www.fdata.global/north-america

December 27, 2023

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

Sent via electronic mail to 2023-NPRM-Data-Rights@cfpb.gov.

Re: Required Rulemaking on Personal Financial Data Rights, Docket No. CFPB-2023-0052

The Financial Data and Technology Association of North America ("FDATA North America") appreciates the opportunity to provide comments in response to the Consumer Financial Protection Bureau's ("CFPB" or "the Bureau") Notice of Proposed Rulemaking ("NPRM") on Personal Financial Data Rights, which will, once finalized, implement Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("the Dodd-Frank Act").

FDATA North America and our members have for years been strong advocates for providing consumers, public benefits recipients, small business owners, investors, and other financial services marketplace end users with legally binding financial data rights. As we have seen in other jurisdictions around the world that have granted legal rights and protections to their citizens to access and share access to elements of their financial data, a customer-centric ecosystem in which the end user is in full control of their data leads to a more innovative, more competitive, and more transparent financial marketplace.

Our members' products, services, and tools underscore this reality. 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 ("SMEs") 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

The Bureau's Personal Financial Data Rights NPRM represents a significant and critically important legal framework that will improve competition and lower fees in the financial services

marketplace, bolster innovation, and provide important protections to consumers when they share elements of their financial data with a third-party provider. CFPB Director Rohit Chopra heralded the Bureau's NPRM as a "shift to supercharge competition" and "improve financial products and services."[1] The Director's statement recognizes that the underpinning of a competitive consumer financial marketplace is the ability of any customer to easily select or switch between providers, which ultimately reduces the price of a good or service for customers. Other jurisdictions, including but not limited to Australia, the United Kingdom ("U.K."), the European Union, New Zealand, and Singapore, have enacted legal frameworks to provide these "open finance" regimes in which their citizens and SMEs have full control over their financial data and the ability to easily select from and switch among a vibrant marketplace of third-party providers. Recognizing the obvious benefits of such systems, the governments of both Canada and Mexico are advancing similar regimes of their own. By contrast, consumers in the United States regularly encounter friction when seeking to utilize a third-party financial product, service or tool in the absence of regulation to enforce their legal right to do so.

The financial marketplace has sought unsuccessfully over the last several years to address these issues through the promulgation of complex bilateral data access agreements negotiated between financial institutions and consumer-permissioned data access platforms. These agreements, which generally have thus far only been executed between the largest U.S. financial institutions and data access platforms, are entirely opaque to consumers but dictate the terms and conditions under which end users may digitally share access with third parties to their financial data and the protections afforded to them when they do so. As FDATA North America has previously shared with the CFPB, these agreements can in some cases take multiple years from ideation to execution and are each bespoke. As a result, customers of one financial institution may have different data access rights and protections than customers of another financial institution based on a contract to which they are not a party. Moreover, this approach to open finance is not scalable. It would from a practical perspective be impossible to require data access platforms and third parties to execute data access agreements with every financial institution in the U.S. as a requirement of facilitating consumer-permissioned data access. This status quo, under which the industry does not have a standardized framework to ensure financial institutions and third parties have consistent and clear requirements around the safe collection, use, and storage of consumer permissioned has resulted in financial institutions taking disparate approaches to all data access through the negotiation and execution of complex data access agreements, does not serve the best interests of U.S. consumers or competition in the U.S. financial services market.

To be clear, there exist genuine considerations that may fuel financial institutions' inclination to restrict or block consumer-permissioned third-party provider data access. A lack of standardization regarding the data privacy and protection postures of third parties and a desire by all stakeholders to transition away from credential-based screen scraping to more secure and efficient means of

[1] *See* CFPB Proposes Rule to Jumpstart Competition and Accelerate Shift to Open Banking, https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-jumpstart-competition-and-accelerate-shift-to-open-banking/, issued October 19, 2023.

facilitating consumer-permissioned data, both of which the NPRM directly addresses, have historically been common impetuses driving financial institutions' desire to execute bilateral data access agreements. The prudential regulatory agencies' third-party risk management requirements for supervised financial institutions, which, as we discuss later, we believe requires more consideration in advance of the CFPB's finalization of its Personal Financial Data Rights rule, is another frequent issue cited as a rationale for data access agreements that can limit consumer data access. FDATA North America believes that a final Section 1033 rulemaking must provide the market with sufficient clarity regarding the roles and responsibilities of data providers, authorized third parties, consumer-permissioned data access platforms, and, most importantly, consumers, to finally transition the U.S. financial services ecosystem to an open finance regime.

Of course, even amidst these challenges, U.S. consumers and SMEs have benefitted from a more diverse and innovative financial marketplace than exists in many other countries. FDATA North America member companies today empower consumers to grow their retirement savings, more easily and affordably manage their investments, pay their debts, track and plan their spending and saving, file their taxes, access affordable credit, and more efficiently manage their public benefits. Our members also work alongside SMEs to help them seamlessly manage their accounting, payroll, tax preparation, and credit needs. But as the Bureau noted in its statement accompanying the release of its Personal Financial Data Rights NPRM, the ability of both consumers and SMEs to access these third-party tools and services today is inconsistent, which significantly impairs the ability of third-party providers to compete with incumbents.[2]

Consumers Are Demanding a More Competitive Financial Services Marketplace

For years, but particularly in the period during the economic uncertainty of the COVID-19 pandemic and the sustained inflation that has followed it, it has been obvious that consumers are demanding access to financial solutions in new and novel ways that better meet their needs. Digital financial services can help address these demands. Research commissioned by an FDATA North America member company last year found that two-thirds of consumers in the U.S. and U.K. reported that financial technology ("fintech") helped them weather economic challenges. Half said fintech helped them feel more in control of their finances and an overwhelming nine in ten users saw benefits from using fintech tools.[3]

To benefit from these third-party tools, products, and services, consumers require the ability to permission access to and to use their own financial data. When combined with a more efficient or easier-to-understand user experience or at lower costs than a consumer's existing financial institution offers, the ability of an end user to share access to elements of their account transaction and balance history can unlock significant benefits.

[2] *Id.*
[3] *See* Plaid's 2022 Consumer Survey: The Fintech Effect, https://plaid.com/blog/fintech-effect-report-2022/, released October 18, 2022.

The growth of the fintech industry over the last several years underscores this trend of consumers and SMEs voting with their smartphones. A July 2018 U.S. Department of the Treasury report found that from 2010 to the third quarter of 2017, more than 3,330 new technology-based firms serving the financial services industry were founded.[4] Across the globe, KPMG found that investments in fintech firms for the first half of 2023 grew from $22 billion in 2017[5] to more $52 billion.[6] The Boston Consulting Group estimated earlier this year that the size of the U.S. fintech market will exceed $1.5 trillion by 2030.[7]

The competition third-party fintech tools provide, both with each other and with traditional financial institutions, significantly benefits consumers, lowers costs, and improves access to mainstream financial services products, services, and tools across the country. In the U.S., black-owned SMEs were nearly five times as likely to access Paycheck Protection Program loans during the COVID-19 pandemic from fintech platforms than from traditional financial institutions.[8] Globally, the World Bank reported in 2021 that 1.2 billion previously unbanked adults gained access to financial services "primarily boosted by the increase in mobile money accounts."[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. But in markets in which legally binding consumer data rights have been implemented, the rate of adoption is remarkable. According to Open Banking Limited, the U.K.'s open banking implementation entity, 10.8 million payments were made in June 2023 utilizing the country's open banking framework – nearly double as many as compared to the same month the previous year.[10] More than one in nine British consumers are now active users of the U.K.'s open banking framework.[11]

Finally, the U.K. market demonstrates that the provision of a legally binding consumer data right enables a more competitive marketplace. In just the last three years, the number of regulated third-party providers of financial services, products and tools across the pond has increased by nearly

[4] *See* U.S. Treasury, A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation, https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf, issued July 2018.
[5] *Ibid.*
[6] *See* H1 2023 – Pulse of Fintech, https://kpmg.com/xx/en/home/industries/financial-services/pulse-of-fintech.html, issued July 2023.
[7] *See* Fintech Projected to Become a $1.5 trillion Industry by 2030, https://www.bcg.com/press/3may2023-fintech-1-5-trillion-industry-by-2030, issued May 3, 2023.
[8] *See* Lender Automation and Racial Disparities in Credit Access, https://www.nber.org/papers/w29364, issued October 2021.
[9] *See* On Fintech and Financial Inclusion, https://blogs.worldbank.org/psd/fintech-and-financial-inclusion, issued October 26, 2021.
[10] *See* Over 1 in 9 Brits Now Use Open Banking Services as Open Banking Payments Reach Record High, https://www.openbanking.org.uk/news/open-banking-impact-report-october-2023/, issued October 24, 2023.
[11] *Ibid.*

25%.[12] The experience of the U.K. market clearly indicates, as so many other countries have also recognized, that providing consumers with more control of their data – and with the ability to choose from a broad array of third-party financial providers – boosts market competition.

The Proposed Rule, Once Finalized, Will Meaningfully Improve Competition and Consumer Centricity in the U.S. Financial Services Ecosystem

The CFPB's NPRM implementing a personal financial data right in the U.S. will, once finalized, deliver the same consumer and competition benefits in the United States that other countries with similar regulatory frameworks have already realized. Having for many years encouraged the Bureau to use its Section 1033 authority to promulgate a rule providing legally binding consumer financial data rights, FDATA North America congratulates the CFPB for this significant milestone and expresses our appreciation of the substantial effort that clearly contributed to the proposed rulemaking.

We will focus the majority of our substantive comments on those areas for which we encourage the CFPB to consider potential amendments between the NPRM and a final rule implementing Section 1033 of the Dodd-Frank Act. Before we do so, however, we would like to highlight the many elements of the NPRM that we believe will appropriately and meaningfully progress the U.S. financial services marketplace towards an open finance ecosystem:

- The NPRM proposes to create a legally binding consumer financial data right that would, for the first time, provide U.S. consumers with a data portability right and the ability to select the financial product, tool, or service best suited for their unique financial position. Importantly, the NPRM details the types of data that would be required to be made available to a consumer to share access to, including transaction, balance, payment, historical, and identity data.

- The Bureau's proposed rule would require that financial institutions build and deploy developer interfaces through which all covered data would ultimately be accessed by authorized third parties at a consumer's direction. This approach will, once implemented under the timeline proscribed by the NPRM, allow for more efficient consumer-permissioned data access for covered data included in covered accounts under the rulemaking.

- The NPRM prohibits data providers from "imposing any fees or charges for establishing or maintaining" developer interfaces "or for receiving requests or making available covered data through the interfaces."[13] This provision of the Bureau's proposed rule is both appropriate and timely, as some financial institutions have in recent months sought to funnel all consumer-

[12] *See* Open Banking Limited Regulated Providers, https://www.openbanking.org.uk/regulated-providers/, accessed November 9, 2023.
[13] *See* Proposed Required Rulemaking on Personal Financial Data Rights, issued October 19, 2023.

permissioned data access through a forced, bank-owned intermediary that aspires to commercialize customers' data access requests. The inclusion of a prohibition on data providers from assessing fees to build or maintain developer interfaces or for accessing data from the interfaces directly addresses a current issue in the marketplace that has resulted in data access restrictions for some consumers.

- The NPRM appropriately provides that authorized third parties are best positioned to collect a consumer's informed authorization, noting that incumbents may have incentives to use the collection of user authorization as a means to restrict data access.

- The proposed rule's provision of a 12-month mandatory reauthorization window partially achieves adequate consumer protection without introducing undue friction into the user journey, but the Bureau should clearly provide that any instance in which a consumer refreshes their data, including a refresh authorized by a consumer as part of an active membership or ongoing service that reasonably and specifically contemplates a recurring refresh (e.g. self-contributing tradelines to a credit file), or facilitates a payment with an authorized third party constitutes a new authorization for the purpose of restarting the 12-month reauthorization window. As the Bureau is aware, the U.K.'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 U.K. ultimately abandoned this requirement for a more streamlined approach to customer reauthentication. The U.S. marketplace could reap the benefit of this natural experiment were the Bureau to make it explicit that the consumer need not reauthenticate more frequently than they are required to reauthorize. Furthermore, as long as the consumer is relying on the same data access provider, they should be able to update permissions or connect a new third-party data recipient during the 12-month window without the data provider reauthenticating the consumer each time.

- From a practical perspective, however, the Bureau should consider allowing authorized third parties to retain historical data for some period of time after the 12-month period ends so that the product, service, or tool the consumer has elected to use to manage their financial wellbeing remains populated if the consumer elects to reauthenticate shortly after the 12-month authentication window expires.

- The proposed rule provides a pathway for industry standards to be recognized by the CFPB and then relied upon by data providers to satisfy certain obligations under the rule. The framework the NPRM utilizes to define the parameters of an industry standards body – Office of Management and the Budget Circular A-119 – provides the market with unequivocal governance, due process, and representation criteria. Once recognized, the ability of data

providers to rely on an industry standard to deploy their developer interfaces – and for authorized third parties to access consumer-permissioned data through industry standard developer interfaces – will significantly reduce costs across the ecosystem.

- The NPRM properly requires that authorized third parties meet certain data privacy and data protection standards, including those provided under sections of the Gramm-Leach-Bliley Act ("GLBA") and the Federal Trade Commission's ("FTC") Safeguards Rule, to ensure that consumers are protected whether they choose to work with a traditional financial institution or a third-party financial services provider.

We commend the CFPB for proposing a comprehensive, thoughtful approach to implementing Section 1033 of the Dodd-Frank Act in a manner that will, once implemented, improve consumer financial control, transparency, and outcomes in the U.S. financial system. The NPRM recognizes and builds upon the elements of open finance that market stakeholders have thus far been able to deliver in the absence of regulation and addresses the overwhelming majority of issues that exist in the market today that result in an unlevel playing field for consumers in which a consumer's ability to benefit from a third-party financial services provider depends on with which financial institution they bank.

Elements of the NPRM That Warrant Further Consideration

To fully realize the objectives of Section 1033 of the Dodd-Frank Act, which Director Chopra has explained as "a shift towards open and decentralized banking,"[14] FDATA North America respectfully offers that there are areas of the NPRM that should be amended before the CFPB issues its final Personal Financial Data Rights rulemaking next year. We provide a detailed overview of our recommended changes in the following sections but summarize our suggested amendments here:

- The Bureau proposes in its NPRM to include Regulation E asset accounts, including digital wallets, and Regulation Z credit cards as covered under its initial rulemaking. FDATA North America views this set of covered accounts as too narrow. While we understand that the Bureau proposes this limited scope as a starting point, FDATA and our members would strongly urge inclusion of public benefits, small business, investment, retirement, and other types of non-transaction accounts held at traditional financial institutions, as well as mortgages, auto loans, and all forms of time deposit accounts. Our member companies currently provide tens of millions of U.S. consumers and SMEs access to these non-covered data types, and they would be at risk of losing such access were it not guaranteed under a Section 1033 rulemaking.

[14] *See* CFPB Proposes Rule to Jumpstart Competition and Accelerate Shift to Open Banking, https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-jumpstart-competition-and-accelerate-shift-to-open-banking/, issued October 19, 2023.

- The NPRM's proposed limitations on secondary data usage would, if included in a final rule, both cause negative consumer and economic outcomes and inadvertently provide incumbents with competitive advantages, thus potentially undermining one of the very core objectives of the rule. Limitations on how data may be utilized under Section 1033 of the Dodd-Frank Act should focus more expressly on consumer-identifiable data, recognizing that de-identified data has significant value for consumers across the ecosystem, including for research and product enhancements, among many other use cases, A final rule should clearly allow for consumer-permissioned data to be used for product enhancements, fraud protection and security purposes, and other critical uses. Beyond this, we believe it is vitally important to preserve the ability of innovators to leverage at least some secondary use of consumer-identifiable data – subject to the user's consent and ability to opt-out or opt-in – to ensure their products and services may continue to deliver compelling solutions and insights.

- The NPRM would allow data providers to deny authorized third-party access to consumer-permissioned data "based on risk management concerns."[15] Barring clarity from the Bureau and prudential bank regulators, the net effect of this provision will be disparate standards across financial institutions, which is ultimately contrary to the standardization proposed and promised through this rulemaking.

- The final rule should not automatically require an authorized third party to delete previously acquired data when a consumer revokes access to a covered account as this may have unintended consequences that are not aligned with the consumer's intent. Upon revocation of access, the consumer should be able to decide whether or not previously acquired data should be retained by the authorized third party. As an example, a consumer may authorize a third party to access data from a covered account to assist with creating and managing a financial budget. The consumer subsequently changes data providers and wishes to revoke the authorized third party's access to the original data provider's covered account as it is no longer necessary. The consumer does not want the authorized third party to delete the historical data as its essential to continue receiving the benefits the authorized third party is offering. Under the proposed rule's current language, the authorized third party is obligated to delete the covered data once the consumer deauthorizes access to the covered account. We believe it to be in the consumer's best interest to decide whether or not an authorized third party should delete covered data when they revoke that third party's access to said account.

- The minimum quantitative standards included in the NPRM for data provider developer interfaces should include data quality and volume standards in addition to the reliability and call time standards that were proposed. We also note that the NPRM's proposed 3,500 millisecond standard for average developer interface call time is well below today's industry standards, which could have the perverse impact of actually slowing consumer-permissioned third-party data access over time.

[15] *Id.*

- The Bureau's final Section 1033 rule should clearly restrict not only data providers from assessing fees for building and maintaining their developer portals and for facilitating data access requests through them but also any forced intermediaries a data provider attempts to insert into the consumer-permissioned data ecosystem, with a particular focus on intermediaries owned by large market incumbents.

- The NPRM would allow data providers to confirm with their customer that they provided their authorization to a third party to access their data; however we do not believe it unambiguously prevents, as drafted, data providers from using the authorization confirmation or authentication process provided under the proposed rule to either induce friction into the confirmation process or to use the opportunity to market their own products, tools, or services, which may be more expensive for or less well-suited to the consumer.

- The NPRM proposes a pathway through which an industry technology standard recognized by the CFPB would become the means through which data providers would be permitted to implement their developer portals; however, the proposed rule fails to clearly articulate that various authentication processes other than credential-based access may be utilized to access developer interfaces and, in so doing, indirectly picks winners and losers in the consumer-permissioned financial data ecosystem. The Bureau should instead consider a final rule that allows data providers to rely on either an industry standard or a commonly used technology for the purposes of deploying a compliant developer interface.

- The NPRM would allow data providers to utilize tokenized account numbers ("TANs") when providing access to authorized third parties. FDATA North America notes that TANs are a complex issue beyond only the open finance context and that challenges with the interoperability of TANs in a number of use cases raise serious questions about the implications of transitioning to tokenized data elements as proposed under the rule. As a result, the Bureau should remove TANs from its Personal Financial Data Rights rulemaking. To the extent the Bureau maintains an interest in addressing the use of this technology within the marketplace, it should coordinate with the prudential financial regulators in a separate guidance or rulemaking. If, however, the Bureau opts to include its proposed approach to TANs in its final Section 1033 rulemaking, it is vital that the CFPB clarify that a TAN permissioned on behalf of a consumer is permitted to be used perpetually so long as their authorization is valid.

- The CFPB should clearly and unambiguously provide in its final Section 1033 rulemaking that legacy data access technologies may be utilized to access data in circumstances in which no developer interface exists to access consumer-requested data, or when a developer interface is not capable of reliably facilitating consumer-permissioned data access. The provision of a fallback option will be particularly important to the extent that the Bureau opts not to include additional covered accounts under the final rule, given that many data providers are unlikely

to include non-covered accounts in their developer interfaces in the absence of a regulatory requirement to do so.

- The NPRM proposes that consumer-permissioned data access platforms that facilitate data access for credit decisioning use cases, among others, should be regulated as consumer reporting agencies; however, in instances in which a data access platform makes no assessment of a consumer's creditworthiness, the application of the Fair Credit Reporting Act ("FCRA") is needlessly complex, conveys no discernable additional consumer protection, and presents the potential for creating consumer confusion and harm.

- The NPRM makes no reference to FDATA North America's long-advocated position that the Bureau should extend its supervisory authority to data access platforms. Though it recently noted it had conducted a voluntary examination of one such platform, we again recommend that the CFPB utilize its larger participant authority to exert supervisory oversight data access platforms, with a particular view towards addressing the third-party risk management ("TPRM") issue highlighted above.

A more detailed discussion of each of these recommended amendments to the proposed rule follows.

Detailed Discussion of Elements of the NPRM That Warrant Further Consideration

Scope of Accounts Covered and Beneficiaries of the NPRM's Legal Financial Data Access Right

The NPRM would apply an initial Section 1033 rulemaking to asset accounts subject to the Electronic Fund Transfer Fact and Regulation E, credit cards subject to the Truth in Lending Act and Regulation Z, and related payment facilitation products and services, including digital wallets. While the CFPB correctly notes in its proposal that a plethora of beneficial use cases exist today that depend on consumer-permissioned access to these accounts, we continue to urge the Bureau to unleash the full potential of a customer data access right to ensure that consumers, small business owners, investors, public benefits recipients, and a host of other stakeholders receive the same rights and protections the NPRM would bestow upon Regulation E accountholders and Regulation Z credit cardholders.

The NPRM specifically requests stakeholder feedback on whether Electronic Benefit Transfer ("EBT") data should be covered under this rulemaking. FDATA North America urges the CFPB in the strongest possible terms to include EBT data in its final Section 1033 rule, both to ensure that lower-income consumers are provided the same data rights and protections as the more affluent, and also to ensure innovative and consumer friendly applications and use cases can be developed to support this segment of the consumer market to the same extent as the traditional financial services market.

We also note that there exists a litany of use cases on which customers rely, today, to manage their financial wellbeing, make payments, or engage in other financial activities that require consumer-permissioned data connectivity to other types of accounts held by financial institutions, including auto loans, mortgage loans, student loans, and investment and retirement accounts, among others. As crafted, the NPRM excludes accountholders of these accounts from receiving the same benefits and protections that are bestowed on Regulation E asset accountholders and Regulation Z credit card accountholders under rule.

While we appreciate the Bureau's assurance in the NPRM that it "intends to implement…section 1033 with respect to other covered persons and consumer financial products or services through supplemental rulemaking,"[16] it is important for the CFPB to consider and address the potential market implications of excluding these accounts from an initial Personal Financial Data Rights rule. FDATA North America notes the broad range of market stakeholders, including fintech companies, financial institution representatives, and consumer advocates who responded to the CFPB's Small Business Regulatory Enforcement Fairness Act ("SBREFA") outline of proposals and alternatives under consideration for a Section 1033 rulemaking earlier this year encouraging the Bureau to include a more exhaustive set of accounts under its Personal Financial Data Rights rule. For example: Registered Investment Advisors ("RIAs") and Broker-Dealers ("BDs"), among others, meet the definition of "consumer" under §1002(4) of the Dodd-Frank Act as they are "an agent, trustee, or representative acting on behalf of an individual." The proposed definition of "consumer" in §1033.131 of the NPRM would deny millions of consumers access to the advisory services upon which they depend for retirement, tax, education, medical and general financial management purposes. From a consumer protection perspective, inclusion of accounts administered by RIAs and BDs will provide overarching governance of issues contemplated by the Bureau such as disclosures, data retention, and secondary use.

A rule that fails to include all of these types of accounts, even despite a clear signal from the CFPB of its intention to ultimately use its statutory authority to do so in the future, risks emboldening the custodians of these accounts to make it far more onerous for consumers to obtain their data or to charge for it. Such an outcome would see existing use cases utilized by millions of consumers, investors, and SMEs across the country potentially degrade or stop working altogether. To the extent the Bureau opts not to include additional accounts within the scope of its first Personal Financial Data Rights rule, we request that the CFPB make clear that the exclusion of any financial account from a final Section 1033 rulemaking should not be interpreted as guidance to financial institutions that they must restrict third-party, consumer-permissioned data access to those accounts.

The Bureau should consider the technological implications of a more limited scope of covered accounts under an initial Section 1033 rulemaking. It is impractical to expect that the thousands of data providers that have not yet deployed developer interfaces will provide consumer-

[16] *Id.*

permissioned connectivity to accounts beyond only those that are required under the rule. As a result, and because millions of consumers, investors, and SMEs require this data connectivity already to fuel the use cases on which they rely to manage their finances, 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. As the Bureau considers the NPRM's treatment of legacy consumer-permissioned data access technologies, and as we discuss further in our comment, it will be imperative that the CFPB ensure that existing data access technologies may continue to be used when consumers require connectivity to data held in accounts not covered under a final Personal Financial Data Rights rule.

The Proposed Restrictions on Secondary Use Cases Would Have Significant, Negative Consumer, Competitive, and Economic Impacts

The NPRM proposes to limit third-party collection, use, and retention of covered data to "what is reasonably necessary"[17] to provide the consumer's requested product or service. While FDATA North America strongly associates itself with what we believe to be the intention of the secondary data limits included in the proposed rule – namely that consumer data is not misused – we are concerned that the NPRM's approach to addressing this issue is inappropriately calibrated and would both result in significant consumer and economic harm.

As currently constructed, the NPRM's limitations on secondary uses of consumer-permissioned data would restrict a broad range of existing use cases that today inarguably provide consumer and economic benefits. There exist secondary uses that are compatible with the primary purpose for which the consumer authorized access to their data that are not unexpected by the consumer, and ultimately are good for the ecosystem. These use cases include development of fraud detection tools and improving upon or adding new features to a product or service the consumer is already using.

To strike a reasonable balance, FDATA recommends:

- The CFPB should, in conformance with existing federal and state expectations, exempt de-identified data that cannot reasonably be re-associated or linked to any individual by a third party in possession of the data from secondary use or sharing restrictions, as a way to encourage entities to employ anonymization as a data minimization technique while still enabling valuable business use cases and innovation;
- By default, include compatible secondary purposes as automatically permissible use cases of consumer-identifiable data, similar to the statutory approaches of California, Colorado, Connecticut, Utah, and Virginia; and
- Either offer the consumer the prerogative to generally opt-out of secondary use of identifiable data, either at the moment of authorization or at some later date; or,

[17] *Id.*

- Offer the consumer the opportunity to opt-in to secondary use of identifiable data generally, or for specific use cases.

De-identified data is a vital, privacy-friendly tool for financial institutions and third parties alike that is used for: enhancing existing products and services and designing new offerings; protecting their systems and customers from all manner of security threats; alerting consumers to more affordable or better-suited products or services; and facilitating academic and policy research that is relied upon to inform monetary and fiscal decision making. In crafting its final rule implementing Section 1033 of the Dodd-Frank Act, we urge the CFPB to carefully consider the detrimental impact the proposed broad restriction on secondary data usage would have for these use cases.

We continue to believe that the most appropriate manner in which to achieve data minimization under a final Personal Financial Data Rights rule while ensuring that the important use cases above will continue to provide consumer and economic benefits would be for the CFPB to distinguish in its final rule implementing Section 1033 of the Dodd-Frank Act between consumer-identifiable data and de-identified data. Such an approach should establish clear limitations on how consumer-identifiable data can be used outside of a use case for which a consumer has provided their consent while still allowing for consumer benefits created by use cases that are powered in whole or in part using de-identified data today. The Bureau should rely on existing regulatory precedent to craft this approach in its final rule. Whereas consumer-identifiable data may be defined as data elements that could identify an individual end user, de-identified data, pursuant to FTC guidelines, should in the Bureau's final Personal Financial Data Rights rule be defined as a single data element or a data set that cannot reasonably be reassociated with an individual end user.[18]

To provide additional consumer protections even beyond the FTC guidelines, the Bureau should in its final rule further clarify that de-identified data may be used for secondary use cases only if the consumer is informed and provides their affirmative, meaningful consent that data may be de-identified and be used for other purposes as allowed by law. Consistent with the NPRM's specific proposed limitations on secondary data usage under §1033.421(a)(2), a final Personal Financial Data Rights rulemaking should also restrict usage of de-identified data for secondary use cases intended to target, identify, or expand product offerings and services to individual users. We believe that this approach, under which de-identified data would still be permitted to be used, with disclosure and consent, for those secondary use cases that provide consumer and economic benefits, would appropriately balance consumer protection and privacy with the importance of continuing to enable a slew of important use cases that convey significant benefits today.

As a matter of competitiveness, FDATA North America is concerned that the secondary data use limitations included in the NPRM would apply only to authorized third parties, while data

[18] *See* Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, issued March 2012.

providers operating in compliance with the GLBA would have different and more expansive abilities to interact with, use, and retain de-identified data. An outcome where different market stakeholders operated under disparate de-identified data usage frameworks would result in consumers seeing companies they interact with use their information in different ways, leading to mixed expectations and competitive differences across ecosystem participants. Over time, these competitive differences would accrue significant advantages for market incumbents, which could threaten one of Director Chopra's main objectives in advancing a Personal Financial Data Rights rulemaking: to "supercharge competition."[19]

Prudential Regulatory TPRM Obligations Could Undermine the Objectives of the NPRM

Financial institutions operate in a highly regulated environment and are subject to a litany of regulatory expectations with the potential to interact significantly with the Section 1033 framework the CFPB proposes to implement under the NPRM. While we recognize the complexity of this regulatory environment, FDATA North America is significantly concerned that the NPRM's deference to prudential regulatory TPRM expectations could undermine the objectives of the Bureau's proposed rule and serve to formalize a view by covered data providers that the execution of bilateral data access agreements will be a prerequisite to enable consumer-permissioned data access even after the CFPB finalizes its Personal Financial Data Rights rulemaking. FDATA North America is principally concerned by the framing of §1033.321(a) and (b) of the NPRM, which provide that data providers may "reasonably" deny consumer or third-party access to a developer interface "based on risk management concerns" that are "directly related to a specific risk of which the data provider is aware."[20] Based on the significant experience our members have had over the last several years negotiating and attempting to negotiate bilateral data access agreements with financial institution data providers, we expect that this language will be interpreted by data providers as validation that contractual agreements to address perceived liability concerns with third parties and/or data access platforms will continue to be required for any consumer-permissioned data access to take place even after a final Section 1033 rulemaking. Such an outcome would do little to improve competition in the financial marketplace and would see the continued proliferation of an uneven consumer financial data access landscape.

To be clear: we do not view such a position by financial institutions as baseless. While the prudential bank regulatory agencies sought earlier this year to clarify TPRM responsibilities for financial institutions related to consumer-permissioned data access requests,[21] the expectations of data providers articulated under the new guidance remain ambiguous. Faced with this reality, financial institutions understandably have continued to view it as their obligation to codify duties and obligations on those market actors who are connecting to their systems through provisions

[19] *See* CFPB Proposes Rule to Jumpstart Competition and Accelerate Shift to Open Banking, https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-jumpstart-competition-and-accelerate-shift-to-open-banking/, issued October 19, 2023.
[20] *Id.*
[21] *See* Federal Register, Interagency Guidance on Third-Party Relationships: Risk Management, https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12340.pdf, issued June 9, 2023.

embedded in proposed bilateral data access agreements that financial institutions require consumer-permissioned data access platforms to execute as a condition of building permissioned data access connectivity for their consumers. The spread of these bilateral data access agreements has not served either the marketplace or consumers well. The CFPB noted in the materials it released accompanying the NPRM that one of the principal motivations for proposing a Personal Financial Data Rights rulemaking was to address the inconsistencies among these disparate agreements, noting, "their terms often vary in key respects that undermine the consistency of data access across the system."[22] In practice, the propagation of bilateral data access agreements has stymied competition in the marketplace and created barriers to entry for smaller data access platforms, as a requirement that a data access agreement be executed with each of the nearly 10,000 data providers covered under the NPRM is obviously not scalable.

Perhaps the thorniest area in each of these bilateral data access negotiations, which can take, in some cases, years from inception to execution, is the question of liability. FDATA North America is not aware of any bilateral data access negotiation in which a data provider did not represent their view that prudential regulatory TPRM expectations require the execution of a bilateral data access agreement that apportions liability in the event of an adverse customer experience. Unfortunately, we are concerned that the NPRM as currently proposed will effectively enshrine this perspective across the marketplace. By enabling data providers to restrict consumer-permissioned data access requests "based on risk management concerns" that are "directly related to a specific risk of which the data provider is aware," the NPRM empowers financial institution data providers to prohibit authorized third parties from accessing their developer interfaces without first executing a bilateral data access agreement, thus overriding their consumers' consent. Permitting compliance with the CFPB's proposed framework in such a way would diminish the basic tenet of personal financial data rights embodied in Section 1033 of the Dodd-Frank Act.

While we are deeply sympathetic to the TPRM requirements with which financial institutions are obligated to comply, we view the combination of the strong data security and privacy requirements included in the NPRM with the existing liability frameworks established under Regulation E and Regulation Z as entirely sufficient to protect financial institutions, and, more importantly, their consumers, from financial harm resulting from enabling consumer-permissioned data access requests. In particular, we note the Bureau's revisions in December of 2021 to its Electronic Financial Transaction Act Frequently Asked Questions, which provide guidance that nonbanks, including peer-to-peer payment providers, may be considered "financial institutions" under

[22] *See* CFPB Proposes Rule to Jumpstart Competition and Accelerate Shift to Open Banking, https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-jumpstart-competition-and-accelerate-shift-to-open-banking/, issued October 19, 2023.

Regulation E.[23] This more expansive approach to entities with Regulation E responsibilities provides robust consumer protections from unauthorized transactions resulting in financial harm.

To address the significant potential for the NPRM's provision of TPRM to serve as a rationale for a data provider to restrict data access, and the strong likelihood that the proposed framework will be interpreted as codification of the need for bilateral data access agreements to continue to exist in the ecosystem, the CFPB should coordinate with the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation ("FDIC"), and the Federal Reserve, and use its role as a Board member of the FDIC and as a member of the Financial Stability Oversight Council to advocate for amendments to the prudential regulators' joint TPRM guidelines in manner that ensures that the Bureau's Section 1033 rulemaking can be easily and uniformly implemented. We also encourage the Bureau to work with the prudential bank regulators to create clear and consistent standards upon which data providers and third parties may rely to ensure that data access facilitated under Section 1033 of the Dodd-Frank Act is conducted in compliance with prudential regulatory TPRM requirements.

The Bureau Should Consider Additional Quantitative Minimums for Data Provider Developer Interface Portals

The Bureau's NPRM recognizes the importance of ensuring that data provider developer interfaces are reliable and efficient methods through which to enable consumer-permissioned data access by mandating quantitative minimum interface standards. While FDATA North America commends the CFPB for requiring that data provider developer interfaces meet certain monthly uptime and response time standards, we are concerned that the NPRM fails to adequately ensure that developer interfaces can handle the volume of data required to enable consumers-selected third-party use cases. We also encourage the Bureau to include in a final Section 1033 rulemaking more stringent requirements pertaining to the accuracy of the data provided via developer interfaces. We view the inclusion of quantitative minimums for these attributes as essential given the CFPB's clear aspiration that all covered data requests will ultimately be facilitated through developer interfaces as opposed to other means. Finally, given FDATA North America's experience in other jurisdictions, we encourage the Bureau to carefully consider the efficacy of a regime in which data providers are ultimately responsible for self-reporting the performances of their respective developer interfaces.

The NPRM generally requires that a data provider's developer interface be available to facilitate consumer-permissioned data access requests at least 99.5 percent of the time as measured on a monthly basis and that such data requests be enabled, on average, in no more than 3,500 milliseconds. The inclusion of these two minimum quantitative standards is critical; however, the

[23] *See* Electronic Fund Transfers FAQs, https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/, issued December 13, 2021.

CFPB should consider that bilateral data access agreements that have been executed to date generally require more rigorous developer interface uptime and response time minimums. We encourage the Bureau to contemplate the potential that setting minimum standards for these two developer interface criteria below existing market norms could paradoxically create a "race to the bottom" over time wherein existing developer interfaces that perform significantly better than the NPRM's minimum standards could degrade. As it crafts its final Section 1033 rulemaking, the CFPB should consider raising its proposed minimum quantitative standards for both areas.

We further believe the NPRM needs to provide a clearer prohibition on data providers implementing access caps that would restrict the ability of authorized third parties to access data based on a consumer's direction to do so. While the NPRM appropriately restricts a data provider from "unreasonably restrict[ing] the frequency with which it receives and responds to requests for covered data from an authorized third party through its developer interface" and notes within the analysis that this form of restriction can commonly manifest as an access cap, the NPRM allows a data provider to apply frequency restrictions "in a manner that is non-discriminatory and consistent with the reasonable written policies and procedures that the data provider establishes and maintains pursuant to §1033.351(a)."[24] FDATA North America does not view this approach as sufficient to adequately ensure data providers do not inhibit access in a method or form that could easily be construed as an access cap. Accordingly, we encourage the Bureau to issue alongside its final Personal Financial Data Rights rule guidance that makes clear the limited circumstances under which data access frequency restrictions may reasonably be implemented by data providers.

The NPRM similarly does not include any minimum quantitative standards pertaining to the accuracy or quality of covered data that data providers must make available through developer interfaces. While §1033.351(c)(1) of the NPRM would require covered data providers to create and maintain policies and procedures "reasonably designed to ensure that covered data are accurately made available through the data provider's developer interface,"[25] no provision is made under the proposed rule for ensuring that these policies and procedures actually assure the accuracy of the data made available through a developer interface. We therefore encourage the Bureau to include data accuracy requirements for data providers' developer interfaces that make clear that substantively identical covered data provided to the consumer through the data provider's consumer-facing portal must also be made available through the data provider's developer interface.

Finally, the NPRM would require data providers publicly disclose the performance of their developer interface on a monthly basis. The experience of other markets in which data providers are required to self-report the performance of their developer interfaces, including the U.K., has demonstrated the importance of regulatory oversight over and validation of the data providers'

[24] *Id.*
[25] *Id.*

published performance metrics.[26] To ensure that data provider developer interfaces perform as intended under the NPRM, and that consumers have unfettered access to take advantage of the financial tools, products, and services that a more vibrant, competitive financial services marketplace will offer, it is vitally important that the CFPB provide for regular testing of data providers' developer interfaces against the quantitative minimum standards included in the final Section 1033 rulemaking.

The Final Rule Should Clarify that Forced Intermediaries May Not Assess Fees for Consumer-Permissioned Data Access

We applaud the inclusion of a clear prohibition in the NPRM from data providers imposing any fees or charges on either a consumer or an authorized third party in connection with either establishing or maintaining a developer interface or processing requests or making covered data available through a developer interface. This bright-line restriction appropriately reflects the notion that the transaction, balance, identity, and other non-proprietary data held by a provider of financial services belongs to the consumer who holds an account with that provider, and that the consumer should not be required to bear any costs associated with accessing their own data.

The inclusion of this restriction is timely. As one example, some large financial institutions have over the last several months informed consumer-permissioned data access platforms of their intention to block any consumer-permissioned, third-party data access that is not facilitated through a forced intermediary utility, Akoya, which owned by the largest financial institutions in the country. In some cases, the utility has indicated its intention to impose fees as a condition of permitting consumer-permissioned, third-party data access. The consequence of this behavior has been to significantly impair the abilities of consumers of some financial institutions to utilize third-party financial products, tools, and services, as data access platforms have historically taken the position articulated under the NPRM: that consumers should not be charged for accessing their own financial data. More broadly, the ability of incumbents to assess fees to allow their consumers to access and share access to their financial data, if permitted to propagate within the financial marketplace, would stifle competition and hamper innovation.

The NPRM does not in our view clearly enough address this pressing issue. As the Bureau considers its final rule implementing Section 1033 of the Dodd-Frank Act, we urge it to consider amending §1033.301(c) of the NPRM to clarify the subsection's application not only to data providers themselves but also to any incumbent-owned utility to which a data provider may outsource in order to satisfy the obligations of §1033.301(a). We view this modification as

[26] *See, for example,* U.K. Competition and Markets Authority letters to Barclays Bank U.K. and Lloyd's Banking Group, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1061957/final_public_letter_Barclays_bank__Part_2___public_version_.pdf and https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1061956/LBG_Article_12_draft_public_letter__public_version_.pdf, both issued March 21, 2022.

consistent with the overall intention of this provision of the NPRM and as a critical measure towards ensuring a more competitive financial marketplace in which consumers have unmitigated potential to choose from a wide range of financial services providers and that they be able to do so without cost.

To be clear, FDATA North America does not believe that any data provider should be required to provide consumer-permissioned third-party data access to proprietary data under a Personal Financial Data Rights rulemaking. The NPRM appropriately excludes such data from the purview of the rule under §1033.211(a). To the extent that a data provider applies analytics to covered data, cleanses or categorizes data, or holds confidential information, we agree with the notion that a data provider should not be obligated to make such data available through its developer interface, but that market stakeholders may continue to negotiate and execute agreements bilaterally to access and utilize such data with a consumer's express, informed direction to do so.

Ensuring that a Data Provider's Authorization Confirmation Does Not Induce Undue Friction in the Consumer Journey

FDATA North America commends the Bureau for acknowledging in its NPRM that third parties are appropriately positioned to obtain authorization from consumers to share elements of their covered financial data. By proposing a framework under which third parties must meet certain consumer disclosure and consent requirements as a condition of being deemed authorized, the NPRM achieves its dual objectives of ensuring consumer protection while encouraging competition.

The NPRM does, however, propose to allow data providers to confirm with a consumer the account(s) to which an authorized third party is seeking access and the categories of covered data the third party intends to access with the consumer's consent. We do not believe this framework is necessary and are concerned that it is needlessly burdensome. The Bureau's proposed rule requires that authorized third parties provide consumers with a simple process through which to revoke their authorization and clear disclosures outlining that process, ensuring that end users maintain full control over how their data is accessed and used by authorized third parties at all times. Given this consumer control, the strong consent, disclosure, data privacy, and data security requirements for authorized third parties included in the proposed rule, the transition the NPRM provides from credential-based authentication to more secure methods, as well as the broad ability afforded to data providers under §1033.321 to deny authorized third-party data access over concerns related to risk management, specific risks, or a lack of information, it is not clear to us that affording a data provider with the ability to confirm a consumer's authorization every time they seek to share data with a third party conveys any measurable consumer benefit. On the other hand, in practice, this provision if included in a final rule, would likely become standard practice for the vast majority of data providers, which will result in longer consumer onboarding processes with third-party providers of financial services, products, and tools that will, over time, hamper competition.

FDATA North America is also concerned that the data provider authorization confirmation process could be viewed as an opportunity by a data provider to attempt to thwart a consumer's access to third-party providers. While we suggest that the CFPB clarify in its final rule that a data provider may confirm a consumer's authorization to share access to their data with an authorized third party only when reasonably necessary, we encourage the Bureau to clarify that any instance in which a data provider deploys an authorization confirmation may not be used to market their own product, tool, or service or otherwise discourage a consumer from using the third-party provider to which they have already provided their authorization.

The Use of Tokenized Account Numbers Disrupts Existing Use Cases and Should Be Removed from the Rulemaking

The NPRM proposes to permit data providers to "mak[e] TANs available to authorized parties in lieu of full account and routing numbers,"[27] so long as the TAN "contained sufficient information to initiate payment to or from a Regulation E account."[28] While FDATA North America understands the Bureau's intention of including this provision in its Personal Financial Data Rights proposal is "mitigating fraud risks,"[29] we are concerned that the significant technological challenges posed by the deployment of TANs requires independent review by not only the CFPB but also the prudential bank regulators. As a result, we strongly suggest that the CFPB remove from its final rulemaking Example 1 to §1033.211(c) of the NPRM, which would allow data providers to use a tokenized account and routing number "instead of, or in addition to a non-tokenized account and routing number."[30] To the extent the Bureau wishes to consider the transition by the financial services marketplace towards TANs, we respectfully suggest that it should do so under a separate rulemaking.

Over the last several years, some large financial institutions have mandated through bilateral data access agreements that the only mechanism through which to facilitate consumer-permissioned access to account and/or routing numbers is through the use of masked or tokenized data. In practice, the deployment of this technology has significantly impaired or altogether broken a number of third-party use cases for certain third-party users of consumer permissioned data, including payment risk evaluation, bill payment and payment initiation. These outcomes have ultimately led to impaired service for consumers, which we believe outweighs the advancements that have been made to the deployment of TANs to date, particularly given the NPRM's strong data privacy and security provisions, and the framework it requires to ensure that consumers have full control of and transparency into how their financial data is accessed and used at all times.

[27] *Id.*
[28] *Ibid*
[29] *Ibid.*
[30] *Ibid.*

The Bureau should also consider that TANs have somewhat perversely enabled a new means through which bad actors have increasingly sought to commit fraud in the last several years. Using a TAN, a fraudster will apply for multiple loans using the same bank account. Because only a TAN is provided, the lender is unable to determine that it is in fact making multiple loans to the same consumer. The bad actor will then revoke access after the loan is disbursed, thus disabling third parties' ability to determine which account the funds went to, making it impossible to identify the account originating the fraud or to recover the funds. One FDATA North America member has reported that financial institutions that have deployed TANs accounted for as much as 80% of its R04/invalid account number returns in October or 2023.

To the extent that the CFPB does ultimately decide to retain the NPRM's proposed provision of TANs in its final Personal Financial Data Rights rulemaking, it is critically important that the Bureau provide clarification regarding the instances in which TANs may be deployed under the final rule. For example: TANs are not currently usable for any FedNow payments or for some RTP payments. As a result, facilitation of payments use cases under a final Section 1033 rulemaking by authorized third parties that rely on TANs would inherently settle more slowly than payments facilitated by incumbents that have onboarded with FedNow or RTP. To address this issue, the CFPB should either remove TANs entirely from its rulemaking or clearly articulate in its final rule the circumstances in which TANs may not be utilized in order to maintain a competitive consumer payments marketplace.

Finally, if the Bureau opts to include TANs in its final rule, we urge the CFPB to make clear that an individual TAN issued by a data provider should persist for as long as the consumer has provided their authorization to a third party to access their data. Deployment of multiple TANs under the same consumer authorization will cause recurring payments to fail, which can lead to late fees and other consumer harms through no fault of the consumer themselves. Provision in the final rule that a TAN must persist so long as the consumer has authorized a third party to access it will ensure that consumers' payments are facilitated as they directed them to be to an authorized third party.

FDATA North America understands the Bureau's interest in TANs as a technology with the potential to increase consumer protection in the financial ecosystem. But, given the complexities associated with TANs, we request the CFPB utilize a separate rulemaking to the extent it seeks to create regulatory requirements pertaining to masked or tokenized data, including for account numbers.

A Fallback Method of Consumer-Permissioned Data Access is Required

As FDATA North America has conveyed to the CFPB consistently since the Bureau first began consideration of a Personal Financial Data Rights rulemaking in 2016, all market stakeholders, including data providers, consumer-permissioned data access platforms, and third-party financial services providers support a transition away from credential-based data access methods in favor

of the efficiency and security afforded by the developer interfaces mandated under the NPRM. But a final rule implementing Section 1033 of the Dodd-Frank Act must recognize that, even after the implementation timeline mandated under the NPRM, there will still be instances in which consumer-permissioned data is not accessible via a developer interface for any number of reasons. For covered data, this may be because a developer interface is not accessible, data accuracy issues exist in a developer interface, or a data provider is noncompliant with the CFPB's rulemaking. The Bureau should also recognize, as we outlined earlier in this submission, that, as currently constructed, a wide range of financial accounts are not included under the NPRM. As a result, it is unlikely that all covered data providers will elect to voluntarily add data included in these accounts to their developer interfaces in the absence of any regulatory mandate to do so, making legacy technology the only method through which consumers may direct third parties to access their data.

To ensure that consumers may maintain the ability to benefit from a competitive ecosystem of financial products, services and tools, and consistent with the approaches of other jurisdictions that have implemented open finance regimes, we encourage the CFPB to clarify in its final Personal Financial Data Rights rule that credential-based authentication or PII and account number-enabled access, both of which are widely used today by financial institutions to authenticate their own customers, may serve as a permissible option to facilitate consumer-permissioned data access in instances in which no developer interface is available or the data provided through a dedicated access portal is incomplete or unreliable. The approach included in the NPRM would impose a requirement on data providers that they prohibit consumer-permissioned third-party access to data once they have established and maintained a developer interface; however, the proposed rule makes no provision for ensuring consumers may continue to permission access to their financial data to authorized third parties in circumstances in which a developer interface's reliability, data quality, or responsiveness is unstable, or in which a data provider's interface does not include accounts that are not covered by the Bureau's Section 1033 rulemaking but for which a consumer has provided their direction to a third party to access. In these circumstances, the only method to ensure that a consumer maintains the ability to access third-party financial products, tools, and services – including those that may already rely on today – is for the Bureau to allow for credential-based authentication or PII and account number-enabled access to be protected.

FDATA North America recommends that the Bureau stipulate in its final Section 1033 rulemaking that any qualified industry standard recognized by the CFPB under the final rule must develop and enforce criteria that make clear the circumstances under which a data provider may not restrict the use of a fallback option to facilitate a consumer's request to access or share access to their financial data. In such cases, an authorized third-party accessing data using a fallback option to access consumer data should still be required to comply with the authorization, disclosure, and other third-party obligations articulated under the NPRM. Such a framework would ensure that even when legacy technology is the only means through which a consumer's data may be accessed at their direction, strong consumer protections will exist under which the data access is facilitated. This approach would also have the benefit of providing a market incentive for data providers to build

and deploy developer interfaces that contain data beyond what is minimally required under the NPRM.

The Fair Credit Reporting Act Should Not Apply When Entities Facilitate Covered Data Access

The commentary provided alongside the NPRM asserts, without precedent, that consumer-permissioned data access platforms should be considered consumer reporting agencies under FCRA in instances in which they facilitate, at a consumer's direction, access to data for a credit decisioning use case and otherwise meet the requirements of the FCRA. FDATA North America urges the Bureau to reconsider this approach, as FCRA was neither intended nor designed to capture the activities of consumer-permissioned data access platforms. Moreover, the significant consumer protections included in the NPRM required to be implemented by both authorized third parties and consumer-permissioned data access platforms, including clear disclosure and consent management, data privacy standards, and data revocation enablement, among myriad others, in our view provides an appropriate, comprehensive, and eminently more workable framework through which to ensure end users are protected when they grant permission to access elements of their financial data.

In contrast to the credit reporting marketplace that existed in 1970 when Congress first enacted FCRA, end-to-end consumer control and transparency is an inherent feature of the consumer-permissioned financial data marketplace. When account connectivity is first established with an authorized third-party financial service provider, data access platforms typically present conspicuous disclosures regarding what data is being accessed, for what purpose, and for what length of time. Such disclosures will be mandatory under the proposed rule. In many cases, financial institutions, in coordination with data access providers and data recipients, present to their account holders a dashboard enumerating the various data connections they have established to their accounts, and which data elements they have permissioned to fuel the use cases for which they have connected. The consumer's control of their data in the consumer-permissioned financial data marketplace, which a final Personal Financial Data Rights rulemaking will codify, is a key feature of the ecosystem in which third-party financial providers and data access platforms operate today.

The type of data collected and the manner of data collection conducted by consumer-permissioned third parties operating under a final Section 1033 rulemaking is very different than traditional consumer reporting agencies. Consumer-permissioned third-party providers can only make use of the specific data fields to which the consumer has expressly granted them access, and, as a general rule, only access that data under scenarios for which the consumer has requested that they do so and for only the purpose(s) authorized by the consumer. Consumer-permissioned data access platforms never access a consumer's data unless they have been granted consent from that consumer to do so.

Subjecting data access platforms to the requirements of FCRA when they are providing consumer-permissioned data access for lending and other credit-decisioning use cases would pose significant and negative implications for consumers. To the extent that consumer-permissioned data access platforms are required to function as credit reporting agencies under FCRA, financial institutions may be required to become furnishers under the statute for certain use cases to which their customers had elected to share their data. Such an obligation on financial institutions would very likely result in restrictions on the types of third-party tools offered to end users and would impose significant new legal and compliance burdens on large and small financial institutions. Without a bilateral data access agreement in place to address perceived FCRA-related liability issues, financial institutions could elect to restrict consumer-permissioned access to data by credit decisioning use cases under the "reasonable denials related to risk management" provisions set forth under §1033.321 of the NPRM. This outcome would undermine the principal objectives of Section 1033 of the Dodd-Frank Act: facilitating greater competition and lowering fees in the financial marketplace and providing consumers with the ability to select the third-party providers best positioned to help them manage their finances. This desired outcome naturally should extend to providing consumers with the ability to select from a competitive marketplace of affordable, mainstream credit opportunities.

Application of FCRA's dispute resolution mandates would also create confusion if applied to consumer-permissioned data access under Section 1033 of the Dodd-Frank Act. Indeed, the proposed rule's own requirements around data use, authorization disclosures, and accuracy requirements, among others, are in tension with those of the FCRA, which would create acute compliance challenges for institutions navigating the complexity and overlap between Section 1033 and FCRA.

The data accuracy requirements are a case in point: While FCRA generally requires consumer reporting agencies to correct inaccurate data within 30 days of a consumer's dispute, platforms that facilitate consumer-permissioned data access are merely providing authorized third parties selected by the consumer with access to data held by another financial services provider. These platforms do not have the ability to correct inaccurate data held by a data provider and any requirement that they do so within a 30-day period creates significant risk that diverging consumer records would be created: one held by the original data provider; an alternate version that has been "corrected" by the consumer-permissioned data access platform; and potentially several other versions maintained by third-party data recipients to which the consumer has permissioned the use of their data. Indeed, the proposed rule expressly limits Section 1033's accuracy obligations to the transmission of data, creating two different accuracy standards that in many cases will apply to the same data.

While we wholeheartedly agree with the notion that consumers should have full transparency into and control over how their financial data is being used, for what purpose it is being accessed, and by whom, FDATA North America does not believe that applying FCRA to instances in which consumer-permissioned data access platforms are merely facilitating access to credit decisioning

use cases conveys any additive consumer protections than what the NPRM already proposes to establish for both data access platforms and authorized third parties. The corresponding and significant risks of consumer harm and confusion in requiring data access platforms to assert themselves as credit reporting agencies should serve as a rationale for the CFPB to exclude from its final Personal Financial Data Rights rule any such requirement.

The CFPB Should Directly Supervise Consumer-Permissioned Data Access Platforms

At every stage of the Bureau's consideration of a rulemaking implementing Section 1033 of the Dodd-Frank Act, FDATA North America has encouraged the CFPB to utilize its statutory authority to directly supervise consumer-permissioned data access platforms. Although the NPRM makes no reference to doing so, we take this opportunity to once again urge the Bureau to consider utilizing its larger participant authority to undertake supervision of these important market stakeholders. Doing so would allow the Bureau to more actively monitor the consumer data access ecosystem but also should be considered as a pathway to meaningfully address the challenges presented by the prudential bank regulator TPRM concerns we articulated earlier in this submission.

From a consumer protection standpoint, a supervisory regime for consumer-permissioned data access platforms would enable the CFPB to extend TPRM-like supervisory guidelines and expectations to the companies that facilitate consumer-permissioned data access throughout the ecosystem. The data access platforms would then be able to rely on those guidelines as they onboard and partner with authorized third parties, ensuring an even application of the data minimization, privacy, security, and risk management requirements for third parties articulated under the NPRM. Given the critical role that data access platforms play today and will continue to play after implementation of the Bureau's Personal Financial Data Rights rulemaking, in oversight of third-party usage of and access to consumer-permissioned financial data, the application of this type of TPRM-like regime would meaningfully benefit the ecosystem and the consumers it serves.

Supervision of data access platforms would also provide an avenue to address the potential for the prudential bank regulators' TPRM guidance to undermine the objectives of the CFPB's Section 1033 rulemaking. By extending direct supervision to consumer-permissioned data access platforms, the Bureau and the prudential regulators could provide a safe harbor for federally regulated financial institution data providers covered under the Bureau's final Section 1033 rulemaking to allow consumer-permissioned data access with CFPB supervised entities without a requirement for extending additional TPRM requirements to those platforms. Such a framework would ensure that data providers need not execute bilateral data access agreements with any authorized data access platform or third party that seeks to access its developer interface, ensuring a vibrant and competitive financial marketplace is permitted to thrive once the Bureau finalizes its Personal Financial Data Rights rulemaking.

Conclusion

Once again, FDATA North America appreciates the thoughtfulness with which the CFPB has crafted its NPRM implementing Section 1033 of the Dodd-Frank Act. Once finalized, the rule will provide consumers with meaningfully more control over their financial data, improve competition in the financial marketplace, and allow the U.S. to keep pace with the many other countries and jurisdictions that have adopted their own open finance frameworks. To fully realize the benefits of a Personal Financial Data Rights rule, we encourage the Bureau to make the following amendments to its NPRM before finalizing its regulation:

- Expand the scope of covered accounts under the rule to include public benefits, investment, retirement, and other types of non-transaction accounts held at traditional financial institutions, as well as mortgages, auto loans, and all forms of time deposit accounts.

- Adjust the NPRM's proposed limitations on secondary data usages to both exclude de-identified data and to ensure that existing use cases with significant consumer and economic benefits are not inadvertently hindered.

- Work closely with the FDIC, OCC, and Federal Reserve to secure amendments to the prudential regulators' TPRM requirements in a manner that ensures that the Bureau's Section 1033 rulemaking is deployed as intended.

- Amend the proposed minimum quantitative standards for developer interfaces to ensure that consumers may provide authorized third parties with consistent access to accurate data.

- Extend the NPRM's prohibition on data providers from assessing fees to build or maintain their developer interfaces or to enable consumer-permissioned data requests through their developer interfaces to any incumbent-owned utility a data provider utilizes to satisfy its obligations under the rule.

- Ensure that data provider authorization confirmation processes do not introduce undue friction into a consumer's onboarding experience with an authorized third party.

- Eliminate the NPRM's proposal to facilitate a transition to TANs.

- Clearly provide as a condition of recognition of a qualified industry standard that legacy technologies may be utilized to access data with a consumer's permission in circumstances in which a data provider's developer interface may not be reasonably used for that purpose.

- Exclude consumer-permissioned data access platforms from a requirement to assert themselves as credit reporting agencies under FCRA in instances in which they are simply enabling consumer-permissioned access to covered data for credit-decisioning use cases.

- Provide through a separate "larger participant" rulemaking for direct supervision of consumer-permissioned data access platforms.

On behalf of FDATA North America, thank you for your consideration of our comments in response to the NPRM and for your continued work on this critical issue. We look forward to continuing to serve as a resource for the CFPB as it finalizes its Personal Financial Data Rights rule next year.

Sincerely,

Steven Boms
Executive Director