www.fdata.global/north-america

January 25, 2023

Comment Intake
Consumer Financial Protection Bureau
1700 G Street NW
Washington, D.C. 20552

SENT VIA ELECTRONIC MAIL TO Financial_Data_Rights_SBREFA@cfpb.gov.

Re: Outline of Proposals and Alternatives Under Consideration for SBREFA: Required Rulemaking on Personal Financial Data Rights

The Financial Data and Technology Association of North America ("FDATA North America") appreciates the opportunity to provide its perspectives in response to the Consumer Financial Protection Bureau's ("CFPB" or "the Bureau") outline of proposals and alternatives under consideration for the Bureau's Small Business Regulatory Enforcement Fairness Act ("SBREFA") panel that will inform its rulemaking implementing Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("the Dodd-Frank Act").

FDATA North America was founded in early 2018 by several financial technology firms whose technology-based products and services allow consumers and small and medium enterprises ("SME") to improve their financial wellbeing. As the leading trade association advocating for customer-permissioned access to financial data, FDATA North America's members include firms with a variety of different business models. Collectively, our members provide more than 100 million American consumers and SMEs access to vital financial services and products, either on their own or through partnerships with supervised financial institutions. Regardless of their business model, each FDATA North America member's product or service shares one fundamental and foundational requisite: the ability of a customer to actively permission access to some component of their own financial data that is held by financial services providers.

Introduction

As a trade association that represents dozens of financial technology companies that are focused on enabling greater competition and choice in the financial services marketplace, we believe that a broad rulemaking implementing Section 1033 of the Dodd-Frank Act will create more competition, lower prices and fees, and improve access to the financial services marketplace. At the center of such a framework must be an unambiguous and legally binding customer financial data right, which will ensure that consumers and small businesses could easily shop for financial services and products among scores of potential providers in an open, transparent marketplace in which they at all times have the ability to access and permission access to elements of their financial data.

Of course, it is not sufficient to merely provide end users with access to their financial data. While such access is highly valuable to a consumer who lacks the ability to see the totality of what they have and what they owe across multiple accounts, the ability of the end user to act based on this data access is an essential element of any open banking ecosystem. As a result, a Section 1033 rulemaking through which customers can easily switch between the providers of products, services and tools most appropriate for their unique financial position represents, in our view, represents the best outcome of the Bureau's ongoing rulemaking process.

This ability of any customer to easily select or switch between providers of goods or services is the foundational element of market competition, which in turn reduces the price of the good or service for customers. Through various statements and orders, the Biden Administration and the Bureau have made it clear that they believe increased centralization and weakened competition within the financial services marketplace has led to worsening customer value, fewer choices, and increasing prices.

For far too long, U.S. consumers and SMEs have faced significant difficulty switching from one financial provider to another due to friction caused by a system that has historically exerted barriers to doing so. To wit: a recent study found that the average American adult has used the same primary checking account for more than 14 years.[1] The status quo, under which financial institutions exercise control over their customers' data, and, in some cases, limit the ability of their customers to utilize their own data to shop for alternative providers, offers little benefit to the consumer or small business. While, in some cases, financial institution throttling or blocking of third-party tools may be positioned as being based on security or regulatory compliance postures, competitive concerns unquestionably have fueled some of this behavior as well. In these instances, the end user typically is unaware as to why the product or service they are trying to use – or even have depended on for their financial wellbeing in the past – is not functioning or supported.

In an attempt to tackle mounting market concentration, President Biden issued in July 2021 an Executive Order on Promoting Competition in the American Economy. Included in the Executive Order was a directive for the Bureau to consider "commencing or continuing a rulemaking under Section 1033 of the Dodd-Frank Act to facilitate the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new, innovative financial products.[2]" This encouraging statement from the White House clearly demonstrated that the establishment of a customer financial data right is a priority for the administration, and one that FDATA North America and its members strongly support.

The current lack of a legally binding customer financial data right in the U.S. sees competition in data-driven financial services stifled by financial institutions that in some cases may override

[1] Mary Wisniewski, *Survey: While checking fees vary wildly by race and age, Americans stay loyal to their banks*, Bankrate (Jan.15, 2020).
[2] White House Executive Order on Promoting Competition in the American Economy. July,9 2021.

customer direction to authorize sharing of their financial data. These restrictions include broad, as well as specific, attempts to directly limit third parties' access to data despite customer authorization; degradation of data sharing that effectively thwarts customer-directed access to financial data; and self-imposed mandatory reauthentication requirements and targeted blocking of sharing specific data fields in ways that effectively disable competing services. This unlevel playing field has, to date, been dictated by opaque bilateral data access agreements between financial institutions and aggregation firms that enumerate what choices customers have to utilize their own financial data and the protections they are afforded when they do so. These barriers artificially stifle both customer choice and marketplace competition, and create an environment in which fees charged to end users may stay stagnant – or even increase – over time.

Competition issues cannot take a back seat as the regulatory and technological framework in customer-permissioned data sharing continues to evolve. FDATA North America and its members have long advocated for a regulatory approach that facilitates the sharing of data by customers with, and between, their financial service providers, based on consent and with safeguards for privacy and security. Systems that achieve these objectives have been implemented in the United Kingdom, Australia, New Zealand, and several other countries. The success of these regimes, including increased competition in the financial services market, has motivated other countries, including both Canada and Mexico, to pursue similar frameworks. Unlike this growing list of other large economies across the globe, the U.S. currently lacks any distinct legal assertion of a customer's legal right to access and permission access to their financial data.

However, even in the absence of a legally binding customer financial data right, U.S. consumers and SMEs have enjoyed some level of increased competition for financial services in recent years, including for products driven by their ability to permission access to their own financial data. These services allow customers to take greater control over their financial lives and opportunities: to find new sources of affordable credit based on innovative underwriting models, to initiate payments to friends, family and vendors in real time and without fees, and to help manage their financial outlook across multiple accounts and plan effectively for the future, to name a few. As the Bureau notes in in its SBREFA outline, however, these opportunities to access third-party financial services tools, products and services are not ubiquitous, and the ability of a consumer or SME to utilize such third-party services differ depending on the financial institution with which they bank. In a time of enormous economic uncertainty, these services are more important than ever to help consumers and SMEs navigate difficult financial circumstances.

The Growing Financial Services Marketplace

Innovation in the financial services marketplace over the last several years has been powered principally by customers' ability to permission access to and to use their financial data, often in conjunction with cutting edge machine learning and other data analytics technology. Much of

this financial data is associated with consumers' and SMEs' transaction history at their existing accounts with financial institutions.

A July 2018 U.S. Department of the Treasury report demonstrated this growth, showing that from 2010 to the third quarter of 2017, more than 3,330 new technology-based firms serving the financial services industry were founded, and the financing of such firms reached $22 billion globally in 2017.[3] Accenture has estimated that investments in fintech companies reached $53 billion globally in 2019.[4] As of 2018, lending by such firms made up more than 36% of all U.S. personal loans, up from less than 1% in 2010.[5]

Moreover, "survey data indicate that up to one-third of online U.S. consumers use at least two fintech services — including financial planning, savings and investment, online borrowing, or some form of money transfer and payment"[6] – which compete directly with traditional financial institutions' products. In 2020, for example, *Forbes* listed a dozen personal finance startups among its top 50 fintech companies.[7] As the 2018 Treasury report notes, some digital financial services reach up to 80 million members, while financial data aggregators can serve more than 21 million customers.[8]

These more recent market entrants compete both with each other and with traditional depository financial institutions to provide innovative financial products that greatly benefit consumers, including by lowering costs and expanding access by filling gaps in the market. The direct line between competition and innovation is well-chronicled, as the Treasury report noted:

The increasing scale of technology-enabled competitors and the corresponding threat of disruption has raised the stakes for existing firms to innovate more rapidly and pursue dynamic and adaptive strategies. As a result, mature firms have launched platforms aimed at reclaiming market share through alternative delivery systems and at lower costs than they were previously able to provide. Consumers increasingly prefer fast, convenient, and efficient delivery of services. New technologies allow firms with limited scale to access computing power on levels comparable to much larger organizations. The relative ubiquity of online access in the United

---

[3] U.S. Treasury, *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation* (July 2018).

[4] Michael Del Castillo et al., *The Forbes Fintech 50: The Most Innovative Fintech Companies In 2020*, Forbes (Feb. 12, 2020).

[5] Treasury Report at 5.

[6] *Id.* at 18.

[7] Kelly Anne Smith, *The Future of Personal Finance: Fintech 50 2020*, Forbes (Feb. 12, 2020)

[8] Treasury Report at 5.

States, combined with these new technologies, allows newer firms to more easily expand their business operations.[9]

Unfortunately, much of this transformative potential remains stifled in the U.S. as a result of a lack of a legally binding customer data right. Experience in the United Kingdom, however, where open banking has been a reality for more than four years, demonstrates that the Treasury report's linkage between competition and innovation is anything but theoretical. According to the U.K. Open Banking Implementation Entity, more than six million customers are now regular users of open banking-enabled tools, representing growth of more than one million new active users in less than six months. At the end of 2021, cumulatively over 26.6 million Open Banking payments were made in the U.K., an increase of more than 500% in just 12 months.[10]

Moreover, the availability of services continues to expand. Adoption has continued to grow, with 10 – 11% of digitally-enabled consumers now estimated to be active users of at least one open banking service. This is up from 6 – 7% in March 2021.[11] The U.K. Open Banking Implementation Entity also found that these services have helped consumers save more and build a financial cushion, with 22% saying that an Open Banking empowered savings app was their first adult savings account, and revealed that 91% of consumers found Open Banking-enabled financial services easy to setup, and 76% intend to continue to use them[12] Most relevant to the underlying purpose of the Bureau's decision to move forward with a Section 1033 rulemaking, recent U.K. data has shown a consistent *increase* in the number of financial services providers, bucking trends of market consolidation in other sectors and driving down prices for customers.[13]

General Comments on SBREFA Outline

FDATA North America congratulates the Bureau on proposing a legally binding consumer data portability right that covers some financial data that is currently available to consumers via their online banking portals. We have long advocated for a customer-centric open finance regime in the U.S. with appropriate regulatory oversight to ensure consumer and SME protection. Such a framework should, in our view, include supervisory oversight of financial data aggregators by the Bureau. A well-designed open finance system should also include minimum governance requirements for third-party financial technology applications, clear lines of regulatory jurisdiction and supervisory expectations for all industry stakeholders.

Areas We Firmly Support

[9] *Id*. at 6.

[10] UK Open Banking Implementation Entity (OBIE) "Five Million Users-Open Banking Growth Unpacked." (Dec 2021)

[11] UK Open Banking Implementation Entity (OBIE). The Open Banking Impact Report June 2022.

[12] UK Open Banking Implementation Entity (OBIE): "The Open Banking Impact Report." (Oct 2021)

[13] Statista.com. UK: number of regulated open banking providers. (Sept. 2021)

We are encouraged by the framework the Bureau is contemplating in this outline. While we intend to focus the majority of our response to the SBREFA outline on those areas where the Bureau is specifically seeking feedback, we would first like to commend certain elements of the eventual Section 1033 rulemaking discussed in the SBREFA outline that we believe are particularly important. These include:

- A legally binding requirement that data holders must provide their customers the right to access and share access to non-proprietary data elements that are available to them today either online or in print, including historical transaction data, when proper authorization has been granted. We particularly applaud the Bureau's inclusion of data fields such as account number and fees as covered data, which are integral to several critical customer use cases, and which are not universally available for customers to share with third parties in the marketplace today.

- Recognition that data providers should not be permitted to determine whether a third party, which has received customer authorization and meets minimum cybersecurity requirements, may or may not access that customer's financial data. In the absence of a Section 1033 rulemaking, such restrictions exist today stymie the ability of customers to access important products or tools that can improve their financial wellbeing.

- Recognition that significant progress has been delivered by the market to date in transitioning from legacy technology towards dedicated data access portals implemented by data providers. We appreciate the Bureau's technology-agnostic approach in the SBREFA outline, its framework around data access portal reliability and usability metrics, and its acknowledgement that the transition from credential-based screen scraping to dedicated data access portals could represent a challenge for smaller financial institutions. We share the Bureau's view that a comprehensive shift away from a dependence on credential-based data access would best serve and protect customers over the long term. The Bureau should acknowledge, however, that credential-based data access must continue as an option when no alternative exists, and as a backup option for all third parties when third party portals do not function, experience latency, or fail to provide all of the necessary data. We strongly support the proposals included in the Bureau's SBREFA outline to set forth standards regarding functionality and availability of dedicated data access portals, and the data points proposed to be required.

- A proposed framework that includes minimum data security, data privacy, and risk management standards for any authorized third party that accesses customer-permissioned financial data, based on the principle of data minimization, under which only the data that is required to deliver the use case selected by the customer may be accessed. The U.S'. patchwork of state-led data privacy and protection regimes has historically created obstacles to enabling a true open banking regime under which uniform consumer privacy controls exist regardless of whether consumers choose to work with a financial institution or a third-party

provider. Across the globe, customer protection is a foundational element of open banking frameworks and rightfully should underpin a Section 1033 rulemaking.

Areas Needing Further Consideration

Overall, the SBREFA outline envisions a rulemaking that would meaningfully improve customer-permissioned data access and competition in the financial services sector, and we applaud the Bureau for its diligent and thoughtful work over the last several years that has led to this point. To fully meet the Bureau's stated policy goals in moving forward with a Section 1033 rulemaking, however, we believe the CFPB should consider addressing the following issues in its eventual Section 1033 proposed rule:

- The scope of covered account types is too narrow. The Bureau's SBREFA outline proposes to cover only consumer deposit, transaction and credit card accounts. While we understand that the Bureau proposes this limited scope as a starting point, FDATA and our members would strongly urge inclusion of small business, payroll, and investment accounts, providers of government benefit accounts used to distribute needs-based benefits programs, other types of non-transaction accounts at financial institutions, including mortgages, auto loans, and all forms of time deposit accounts. Our member companies currently provide tens of millions of U.S. consumers access to these non-covered data types, and they would be at risk of losing such access were it not guaranteed under 1033.

- The proposal does not include our long-advocated position that the Bureau should extend its supervisory authority to data aggregators.

- The outline does not differentiate between customer-identifiable data and de-identified data. Limitations on how data may be utilized under Section 1033 should focus more expressly on customer-identifiable data, recognizing that de-identified data has significant value across the ecosystem, including for research and product enhancements, among many others.

- The Bureau seems to believe that its December 2021 updates to its Electronic Financial Transaction Act Frequently Asked Questions[14] and existing Regulation E guidance on liability are sufficient to cover the account types in this proposal. While we agree with this as a starting point, if the scope of covered account types is expanded as we suggest, similar liability principles should be considered for these accounts as well. In any case, we strongly support the underlying principle that the entity responsible for a data breach that causes financial loss to an end user should be responsible for making that end user whole, and that data providers should not be able to claim liability concerns as a means of restricting data access.

[14] CFPB Compliance Aid. Electronic Fund Transfers FAQs

- Alternatives for credential-less data access and fallback connectivity methods require further development. It is critical for the Bureau to develop a Section 1033 rule that promotes progress toward credential-less data access methods, while temporarily allowing the continuation of credential-based screen scraping as a permissible option. In 2023 the vast majority of U.S. financial institutions have not developed credential-less forms of data access, such as tokenized account access or dedicated data access portals, and as such continue to rely exclusively on credential sharing methods.

- As a practical matter, the timeline for implementation for credential-less data access needs to be calibrated based on financial institution size.

- The ability of data providers to challenge customer authorization to third parties needs more elaboration to avoid data holders using this as a rationale to block from accessing their own data or sharing it with third parties of their choosing.

Detailed Responses to Proposals Under Consideration

A. Coverage of data providers subject to the proposals under consideration.

Questions 5-10. The Bureau proposes in its SBREFA outline to apply a Section 1033 rulemaking to asset and transaction accounts covered under Regulation E and Regulation Z, and notes that it "intends to evaluate how to proceed with regard to other data providers in the future." It is our view that this limited interpretation presents material risks of both failing to unleash the full potential of a customer data access right and impacting a litany of existing use cases on which customers rely, today, to manage their financial wellbeing, make payments, or engage in other financial activities.

The products and services offered by FDATA members currently power use cases across a wide spectrum of the financial ecosystem. These applications, products, and services today depend on access to data held in mortgage accounts, government benefit accounts, brokerage accounts and financial accounts held by companies other than financial institutions, including utility, non-financial, and payroll service providers. The utility of facilitating a legally binding customer data access right to this broader set of data is obvious. Financial planning use cases can only give a customer the full picture of their financial health if they include the widest possible number of a consumer's accounts. A more robust view of a customer's financial situation may enable lenders to extend affordable credit to a broader set of applicants. Similarly, financial planning and investment professionals need access to the widest possible variety of accounts to give their customers a comprehensive and accurate picture of their financial health and to enable positive financial outcomes via personalized and compliant advice. And, critically, inclusion of government benefit accounts is necessary for the tens of millions of financially vulnerable Americans who depend on these benefits to manage their household finances each month.

The exclusion of these account types from the SBREFA outline is the most conservative interpretation of the Bureau's statutory authority granted under Section 1033, and unnecessarily and severely limits the potential for customer-permissioned data access to improve the financial wellbeing of millions of consumers and SMEs. These exclusions also risk sending a message to the custodians of these accounts that they have no legal requirement to make available the data held in these accounts to their customers or to third parties to whom their customers grant access to this information. Such an outcome would see existing use cases utilized by millions of consumers and SMEs across the country potentially degrade or stop working altogether.

The Bureau must also consider that, if all the use cases described above are not covered under this rulemaking, third-party data access via credential-based screen scraping or Personally Identifiable Information ("PII") and account number-enabled access will need to remain in place to power these use cases, on top of whatever access systems are required for the data types covered under this rule. Such an outcome would create technological complexity for data holders, data aggregators, and data recipients alike. For example, certain data holders provide both accounts covered under the Bureau's proposal and those that are not. This subset of data holder could have conflicting data access requirements that would cause one set of data to be subject to credential-less access means, while the other set of data could continue to use credential-based access.

A recent data connectivity survey that we conducted among our members revealed strong correlations between the asset size of data providers and the means of and customer data access. Only the very largest U.S. financial institutions have developed dedicated data access portals to date, and no U.S. bank outside of the top 10 in asset size as of the fourth quarter of 2022 has done so. Since the U.S. financial system is composed of thousands of financial institutions of varying size, FDATA is sympathetic to the cost burden they will face under this rule; however, we simultaneously believe that this must be balanced with the consumer impact of exempting too many data providers. If smaller providers are entirely excluded from the Bureau's eventual Section 1033 rulemaking, existing connectivity would be severed to the detriment of millions of consumers' and SMEs' financial wellbeing. FDATA therefore does not support complete exclusion of smaller data providers from this rule, but instead recommends the rule require them to make covered data for covered accounts available to their customers and third parties of their customers' choosing using alternative data sharing methods for the foreseeable future.

B. Recipients of information.

Consumers. Question 11. FDATA respectfully offers that the Bureau should strongly consider how it might apply the benefits and protections of a Section 1033 rulemaking to a broader universe of end users. The Bureau proposes in its SBREFA outline to define covered recipients of data under an eventual Section 1033 rulemaking as "an individual." Unfortunately, limiting the beneficiaries of a Section 1033 rulemaking to only individual consumers creates risk that small businesses, including sole proprietors, and investors, among other parties, would not

realize the benefits of a legally binding data access right and the protections afforded thereunder that a Section 1033 rulemaking will bring to bear.

Moreover, excluding small business owners and investors from the definition of covered recipients of information under a Section 1033 rulemaking could stymie the progress the marketplace has made over the last several years towards more efficient data access methods, where these account holders have routinely been considered as covered entities as data providers have built dedicated data access portals, in no small part due to a presumption by the marketplace that the final Section 1033 rulemaking would include these stakeholders. Though we understand the Bureau's rationale in the SBREFA outline for proposing to define covered recipients of information as only individuals, FDATA requests that the Bureau consider the potentially significant, negative impacts of excluding small businesses and investors under the rule.

Third parties. *Questions 12-21*. The Bureau's SBREFA outline proposes requiring third parties to present certain disclosures to a customer before seeking their authorization to access their financial data from a covered data provider. Having presented evidence of that authorization disclosure to a covered data provider, the Bureau is proposing that a covered data provider would be required to make available to the third party, at the customer's direction, the covered data it requests for the duration of time it requests in order to deliver the product, service, or tool for which the customer has opted in. FDATA here stresses the importance of the Bureau unambiguously providing in its forthcoming Section 1033 rulemaking a process by which third parties may present to data holders evidence of having received customer authorization for third-party account access to ensure that data providers cannot be permitted to override customer consent by selectively restricting their customers from sharing access to their data with respect to certain types of third-party use cases.

Today, in the absence of a Section 1033 rulemaking, some data providers are extending such use case-specific limitations. We therefore suggest the Bureau construct a third-party authorization framework to ensure that such use case-specific restrictions are not permissible and that flexibility be provided for new use cases that may be developed by the market in the future.

C. Types of information a covered data provider would be required to make available.

Data elements. Questions 22-27; 38. FDATA supports the inclusion of all proposed data elements, including account identity information, and the exclusion of proprietary data and confidential commercial information under an eventual Section 1033 rulemaking. We also support the Bureau's proposal that the amount of historical data made available under this rule must be the same as consumer can normally access via their online portal. Many use cases from third-party providers rely on historical banking information to accurately assess an individual's financial health, extend credit via cash-flow underwriting, and manage savings, bills, taxes, and accounts payable, among others, and would therefore benefit from the longest possible period of

historical data that this rule would require to be made available. As such, FDATA strongly believes that the benefits to a accessibility period that matches that of existing online portals far outweigh any risks. However, we urge the Bureau to guard against the possibility that covered data providers will use this new requirement to subsequently limit the amount of historical data available to a customer via their online portals.

D. How and when information would need to be made available.

Third party access. Questions 50-56. FDATA has long held that data access via dedicated access portals can be more reliable, faster, easier for the end user, and provide less friction if properly designed and operated as compared to legacy data access methods. FDATA supports a transition to credential-less data access methods as the preferred means of data access over the long term but remains steadfastly technology neutral. We understand that it is not practical to require all covered data providers to transition to credential-less data access methods immediately upon issuance of a final rule, particularly smaller financial institutions. Credential-based access must therefore remain as an option for a least a subset, of covered data providers for an extended time period to ensure compliance with an eventual Section 1033 rulemaking and to ensure that their customers have the same ability to access a competitive financial services marketplace as customers or larger financial institutions. It is imperative that the Bureau require all covered data providers, regardless of asset size and irrespective of the technology utilized to facilitate such data access, to provide data access with equal scope and reliability to ensure that all end users have equal access to their financial data.

One of the themes of the Bureau's SBREFA outline is striking the appropriate balance between the provision of an expansive and secure customer financial data access right and recognition that building dedicated data access portals has represented a resource and expertise challenge for many smaller financial institutions. Since the vast majority of U.S. financial institutions have not yet built dedicated data access portals, credential-based data access remains the most common method available to facilitate customer-permissioned data access to information required to fuel third-party use cases for all but the very largest U.S. financial institutions, with other technologies including PII and account number-enabled access also utilized in the marketplace. We respectfully suggest that this rulemaking should recognize this current reality and facilitate a transition to credential-less data access methods over a period of time for those data providers that have not yet built them.

To ensure that customers do not lose access to third-party tools on which they already rely, the Bureau should provide that existing technologies, including credential-based authentication or PII and account number-enabled access are permissible fallback options in instances in which no other data method is available or reliable. In addition to protecting customers' ability to continue to use the third-party financial tools, products, and services on which they already depend, such an approach would also implicitly create an incentive for smaller financial institutions to invest in and deploy dedicated data access portals, as they would be prohibited from restricting third-

party data access to account information via screen scraping when their customers provide their consent to do so. While such an approach may not be ideal, we would offer that the litany of data privacy, data security, and risk management requirements would provide for significantly greater customer protection, even in situations where credential-based or PII and account number-enabled access remain the only viable methods for facilitating customer-permissioned third-party data access. FDATA would also respectfully offer that, to the extent the Bureau decides to directly supervise data aggregation firms, even greater customer protection would exist for data access facilitated by credential-based data access technology as compared to current practice.

Data portal requirements. Questions 57-68. FDATA fully supports the principle that any dedicated data access portal deployed by a data provider should be as reliable and available as the customer's ability to access their data in their traditional online banking portals. For the large financial institutions that have, and will implement APIs to fulfill this access requirement, FDATA strongly suggests that cost-effective credential-less data access methods be considered as a valid fallback option if an API portal suffers from service interruption of any kind, including whole or partial failure to make available all types of covered data, for any period of time. As a last option, only utilized in serious service disruptions, should institutions who rely on credential-less data access be enabled to deploy credential-based data access as a fallback option. This arrangement can provide certainty to consumers and their third-party providers of choice that their data access, and all the use-cases that rely on them, will operate smoothly and reliably.

Data portal security. *Questions 69-71.* FDATA urges the Bureau to coordinate with the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and other prudential banking regulators to create clear and consistent standards for the security of any data portal deployed by a supervised financial institution. As the prudential bank regulators have historically viewed customer-permissioned data sharing through the lenses of their respective third-party risk management frameworks, data providers have over time developed different interpretations of regulatory expectations when facilitating or allowing third-party, customer-permissioned access to customer data. an outcome under a Section 1033 rulemaking under which there exists any perceived lack of harmonization between the Bureau's forthcoming rule, which will require data providers to allow third-party data access when presented evidence of authorization, and the prudential regulators' third-party risk management guidance, is likely to stifle the competitive, customer-driven marketplace the Bureau envisions in crafting a Section 1033 rulemaking.

Evidence of third-party authority to access information on behalf of consumer. Questions 73-76. As a core principle, FDATA believes that data providers should not be able to override any customer authorization that occurs via an authorized third party which meets the minimum cybersecurity and privacy requirements, nor change the terms of length or access, as long as such authorization is completed according to the requirements set forth in a Section 1033 rulemaking. We therefore urge the Bureau to consider and develop detailed guidelines for the disclosure and terms of use of data authorizations that clearly put consumers in control of their data.

The Bureau also notes in its discussion of authorization in its SBREFA outline that although it believes customers are best positioned to determine the appropriate authorization duration to receive the benefit of a third party's use case, it is "considering proposing that the authorized duration would be limited to a maximum period, after which third parties would need to seek reauthorization for continued access." While it is entirely correct for the Bureau to put customers in the role of determining how long to permit third parties to access their data, we would suggest the Bureau look to experiences in other markets, including the United Kingdom, which demonstrate that mandatory reauthorization or reauthentication events may needlessly and artificially create customer friction. As the Bureau may be aware, the United Kingdom's open banking framework initially called for mandatory 90-day reauthentication events. While this requirement was well intentioned, it failed to recognize that many customers had enrolled in a number of open banking use cases, which in practice resulted in customers being forced to reauthenticate with one of their third-party tools much more frequently than once every three months, leading consumers to abandon applications not for lack of value, but because of frustration from having to continuously reauthenticate. Regulators in the United Kingdom ultimately abandoned this requirement for a more streamlined approach to customer reauthentication.

Liability. FDATA has long advocated that the entity responsible for a data breach that results in financial loss is the entity that is responsible to make that consumer or SME whole, and it is the responsibility of an entity that has suffered a data breach to notify impacted consumers and SMEs, either directly or through a service provider. We believe that such notification must include a summary of what data was accessed and/or lost and potential steps impacted parties may take to mitigate financial harm as a result of the breach. Parties in the ecosystem should make reasonable efforts to cooperate with an entity that has suffered a data breach to assist in identifying impacted consumers and SMEs.

Consumers and SMEs should be afforded the presumption of being eligible for reconstitution when they request remuneration for financial loss as a result of a data breach, so long as they are provided a minimum of one year from the date a financial loss was experienced as a result of fraud or a data breach to request compensation and they demonstrate a connection between their financial loss and a data breach. FDATA has also taken the position that consumers and SMEs should not be eligible for compensation of financial losses for authorized or first-party fraud provided the entity or entities through which the fraud was facilitated deployed reasonable anti-fraud and/or security protections.

We also support requiring third parties that have experienced a data breach as a result of a malicious attack to notify their data aggregator(s) after identification of the breach as soon as practicable or, in any event, within 24 hours. In such instances, data providers to that third party should be notified of the breach, either by the aggregator or, at the aggregator's direction, via the third party, subject to applicable regulatory or legal requirements.

E. Third party obligations.

Data minimization, Question 88. We agree with the limitation standard set forth in this section. Third parties should be limited to collecting only those data which have been authorized by customer and which are necessary to fulfill the use case for which the customer has opted into, as defined by the third party providing the financial service, product, or tool. So long as the customer has been made aware that the data is being collected, the data provider should not restrict the ability of their customer to permission access.

Because of the variety of use cases in the market, and the potential for new innovation based on different combinations of data elements, the Bureau should not attempt to define use case-based data scope limitations in regulation.

The Bureau should recognize, however, that in order to serve the authorization and disclosure function certain data types that are not required for the customer's desired use case need to be collected by the authorized third party. For example, in order to revoke access, an authorized third party needs to be able to identify a user by their name or another identifiable piece of information. Therefore, the authorized third party must be able to gain consumer authorization to collect that information.

Duration and frequency of third-party access. Questions 91-97. FDATA believes that this rulemaking should provide end users the ability to revoke or re-authorize data access as they wish.

Limits on secondary use. Questions 98-102. FDATA is concerned that the Bureau's proposed limitations on permissible secondary use cases could have significant, negative impacts on a broad range of stakeholders. To remedy this concern, we encourage the Bureau to differentiate between customer-identifiable data and de-identified data. While we agree with imposing clear limitations on how customer-identifiable data can be used outside of a consented use case, this must be balanced with an appreciation for the consumer benefit created by de-identified data today, including its importance in designing product improvements, performing macroeconomic research, and informing policymaking.

Whereas customer-identifiable data may contain elements that could identify an individual end user, de-identified data, pursuant to Federal Trade Commission ("FTC") guidelines, is a single data element or a data set that cannot reasonably be reidentified to an individual end user. As it considers its framework for disclosure, consent, and data usage under a Section 1033 rulemaking, we would suggest that failing to distinguish between these two distinct types of data could create unintended impacts for a wide range of stakeholders.

A Section 1033 rulemaking that fails to differentiate between customer-identifiable data and de-identified data and imposes significant restrictions on secondary use cases without making such a

distinction, would substantially limit, or prohibit entirely, the many important uses of anonymized data on which so many stakeholders rely for a number of use cases, including customer protection. For these reasons, we offer that the Bureau should clearly distinguish between customer-identifiable data and data that is de-identified in accordance with existing FTC guidance, particularly with regard to secondary use cases.

In its proposed rule, the Bureau should clarify that de-identified data may be used for secondary use cases only if the end user is informed that data may be de-identified and be used for other purposes as allowed by law. Usage of de-identified data for secondary use cases should not be permitted for use cases intended to target, identify, or expand product offerings and services to individual users. To be clear, FDATA is not in any way suggesting that third parties should be able to access or "mine" all de-identified data from any covered data provider. To ensure that product and credit model enhancements, economic research, and other important use cases, we offer that it is important the Bureau allow for secondary usage of previously permissioned data that has been subsequently de-identified.

Finally, we encourage the Bureau to contemplate the competitive and consumer data right implications of different data use requirements across data providers and authorized third parties. To the extent that the Gramm-Leach-Bliley Act ("GLBA") is a different data use regime than Section 1033, consumers could see companies they interact with use their information in different ways, leading to mixed expectations and competitive differences across ecosystem participants.

Limits on data retention. Questions 103-110. FDATA has long held that third parties should not retain data that is no longer being used, except when requested by law enforcement. There are however some use cases, such as tax filing or lending, that are used relatively infrequently by end users, but only remain useful to consumers if their data is retained for long periods of time. In these specific use cases, the Bureau should clarify that long term data storage is "reasonably necessary" even if there are periods with little customer activity.

G. Implementation period

FDATA urges the Bureau to swiftly require availability of all covered data types for covered data accounts once this rule is finalized. A final rule that clearly allows for the continued use of existing technologies, including credential-based access or PII and account number-enabled access in addition to dedicated data access portals, would facilitate the fastest and easiest transition into compliance and maximize customer benefit, particularly for the thousands of smaller data providers which will not be able to develop credential-less data access portal technology for the foreseeable future.

Additional Comments

Supervision. As discussed earlier in this submission, a regulatory regime in which the prudential regulators are responsible for overseeing the relationships between insured depository institutions and third-party data aggregators, and the Bureau is responsible for overseeing the

relationships between third-party aggregators and their customers would provide the certainty and uniformity necessary to foster a safe and competitive marketplace. Critically, this coverage would ease the burden on the banks themselves and eliminate the uncertainty that banks often use to block or restrict third-party, permissioned access to customer financial data.

The existing regulatory regime lacks this clear delineation of responsibility, providing only vague guidelines that allow for many forms of interpretation, some of which can and are being used to thwart the wider promulgation of innovative technology tools that can meaningfully improve customer financial wellbeing. In order to balance the free flow of commerce with the ever-growing need for data security, FDATA has consistently advocated for the Bureau to undertake a supervisory role over data aggregations firms. Since the failure of any aggregation company would not conceivably jeopardize the safety and soundness of the banking system, prudential regulators are not best suited for this area of oversight. Because the Dodd-Frank Act provides jurisdiction over data access rights to the Bureau, the development of a successful 1033 rule must include a detailed analysis of how it intersects with any guidance issued by the prudential regulators.

We believe that the prudential regulators should retain supervisory authority over the relationship between financial institutions and data aggregators, while the Bureau, upon finalization of this rule, supervises the relationships between aggregators and third-party service providers. This bifurcated approach will best leverage the existing technical expertise of each agency and its staff, align with the spirit of U.S. banking law and regulation and maintain clear lines of jurisdiction.

Conclusion

The Bureau's outline provides a strong framework for a potential Section 1033 rulemaking, the foundation of which is the legal right for consumers and SMEs to access and share access to their financial data. Having engaged with the Bureau on this rulemaking for the past several years, FDATA again commends the Bureau for its thoughtfulness as it begins the formal rulemaking process to implement a critically important financial data access right for customers across the U.S. As the Bureau considers the open questions it has posed to market stakeholders in its SBREFA outline, we respectfully encourage it to:

- Expand the scope to include a broader swath of both covered parties, including small businesses and investors, and account types, including government benefits, utility, nonfinancial, and payroll accounts, and accounts held by financial institutions not covered by Regulation E or Regulation Z, and provide similar liability principles if the scope of covered account types is expanded;

- Guard against potential commercial incentives by data providers to restrict data access for particular use cases by ensuring that customer authorization may not be overridden except in very limited circumstances;

- Require as many financial institutions as practicable to build and implement credential-less data access methods, while allowing sufficient time for small financial institutions to do so;

- Permit credential-based or PII and account number-enabled data access to persist as a fallback option in instances in which data is not accessible through other means;

- Clearly distinguish between customer data and de-identified data with regard to secondary use cases;

- Calibrate the timeline for implementation for credential-less data access based on financial institution size, and

- Directly supervise data aggregation platforms.

On behalf of FDATA North America, thank you for your consideration of our submission in response to the SBREFA outline and for your continued work on this critical issue.

Sincerely,

Steven Boms
Executive Director