirements might be applicable in the context of Section 1033 implementation. The Bureau should firmly establish that consumer-permissioned data is not subject to the FCRA for two primary reasons. First, the fact that a consumer owns the data and is controlling its movement distinguishes it from the FCRA context and the risks the FCRA seeks to mitigate. The FCRA was enacted to provide greater visibility and protection to consumers when it came to information being shared about them. But consumer-permissioned

data, particularly given many of the additional protections in the proposed rule, puts the consumer in charge. Second, unlike the FCRA context, under Section 1033, it is the consumer who is permissioning the transfer of his or her information. In this way, it is more akin to a customer providing a bank statement as part of an application for a home mortgage.

Additionally, in ensuring cohesion and consistency between the Section 1033 rulemaking and the FCRA rulemaking, the Bureau should expressly state that sharing of consumer information between entities—potentially through a data aggregator—is generally outside the scope of a consumer reporting agency. Merely summarizing, or reiterating data about a consumer, even in a different format but without adding any insight or additional information, should not be considered "assembling" or "evaluating" under FCRA, particularly when it is customer-authorized. Inappropriately capturing mere transmission activity would have significant impacts for the industry and impose substantial operational costs on covered firms, particularly those who only pass information on.[18] It is accordingly imperative that the Bureau consider and clarify the interplay between its ongoing rulemakings to ensure consistency and avoid unnecessary burden.

B. Avoid overly prescriptive disclosure requirements and ensure such disclosures are not used by data providers to dissuade or discourage a consumer from seeking a personal data transfer.

FTA supports the Proposal's avoidance of prescriptive disclosure requirements in favor of principles that can help ensure consumers have access to clear information needed to make informed decisions. FTA believes that consumers should be provided with clear, plain language disclosures, including with respect to the collection, sharing and use of their personal financial information. These disclosures should not be over-engineered, overly-prescriptive, or needlessly impede the user's experience. FTA notes that existing UDAAP and related disclosure rules provide a sufficient framework within which providers can offer consumers clear disclosures.

FTA opposes the required use of model forms for some or all of the content in authorization disclosures—we accordingly support the Bureau's current principles-based approach in the Proposal. The over-engineering of disclosures can have the unintended effect of reducing the likelihood that consumers will review such disclosures or appreciate potential distinctions in disclosure language.

While overly formalistic and prescriptive disclosure requirements should be avoided, the Bureau should encourage an SSO to promulgate disclosure standards and guidelines that can ensure that

[18] *See* Financial Technology Association, *FTA Comment on the CFPB's Outline of Proposals and Alternatives Under Consideration Related to the Rulemaking on Personal Financial Data Rights* (Jan. 25, 2023), available at https://www.ftassociation.org/wp-content/uploads/2023/01/FTA-1033-SBREFA-Comment-Letter-vF.pdf.

certain baseline information is provided to consumers. These guidelines can help all stakeholders craft appropriate disclosures tailored to their particular business model, product or service, and information sharing arrangements. SSO guidelines should further discourage data providers from using disclosures to needlessly create friction for consumers and barriers to them sharing their personal financial information. In no way should disclosures be used for anti-competitive purposes, including dissuading or discouraging a consumer from authorizing the sharing of their data.

C. Establish clear standards around the use of Tokenized Account Numbers to avoid anticompetitive behavior, the undermining of fraud models, and barriers to further innovation in business models.

The Bureau's Proposal currently allows a data provider to transmit tokenized account numbers (TANs) in lieu of non-tokenized account and routing numbers, ostensibly to reduce fraud risks. The Proposal offers no discussion of the use of TANs, but does ask for public comment, including with respect to the impact on consumers and potential need for standards.

FTA urges the Bureau to proceed with caution in allowing the use of TANs absent standards issued by a recognized SSO. While TANs may be used by some providers to mitigate certain fraud risks, they also may serve as a barrier to consumers accessing basic account information and to other providers working to counter fraud and other forms of financial crime. Account and routing information are critical forms of identifying information, and their obfuscation accordingly undermines many common anti-fraud practices. Security of information is better protected through sound API-security standards rather than through standardless tokenization.

Indeed, blanket Bureau permission to use TANs hands excessive power to data providers to restrict applications in anticompetitive ways. It further can chill consumer-centric innovation, including novel payments use-cases, such as account-to-account payment methods.

Rather than the current approach in the Proposal, FTA urges the Bureau to delegate discussion and standards regarding TANs to a recognized SSO, where market participants can ensure an optimal balance between security and maximizing the value of the open banking framework. Consumers should not be blocked from basic identifying account information and third-parties should be able to use such information to help counter fraud and innovate with pro-consumer product offerings.

* * *

FTA appreciates the Bureau's consideration of its comments. We believe that properly implemented, open banking in the United States can drive exciting pro-consumer innovation and competition in financial services. While we are all eager to see this new reality, we equally believe in getting this right in order to build consumer trust and maximize the potential of Section 1033. Our feedback is intended to focus on the consumer and the safeguarding of consumer interests. To this end, we would be happy to discuss the issues raised in this letter further. Please contact the undersigned at penny@ftassociation.org for additional information.

Sincerely,

Penny Lee
President and Chief Executive Officer
Financial Technology Association