Submitted via electronic mail
January 25, 2023

Comment Intake—Financial Data Rights
Consumer Financial Protection Bureau
1700 G Street, N.W.
Washington, D.C. 20552

Re: FTA Comment on the CFPB's Outline of Proposals and Alternatives Under Consideration Related to the Rulemaking on Personal Financial Data Rights

The Financial Technology Association[1] appreciates the opportunity to provide feedback on the CFPB's "Outline of Proposals and Alternatives Under Consideration" related to its rulemaking to 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.[2] We accordingly applaud the Bureau's commencement of the Section 1033 rulemaking process and look forward to serving as a resource.

FTA champions the transformative role of financial technology for American consumers, businesses, and the economy. A core pillar of the 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, speed access to funds, improve transparency and convenience, and enhance financial inclusion.

[1] FIN. TECH. ASS'N, www.ftassociation.org (last visited Jan. 20, 2023). FTA's members include Afterpay, Betterment, Block, Bluevine, Brex, Carta, Earnin, Figure, Intuit, Klarna, Marqeta, MoneyLion, MX, PayPal, Plaid, Ribbit Capital, Stripe, Truework, Wise, ZestAI, Zilch, and Zip.

[2] 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 digital 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.

I. Three Core Principles Should Guide Section 1033 Implementation

As the Bureau proceeds with the section 1033 rulemaking process, it will be important to anchor this important work to clearly identified principles. To this end, FTA suggests the following principles as critical to guiding the development of a personal financial data right capable of best serving and safeguarding consumer interests. These principles will consistently be referenced and reinforced in our responses below to the topics and questions raised in the Bureau's Proposal.

A. Focus on Consumer-centric Implementation

As the Proposal rightly makes clear, the purpose of a new personal financial data right is to promote consumer interests. The touchstone of the final rule, therefore, should be fostering competition and 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 will mean looking to expand the scope of data coverage, where possible, and allowing for consumer-centric use of such data, subject to clear disclosure and consumer consent, as well as robust privacy and security safeguards.

B. Avoid Anti-Competitive Behavior (by Those Holding Data)

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 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 sharing of financial data, restrict data parity, and advance anti-competitive objectives. As discussed in greater detail below, these efforts could occur in the context of limiting categories of covered data, blocking safe forms of data collection and sharing, delaying or impeding access verifications, suggesting application of duplicative supervisory frameworks, and calling for onerous and inefficient disclosure and consent mechanisms.

C. Leverage Existing Frameworks and Technologies, Where Possible

Given the potential complexity of implementing Section 1033, FTA suggests the importance of incorporating existing regulatory frameworks, where possible, to avoid creating new, untested requirements that may delay implementation, increase uncertainty, or complicate compliance. Similarly, the rulemaking should leverage available technologies—while encouraging further development and innovation—in order to afford consumers a secure and seamless user experience. This principle applies in numerous contexts, including with respect to incorporating existing data security regulatory frameworks, disclosure and consent requirements, and data sharing technologies capable of safeguarding data and consumer information. As detailed in our responses below, incorporating existing, well-understood regulatory frameworks and technology solutions can help simplify, streamline, and effectuate Section 1033 implementation.

To that end, in the following sections we respond to key topics raised in the Proposal, including:

---

[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 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/.

- First, we discuss the importance of ensuring that consumers always have access to their data, including through third-party access portals and via secure API or permissioned login approaches;
- Second, we recommend that the Bureau explore a phased approach to expanding covered accounts in order to empower consumers with a more holistic view of their financial health and with access to a broader range of tailored products and services;
- Third, we detail the importance of data parity so that consumers, regardless of their current financial services providers, have access to the same data, subject to key performance standards;
- Fourth, FTA underscores the importance of offering consumers clear and plain language disclosures so that they can make informed decisions regarding the use of their personal financial data;
- Next, we support application of existing data security regulations in order to safeguard consumer data and propose a process for supervising certain larger participants; and
- Finally, we suggest clearly distinguishing between Section 1033 and certain requirements applicable in the FCRA context.

II. The Bureau Should Ensure All Consumers Have Access to Their Data, Including through Secure Third-Party Access Portal Technologies

A. Modern Permissioned Login Approaches Provide Important Data Security Safeguards

Open banking is rooted in the acknowledgement that consumers own their financial data and should have the right to share it with another financial service provider to access various financial benefits. The Proposal outlines considerations regarding "third-party access portal(s)," through which consumers can authorize covered financial data to be sent once they have selected a financial application or services provider. As the Proposal notes, there are currently two broad technological approaches for such data portals, including via data-sharing agreements facilitated through secure application programming interfaces (APIs)[4] and through so-called "screen scraping," whereby the consumer provides the third-party access portal with login credentials (username and password) to access the covered data.

[4] It is worth noting that not all APIs come with a required data-sharing agreement; some allow broader access and instead include a terms of use agreement.

Given ongoing technological and security improvements with this latter approach, as well as contractual relationships between banks and data aggregators that carefully govern the transfer of information, we will use the term "permissioned login" rather than the potentially derogatory term "screen scraping." We encourage the Bureau to adopt this updated and more accurate terminology.

FTA further suggests that as the Bureau assesses API and permissioned login technologies, it centers the analysis on the principle that implementation of Section 1033 should be consumer-centric and in the consumer's best interest. To this end, FTA urges the Bureau to revisit historical concerns with permissioned login approaches given advances in safeguarding sensitive consumer information and recognize time, cost, reliability, and scope of data limitations to immediate and complete adoption of APIs.

More specifically, over the last few years, data platforms have worked in coordination with many of the largest financial institutions to move away from permissioned login approaches to instead share consumer-permissioned data over APIs. FTA believes that the use of secured APIs is an optimal long-term approach to facilitating the sharing of consumer financial data.

That said, permissioned login approaches generally serve as a fallback option when a financial institution does not have an API, which is common for smaller institutions. Permissioned login may also be a fallback option when APIs fail to operate as expected or are subject to other unexpected interruptions. For these reasons, it is in the clear best interest of the consumer for the Bureau to allow for the use of properly safeguarded permissioned login approaches in order to ensure that some consumers are not left out of being able to permission the sharing and use of their own data.

FTA believes, however, that the use of permissioned login approaches must be subject to appropriate safeguards. Fortunately, and consistent with the principle identified above regarding the incorporation of existing solutions, significant advances in permissioned login technologies have helped mitigate previously identified risks. For example, third-party data portals are now able to encrypt and tokenize login credentials to reduce the risk that sensitive information is inadvertently accessed. Providers also commonly separate collected login credentials, including personal identification information and passwords. Additionally, multi-factor authentication for an initial consumer authentication can help reduce the risk of malicious actors gaining access to

consumer information. These advances render permissioned login approaches a secure and viable alternative to APIs, especially when such APIs are unavailable.

B. The Bureau Should Encourage Adoption of API Integrations, Recognize Secure Permissioned Login Approaches as a Viable Alternative in Certain Scenarios, and Minimize Exceptions to Implementation Requirements

While FTA believes that permissioned login approaches should remain viable, especially in situations where APIs are not offered or are not available, we urge the Bureau to focus on encouraging third-party providers to increase API integrations and performance rather than imposing limits on permissioned login approaches. This is critical in ensuring that implementation of Section 1033 is in the consumer's best interest and does not disadvantage those whose primary providers are not able to integrate API solutions.

To this end, small banks and financial institutions are most likely to require substantial time in implementing APIs and should be able to rely on permissioned login approaches until they have API capabilities. One approach to staggering API implementation timelines is to segment FIs based on total assets, with the smallest entities having the most time to meet stated Bureau targets. The Bureau should also consider requiring adoption of the permissioned login best practices noted above that can help safeguard consumer information. And, as noted above, the Bureau should always allow for permissioned login approaches to serve as a fallback option for consumers in the event APIs are not available.

C. The Bureau Should Require Development of Industry Technology Standards that Satisfy Clear Outcomes and Performance Requirements

FTA believes that given the dynamic nature of innovation related to API technologies, it is important that prescriptive regulatory requirements not inadvertently box-in or limit ongoing consumer-centric development of these technologies. A lack of sufficient regulatory guidance, on the other hand, may result in industry disagreements regarding the establishment of appropriate standards.

For these reasons, we caution against prescriptive regulatory rules regarding API technologies, and instead urge the Bureau to require industry standards-development in service of consumer rights by establishing clear baseline principles and expectations that those standards must meet.

An example of a critically important, consumer-centric principle that should be embedded in final standards is the concept of parity between access approaches—the same information, data features and elements should be available to the consumer regardless of whether the information is sent via permissioned login or API. By creating a principles-based framework for required industry standards setting, the Bureau can ensure that API technologies continue to be developed in service of consumer interests. As discussed in further detail below, the Bureau can help facilitate this standards development by setting a deadline for such development,[5] explicitly recognizing that compliance with industry standards would be deemed compliance with Section 1033, and by establishing forums to advance standards development.

III. The Bureau Should Pursue Broad Coverage of Section 1033 to Include Accounts and Activities that Can Give Consumers a Holistic View of Their Financial Health and Help Them Access Improved Products and Services

A. The Bureau Should Explore Its Ability to Expand Covered Accounts and Activities in Subsequent Implementation Phases

As a threshold matter, the Proposal suggests that the products and services offered by covered providers that would be subject to the rule's information sharing requirements would include transaction (or "asset") accounts, including prepaid accounts, as well as Regulation Z credit card accounts (collectively "covered accounts").[6] FTA is supportive of this initial coverage, though believes that consistent with the principle of pursuing the consumer's best interest, it is important that the Bureau explicitly establish a phased approach to increasing coverage to include a broader range of accounts related to additional products and services.

[5] The Bureau might, for example, consider fallback requirements in the event industry standards are not promulgated and accepted by a certain date.

[6] CFPB, *Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights: Outline of Proposals and Alternatives Under Consideration* (Oct. 27, 2022), pp. 11-12, available at https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf.

Consumers will enjoy the greatest benefit from Section 1033 to the extent that it provides consumers a holistic ability to assess financial health and wellness, as well as shop for the broadest range of financial products and services. The more accounts that are covered by this rulemaking's information-sharing requirements, the greater the ability for consumers to accomplish these key objectives. As detailed further below, collection and use of financial data must be controlled and permissioned by the consumer, who is affirmatively seeking particular products and services.

FTA accordingly encourages the Bureau to consider phased inclusion of a range of financial accounts, including brokerage, savings and pension funds, government benefits, payroll, telecom, utility, and government-related accounts, which can provide, for example, benefits information and social security data. As a predicate to this phased approach to adding additional financial accounts, the Bureau should assess its legal authority to broaden its scope of coverage and engage with industry stakeholders regarding their experiences with open banking frameworks in other key jurisdictions, including the UK and EU.

With respect to the first, current, phase of the Section 1033 rulemaking, the Bureau should ensure that payment initiation services are enabled by proper information sharing. It is important that account information sharing is paired with payment initiation services in order to provide consumers with access to cheaper, more convenient payments solutions, as well as to advance fraud prevention strategies. More specifically, consumers can be empowered with the ability to pay securely and directly from a payment account, via API, if requisite account information is shared with the payment provider.

B. The Bureau Should Narrowly Apply Exemptions to Covered Account Providers

The Proposal discusses potential approaches to exempting certain covered account providers. FTA recommends that any such exemptions be narrowly applied given the clear consumer benefit of having financial providers subject to data sharing requirements under Section 1033. The development of secure data-sharing technologies, including APIs, and availability of third-party data portals will increasingly render compliance with Section 1033 feasible for financial providers.

With respect to authorizations for data sharing, in order to increase implementation efficiency, FTA recommends that not all account holders should be required to authorize data if terms clearly

disclose that any account holder can provide such authorization. Requiring all account holders to authorize would delay data sharing, increase costs, and introduce potential confusion.

IV. The Bureau Should Ensure that Broad Categories of Data Are Available to Consumers, Subject to Data Parity Requirements, in Order to Provide Consumers with Expanded Product and Service Offerings; Practical Exceptions to Coverage Should Be Narrowly Construed

A. Key Categories of Data Can Unlock Enhanced Services for Consumers and Help Counter Fraud

As a threshold matter, FTA is strongly supportive of the CFPB's proposed categories of data required for production by data providers and supports inclusion of all categories and fields listed on pages 18-23 of the Proposal. Based on some FTA members' experience with overseas open banking implementation, however, FTA suggests that the Bureau detail and define mandated data elements that data providers must make available in order to ensure that certain FIs do not use discretion to limit sharing, as has been observed in other markets. This will support satisfaction of the overarching principles noted above, namely that implementation of Section 1033 be in the consumers' best interest, that FIs ensure data parity regardless of the access approach or whether the data goes directly to the consumer or to a third-party, and that data holders do not otherwise pursue anti-competitive efforts to restrict or limit access to consumer personal financial data.

To this end, the Bureau currently proposes that it would require data providers to make historical data available, free of charge, for the period of time that the provider makes such data accessible to the consumer on the provider's online account interface. The example suggests 36 months as a common benchmark for such availability. While FTA supports the concept that a provider should make available such historical data, we caution that FIs should not use this rule to begin limiting or reducing the date ranges made available to consumers on such online account interfaces in order to reduce what historical data they must share under this rulemaking. This would be an example of an FI effectively gaming the rule to the detriment of the consumer and for anti-competitive purposes.

To avoid this outcome, the Bureau should establish an appropriate monitoring and reporting structure, including outlining the ramifications of noncompliance, to ensure that an FI is not

improperly restricting or reducing the availability of any data categories, points, or elements. Going further, the Bureau should consider ways to require FIs to *expand* the data made available to consumers—and subsequently made available for sharing under this rulemaking—as technology and new products or services render such expansion reasonable.

Finally, with respect to data fields that should be explicitly included in the rulemaking, FTA highlights here three fields that could help combat fraud, namely in the payments context. First, the data provider should make available the "full name" of the customer, subject to formatting standards, in order to allow sending and receiving institutions to have confidence that the payment is being made to the intended recipient. Some older, traditional FIs have a very low character limit built on archaic architecture, which should be mandatorily updated to help combat fraud.

The second data field is "account type," subject to a clear, universal format for each account type through which a transaction is sent and/or received. More specifically, this would mean sharing whether an account is a business account, personal, checking, and/or savings, among other types of accounts. It would also include indication of what payment rails are available for such accounts (e.g., ACH, RTP, and/or FedNow) and how to distinguish between incoming and outgoing payments.

Finally, "account activity" should also be mandatorily shared, including the account number (to identify recurring connections), how long a customer has held an active account with a given provider, and the date of the last transaction. These data points can be crucial for machine learning algorithms to spot patterns in how bad actors operate and manage bank accounts, identify re-use of such accounts, and overall help tackle fraud more effectively.

B. Data Parity and Availability, Subject to Performance Standards, are Essential in Maximizing Consumer Benefit

The overarching principle that the implementation of Section 1033 should be in the consumer's best interest makes it critical that data should be made fully available and accessible to consumers by their banks—on the same footing among competitors—with key performance standards. This means that in order to avoid a degradation of service when transitioning from permissioned login approaches to APIs, data parity with the online banking interface is crucial, including with respect to common fields and uptime. In all scenarios, at least the same data should be present as in the

online banking interface, but it should also include additional key categories of information as outlined in the subsection above. Additionally, given the state of existing technology and implementation capabilities, APIs must satisfy an agreed industry standard with respect to uptime—and this performance standard should be specifically referenced within the rulemaking.[7]

With respect to additional permissioned login and API standards, as noted above, FTA encourages the Bureau to establish guidelines and principles that facilitate industry standards development. To this end, FTA recommends that the Bureau articulate clear expected outcomes that industry standards must help participants achieve, including data parity to avoid degradation of services as providers shift from permissioned login to API approaches. FTA further suggests that the Bureau leverage existing tools, including explicit recognition of well-crafted industry standards as satisfying Section 1033 and a potential subcommittee within an existing CFPB FACA committee to stimulate standards development informed by a broad group of stakeholders, including fintechs, third-party access portals, and traditional FIs.

Finally, the Bureau is considering whether to impose record retention requirements for covered data providers and authorized third parties. FTA recommends a three-year data retention period, unless otherwise required by law, as appropriate in balancing the costs of such a requirement with the benefits to consumers, including by ensuring that valuable consumer personal data is available to power innovation in financial products and services.

C. Statutory Exceptions Should Not be Used for Anticompetitive Purposes

The Proposal acknowledges a set of four statutory exceptions from making certain consumer information available under Section 1033. While FTA recognizes the need for compliance with these exceptions, we recommend that they are interpreted narrowly in order to prevent FIs from engaging in anti-consumer or anti-competitive behavior by relying on these exceptions in order to withhold broad sets of information. To the extent there are concerns regarding data privacy or security, such concerns should be appropriately addressed by existing regulatory frameworks and other sections of the Section 1033 rulemaking rather than inappropriately expressed through broad interpretation of these statutory exceptions.

[7] See, e.g., Financial Data Exchange (FDX), *Foundational Requirements for Data Providers* (Dec. 2020) (establishing a 99.95% uptime standard).

More specifically, "Confidential Commercial Information" should be limited to non-public information that does not relate to a specific consumers' identity, account, fees, charges, or transaction history, and should not be interpreted broadly for anti-competitive purposes. This exception should not be used to exclude any information that the consumer would be able to access or deduce through a direct connection to the provider, i.e., through its own website or app. Additional information that should never be withheld pursuant to an exception would include customer account and routing numbers. As noted above, concerns regarding privacy or data security should be properly addressed by specific privacy and security provisions in the Section 1033 rulemaking.

Additionally, FTA cautions that other exceptions to data production, including "any information collected . . . for the purpose of preventing fraud or money laundering" could also be broadly interpreted and abused by data providers at the expense of consumers, fraud mitigation efforts, and fair competition. While protection of certain sensitive risk information, including proprietary fraud or customer risk scores, may properly be subject to exception (though they are not necessarily collected), the Bureau should carefully assess whether particular information related to fraud is of greater overall value to reducing fraud by making such information available to be shared as compared to being withheld from disclosure. At the margins, FTA suggests that broad sharing of data within a well-regulated Section 1033 framework will do more to reduce fraud and other financial harms than provincial attempts to silo such data on the grounds that it is sensitive.

V. Consumers Should have the Ability to Understand How Their Data Will be Used, Permission the Use of their Data, and Benefit from Tailored and Innovative Products and Services

FTA members are among the world's leading financial technology firms focused on improving consumer financial services, outcomes, and opportunities. As noted above, financial data is often at the center of financial services innovation and its fair, transparent, and permissioned use is critical to driving ongoing consumer-centric competition and product development. To this end, FTA members take seriously their responsibilities and obligations to customers and view such commitments as essential to building long-term trust.

As part of these commitments, FTA recently 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. 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, as would be consistent with data minimization principles, (iv) plain language disclosures, and (v) non-discrimination.[8]

We note these principles as consistent with the overarching goals of Section 1033 and consistent with unlocking the full value of open banking for consumers. When presented with clear information on data use and practices, consumers are best positioned to authorize sharing and use of their financial data. To this end, prescriptive regulatory limitations and restrictions on data collection, retention and use would undermine consumer interests by reducing the ability of providers to develop new products and services and offer consumers increased competition with their legacy providers. Within this context, FTA provides further feedback on specific elements of the Proposal.

A. Consumers Should be Provided with Clear, Plain Language Disclosures

As noted above, FTA believes that consumers should be provided with clear, plain language disclosures to ensure they are able to make informed decisions, 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. Consistent with the principle noted at the outset of this comment letter that the rulemaking should incorporate existing standards and requirements, where possible, FTA notes that existing UDAAP and related disclosure rules provide a sufficient framework within which providers can offer consumers clear disclosures.

FTA accordingly opposes the required use of model forms for some or all of the content in authorization disclosures. The over-engineering of disclosures can have the unintended effect of reducing the likelihood that consumers will review such disclosures or appreciate potential

[8] Financial Technology Association, *FTA Privacy Principles for the Future of Finance*, available at https://www.ftassociation.org/fta-privacy-principles-for-the-future-of-finance/.

distinctions in disclosure language.[9] The Proposal's discussion of a potential certification requirement is similarly overly formalistic and would likely increase the risk that consumers will ignore or "click through" such disclosures. Additionally, such requirements may increase user friction and harm the consumer experience without evidence of a clear benefit.

While overly formalistic and prescriptive disclosure requirements should be avoided, the Bureau can ensure that certain baseline information is provided to consumers through the use of disclosure guidelines that outline key content or topics that should be included in a disclosure. These guidelines can help providers craft appropriate disclosures tailored to their particular business model, product or service, and information sharing arrangements. The Bureau should also provide guidelines that would discourage FIs from needlessly creating friction for consumers and barriers to them sharing their personal financial information, as well as fostering other anti-competitive behaviors.

B. Consumers Should be Trusted and Able to Make Informed Choices

Provided with appropriate, clear, and plain language disclosures, consumers should be trusted to make informed decisions regarding the duration, frequency, and use of a third party accessing their personal financial information. This approach is a bedrock of American law and norms, and it is essential for maximizing the benefit Section 1033 will provide to consumers by facilitating the ongoing development of innovative and tailored financial products and services. Prescriptive and paternalistic restrictions regarding how consumers are allowed to share and use their data would be antithetical to the purpose of Section 1033, chill innovation, and reduce overall consumer benefit.

To this end, overly restrictive requirements for the deletion of data and consumer reauthorization for sharing and using data should not interfere with access to the products and services consumers desire. With respect to consumer reauthorization, FTA suggests that the Bureau take note of the experience in the UK, where the FCA recently scrapped the prior 90-day reauthorization rule that required consumers to log into their banking account to reauthorize the ability of a third-party

[9] See generally Jeanne M. Hogarth and Ellen A. Merry, *Designing Disclosures to Inform Consumer Financial Decisionmaking: Lessons Learned from Consumer Testing*, Board of Governors of the Federal Reserve System: Federal Reserve Bulletin (Aug. 2011) (noting that "customization may more effectively highlight characteristics of different products or alert consumers when a familiar piece of information may have a different meaning"), available at https://www.federalreserve.gov/pubs/bulletin/2011/pdf/designingdisclosures2011.pdf.

provider to receive that account's information.[10] The FCA noted that the prior rule "creates friction . . . and increases the likelihood of customers dropping off."[11]

Instead of requiring a strong, repeated authentication for reauthorization within the primary account providing information, the FCA now allows reauthorization to occur within the third-party app. FTA supports this approach as consistent with the consumer's best interest; we further recommend that the Bureau allow the consumer to choose time periods for reauthorization within the third-party app (for example, 6 or 12 months) or to base the need for reauthorization on consumer latency if the connection is not used for a sufficiently long period of time (e.g. 6 months).

FTA further believes that consumers should have clear authorization revocation rights so that they can end the sharing and use of their personal financial data. FTA recommends that disclosure of this right be in the account and/or provided in a user experience reminder, rather than as part of a separate contact. This approach will increase ease of access for consumers and reduce friction when a consumer seeks to revoke an authorization.

Finally, to the extent that the Bureau considers deletion requirements of certain consumer personal financial data, FTA recommends a common-sense exception for anonymized information to be kept for research and innovation purposes. This type of data is critical to developing new products and services for consumers, can help develop fraud mitigation tools, and its ongoing retention and use would pose no harm to consumers.

C. Providers Should be Permitted to Use Data to Provide Improved Products and Services Based on the Permission and Informed Consent of Consumers

The Bureau's Proposal discusses potentially limiting a provider's access to and use of information (and duration and frequency of such access and use) to what is "reasonably necessary" to provide the good or service requested by the consumer. FTA cautions that without further guidance and discussion of this standard, it runs the risk of creating uncertainty for providers.

---

[10] Oliver Smith, *Open banking's '90-day' rule finally comes to an end*, AltFi (Oct. 3, 2022), available at https://www.altfi.com/article/9912_open-bankings-90-day-rule-finally-comes-to-an-end.
[11] PYMNTS, *UK's FCA Scraps 90-Day Reauthentication Open Banking Rule* (Dec. 2, 2021), available at https://www.pymnts.com/news/banking/2021/fca-scraps-90-day-reauthentication-open-banking-rule/.

More specifically, in offering a particular good or service—and further improving or tailoring such good or service—a provider may reasonably collect a broad range of data and data elements. Each such data element alone may not be "necessary" for the provision of a particular good or service, but taken together such elements become necessary to offering the good or service. For this reason, the Bureau 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.

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. The Bureau should make clear that data elements used to improve, develop, or innovate from an initial product or service offering are properly considered to be reasonably necessary. Given these business and design realities, absent clarification in the final rule, including potential examples, the term "reasonably necessary" would create uncertainty amongst providers and limit their confidence in using data to improve an offering beyond its essential components.

Based on the above, FTA recommends that the Bureau enhance certainty by publishing guidance on its expectations and examples related to such a "reasonably necessary" standard for data use. Additionally, the Bureau should consider how the requirement of clear disclosure regarding data use and informed consent can help to minimize regulatory concerns. To this end, we note that the GLBA allows FIs use of data that goes beyond a reasonable necessity standard, subject to disclosure and consent safeguards. This existing framework should inform Section 1033 implementation and can put providers on a level playing field when it comes to use of permissioned consumer financial data.

Consistent with this approach, FTA urges the Bureau not to overly restrict "secondary use" of financial data, especially when such use has been explicitly disclosed to the consumer and the consumer has provided informed consent. Potential secondary uses of financial data may include holistic consideration of the consumer's financial health and tailored recommendations for better products and services that may not be obvious when a consumer first engages a new provider. 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.[12] Both of these scenarios may be considered a "secondary use" of data. Restricting these types of secondary uses would violate the overarching principle that Section 1033 implementation should be in the consumer's best interest.

To the extent that there are potential secondary uses objectively deemed so harmful to consumers that it should override informed consent, only specific uses the Bureau so identifies should be precluded. For example, FTA believes 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 would be the appropriate way to address other risks highlighted by the Bureau in the Proposal, including with respect to the protection of sensitive data.

VI. Providers and Data Portals Should be Subject to GLBA Data Security Standards

Consistent with the overarching principle of incorporating existing frameworks that are fit-for-purpose, FTA believes that existing and well-established federal data security laws should serve as the relevant compliance frameworks for Section 1033. To this end, FTA members, for example, comply with various federal, state, and international data laws, including the Gramm-Leach Bliley Act (GLBA). It is our view that the GLBA applies to covered entities, including third-party data portals, and establishes the proper framework for compliance.

To this end, we agree with the Bureau that authorized third parties that seek to access consumer-authorized information are also subject to the GLBA safeguards framework, implemented by the FTC in its Safeguards Rule and by the prudential regulators in the Safeguards Guidelines. Compliance with these frameworks – as verified through an appropriate audit or certification framework – should satisfy any related security requirements under Section 1033 and would avoid confusion, duplication, or uncertainty resulting from additional requirements. Such compliance and certification would also reduce costs by eliminating the need for data providers to separately diligence a data recipient prior to sending authorized information. We note that requiring GLBA compliance is a common approach regulators are using to ensure consistency,

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

including in FinCEN's December 2022 NPRM on beneficial ownership registry access where the Agency proposes using such compliance as the standard in order to "avoid duplicative or inconsistent requirements for information security and protocols" for FIs accessing FinCEN's registry.

VII. Third-Party Data Portals Should be Subject to a Parallel Larger Participant Supervisory Rulemaking

FTA believes that third-party data portals should be supervised by the Bureau pursuant to its larger participant rule supervisory authority. This rulemaking, however, should run in parallel with Section 1033 supervision authorities (not separately) and should help create a consistent, harmonized supervisory regime.[13]

A key feature of CFPB supervision of third-party data portals is that this oversight should preempt or be deemed compliant with additional third-party oversight or requirements by the banking regulators. Bureau supervision should also obviate the need for banks to separately diligence compliance of supervised entities when engaging in activities under Section 1033. A failure to recognize that Bureau supervision effectively "fills the field" of necessary oversight would result in inefficient, costly, confusing, and duplicative compliance requirements.

VIII. Clarifying FCRA Distinctions

The Proposal raises whether certain FCRA requirements might be applicable in the context of Section 1033 implementation. We recommend that the Bureau 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 FCRA seeks to mitigate. 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.

[13] FTA strongly urges the Bureau not to rely on its section 1024(a)(1)(C) authority in order to avoid significant problems with a lack of notice and transparency for examined institutions.

IX. Consumer-Centric Implementation of Section 1033 Will Unlock Financial Choice, Competition, and Opportunity

Evidence from around the globe is showing that empowering consumers to manage and share their financial data is driving profound consumer benefits. In the UK – where the government recently developed an open banking regulatory framework – open banking is driving growth in the number of regulated third-party providers and increasing consumer choice. More broadly in Europe, open banking adoption has exceeded the pace of contactless payment adoption at the same stage of development and is growing with nearly 1 million new users every six months.[14] And in the U.S., the seamless and secure flow of permissioned data allows fintech companies to offer consumers tailored and improved services; a recent survey found that 73% of Americans say fintech gives them more control over their finances and 68% say it helps them reduce financial anxiety.[15]

Given this backdrop, FTA strongly supports the Bureau's efforts to move forward with its implementation of Section 1033, so that consumers can fully realize their right to control their personal financial data. By adhering to the overarching principles established at the outset of this comment letter, the Bureau can ensure that consumers enjoy maximum benefit of this right, while safeguarding against potential risks. We appreciate your consideration of our comments and would be happy to discuss any of the ideas raised herein with you further.

Sincerely,

Penny Lee
Chief Executive Officer
Financial Technology Association

[14] PYMNTS, *Open Banking Bumpy but Adoption Curve Better Than Contactless Payments* (May 23, 2022), available at https://www.pymnts.com/news/banking/2022/open-banking-bumpy-but-adoption-curve-better-than-contactless-payments/.
[15] Plaid, *2020 Fintech Report: The Fintech Effect* (2020), available at https://plaid.com/documents/the-fintech-effect-2020-consumer-report.pdf.