www.fdata.global/north-america

March 2, 2022

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930

Sent via electronic mail to nistir-8389-comments@nist.gov.

RE: NISTIR 8389 (Draft): Cybersecurity Considerations for Open Banking Technology and Emerging Standards

The Financial Data and Technology Association of North America ("FDATA North America") appreciates the opportunity to submit comments to the National Institute of Standards and Technology ("NIST" or "the Institute") in response to its draft paper on Cybersecurity Considerations for Open banking Technology and Emerging Standards.

As the trade association representing open banking use case providers and enablers in the United States and Canada, we respectfully offer that the current draft of NISTIR 8389 would benefit from certain revisions to more accurately define open banking systems, articulate the central role of regulatory leadership in well-implemented open banking frameworks, and reflect the technological realities under which open banking solutions are currently delivered in the United States and in other jurisdictions across the globe.

About FDATA North America

FDATA North America was founded in early 2018 by several financial firms whose technology-based products and services allow consumers and small businesses ("SMBs") to improve their financial wellbeing. We count innovative leaders such as the Alliance for Innovative Regulation, APImetrics, Basis Theory, Betterment, BillGo, Codat, Direct ID, Equitable Bank, Experian, Finansytech, Fiserv, Flinks, Interac, Intuit, Inverite, Kabbage, Mogo, Morningstar, M Science, MX, Petal, Plaid, Questrade, SaltEdge, Trustly, ValidiFi, Vaultree, VoPay, Wealthica, and Xero, among others, as our members.

We are a regional chapter of FDATA Global, which was the driving force for open banking in the United Kingdom, and which continues to provide technical expertise to policymakers and to regulatory bodies internationally that are contemplating, designing, and implementing open finance frameworks. With chapters in North America, Europe, Australasia, Latin America, and India, FDATA Global has established itself as an expert in the design, implementation, and governance of open finance standards and frameworks globally since its inception in 2013.

www.fdata.global/north-america

As the voice of third-party providers of financial technology use cases and leading advocates of open banking in the United States and Canada, we are pleased to provide this response to draft NISTIR 8389. Our letter contains an overview of our critiques, discussion of our views on open banking generally, and a sectional analysis with specific responses to components of the draft report.

Critical Overview

NIST has a long tenure of producing well-regarded research on a variety of complex issues which influences decision makers across all levels of government and in the private sector, and its work on financial issues is regularly relied upon for decisions made by banking regulators. While we appreciate the Institute's research in this important policy space, we respectfully offer that, given the weight and influence of such publications on the myriad of public policy decisions currently under consideration, NISTIR 8389 would significantly benefit from revisions and input from market and government stakeholders to appropriately frame the current open banking environment in the United States as well as to accurately reflect the significant regulatory attention that has already been given to this space.

As one of the earliest federal government research publications on open banking, it is crucial that this report accurately define and describe all the elements of open banking that are relevant to policymakers. Unfortunately, in many cases we believe that NISTIR 8389 overlooks such critical guidance. From the onset, the definition and framing of open banking is too narrow, and critical distinctions between customer-permissioned data access – the foundation of open banking – and non-permissioned data mining, as well as the important differences between propriety and non-proprietary data, are insufficiently distinguished. Use cases are inaccurately described, and the full impact of Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") on the development of open banking in the United States could be better articulated. Screen scraping, which is currently the predominant method of financial data sharing in the United States and globally, is never defined and only mentioned in passing in the section discussing regulatory frameworks in the United Kingdom and the European Union. As a result, this report will leave unsophisticated readers with the erroneous conclusion that open banking relies entirely on Application Program Interfaces ("APIs"), which is incorrect in both the United States and in jurisdictions that have more advanced open banking regulatory frameworks.

FDATA NA is concerned that certain errors and omissions in this paper, which we will detail in the sectional analysis, could misinform both the public and key policymakers as they develop open banking regulations. We respectfully offer that NIST should seek further input from experts and key stakeholders in the open banking field, including data aggregation firms, financial institutions, third-party financial services providers, and financial regulatory agencies, all of whom are currently providing open banking solutions in the United States and/or are contemplating the intersection of open banking and regulatory policy. This combination of NIST's internal academic thought-leadership and outside industry expertise would result in a

more comprehensive document. In the absence of such stakeholder engagement, we are concerned that this draft paper also does not fully appreciate the market and regulatory environment in which open banking use cases are currently delivered to consumers and small businesses in the United States today and will be in the future.

The Sectional Analysis will provide our practitioner perspectives on the current state of open banking in the United States, and specific feedback on items where we believe NISTIR 8389 would benefit from further elucidation. We therefore urge NIST to consider the input provided herein, and from other key stakeholders, and republish a revised version of this report.

Open Banking in the United States

Benefits of open banking: A formalized, legal consumer financial data right for United States consumers and small businesses has the potential to improve financial access and inclusion by providing greater access to safe and affordable credit for thin or no-file borrowers; facilitating access to savings tools; and enabling secure, technology-enabled payment and budgeting tools for Americans with little or no access to traditional bank accounts. FDATA North America has long advocated for the development of open banking regimes through the "hybrid approach" outlined in NISTIR 8389, in which government leads in the development of policies and regulations and the market is then responsible to deliver a thriving, competitive marketplace of financial services and products that improve customer choice and financial access and opportunity. Across all the open banking markets in which FDATA Global operates, policymakers have led the way by first providing regulatory clarity that implements a uniform set of customer rights and protections. Unfortunately, in the absence of regulatory intervention in the United States, a market-driven approach has on its own, led to some market inefficiencies that could be solved by regulation.

While the United States has seen significant growth in the third-party financial provider marketplace, the ability of all customers to utilize third-party tools remains stymied. The absence of universal rules or guidelines governing all providers means that a customers' ability to share their own financial information in many instances depends on which financial institution they hold accounts with. Over the last several years, this uneven playing field has been largely dictated by bilateral data access agreements between financial institutions and customer-permissioned data aggregation firms, which establish reliability and protections for customers and providers, but again tend to differ depending on the agreeing companies. Accordingly, consumers and small businesses' experiences with open banking the US tend to differ widely, and some are left out entirely.

In this context, we eagerly await the finalization of the CFPB regulation implementing Section 1033 of Dodd-Frank, which this draft report accurately identifies as the most critical United States statute to the development of open banking. In our response to the CFPB's October 2020 Advance Notice of Proposed Rulemaking ("ANPR") implementing Section 1033 of Dodd-Frank,

we highlighted several elements that we believe to be keys to success in the proliferation of a true open banking framework in the United States: the creation of a legal consumer financial data right, clear definitions of limited circumstances in which data custodians can override consumer consent, direct CFPB supervision of data aggregators, and a technology-agnostic approach that allows for full operability of current and legacy technologies. Of particular importance, we believe that any non-proprietary data element that is available to an end user through their online banking portal or is included on a paper statement, and that is not the intellectual property of the data holder, should be permitted to be shared with a third-party service provider by any consumer or small business.

Third-party oversight: FDATA North America and our member companies see competition in data-driven financial services stifled by financial institutions that override customer direction to authorize sharing of their financial data, often citing cybersecurity concerns. 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. In each of these cases, competition is substantially inhibited, to the direct and severe detriment of consumers.

The current supervisory regime crafted by United States banking regulators places all responsibility and oversight for third-party risk management on financial institutions themselves, which provides them the basis for unilaterally blocking or restricting third-party providers' access to the customer data they hold. As a solution, we have long offered that the best way to address these third-party risk concerns, and to remove the need for bilateral data access agreements, is the creation of a new federal supervisory regime for data aggregation platforms. Such a supervisory regime should establish a principles-based foundation for data, cyber, and information security practices as well as governance over aggregation firms. The third-party providers of financial services that FDATA NA represents are willing and able to shoulder any appropriate responsibility for cybersecurity and consumer redress that such a supervisory regime would impose.

APIs and screen scraping: While FDATA NA is technology neutral and supports the transition to API access of customer-permissioned financial data, the United States financial system is not yet ready to eliminate existing technological methods of accessing customer data without massive detriments to consumer financial health. This is a lesson clearly learned from other, more advanced markets, which, as the draft paper rightly notes, retain screen scraping as a connectivity method either as a fallback option or for data not available through APIs. In the absence of a fully developed, robust API environment in the United States, screen scraping is a necessary tool to enable consumer and small business data access, particularly for customers of all but the largest United States financial institutions.

Our ANPR response further urged the CFPB to contemplate a "technology-agnostic" approach to the rulemaking which would avoid directly requiring any particular technological form (API, screen scraping, or otherwise) for the sharing of customer financial data. In order to guarantee consumers consistent, reliable access to their own information, this approach must also provide market participants with sufficient flexibility to maintain interoperability of legacy forms of data storage and communication, while also allowing for full integration of any future methods that do not yet exist. We therefore appreciate NIST's clearly stating in this report that "Any proposal of a specific API that would be compatible across heterogeneous systems was purposely avoided in this report," although we would stress, as we do below, that APIs are not necessarily the only technology that can support open banking.

Sectional Analysis

Section 1

While 1.1 accurately describes the benefit to individual consumers provided by open banking, it neglects to mention similar benefits to small businesses, which should be considered in scope of any open banking regime. These enterprises will also receive significant benefits to their financial wellbeing from an open banking system, particularly in meeting their unique credit needs, streamlining and reducing costs of accounting and tax compliance, and managing their finances as they grow. Further, small businesses in the United States are already benefitting greatly from third-party financial data sharing innovations that provide, among many services, streamlined accounting and billing, tax compliance, and critical credit access.

The discussion of multiple financial institutions in 1.2 contains the odd assertion that customers "may be forced to accept most or all of a package of services offered by a financial institution." While customers may find it easier to use multiple financial products from a single financial institution, empirical data disputes this assertion. The majority of United States consumers and small businesses hold multiple different financial accounts across a range of different providers, with one recent study finding the average United States consumer has more than five different accounts spread across multiple financial institutions and third parties[1]. We respectfully submit that this is an essential notion for the authors to understand, as, oftentimes, the most beneficial open banking use case for a customer is the most straightforward: seeing all of their financial accounts in one place at the same time.

The definition of open banking in 1.3 is critical to accurately frame the rest of the paper, but unfortunately, we find this definition lacking. Once again, we would note that small businesses, not just individual consumers, must be considered as within the scope of a U.S. open banking regime. Additionally, this proposed definition would exclude the majority of the existing customer-permissioned financial data marketplace today, as it would require a comprehensive

[1] Mercator Advisory Group. "ATM Banking: It's Not Just About Cash Withdrawal Anymore." (June 2019).

API environment, which neither exists today nor is likely to exist in market for the foreseeable future. As the paper notes later on, even those markets that are significantly more mature in their open banking journeys make broad use of screen scraping and do not rely solely on API connectivity.

NISTIR 8389 neglects to mention the importance of screen scraping in its overview of open banking, mentioning it only in passing later on, and does not provide a clear definition. We offer that "screen scraping" can be defined as the utilization of software to access customer-authorized data from their native online banking portal or mobile application and is critical method of accessing data with the end user's consent and permission. Since the vast majority of customer-permissioned financial data sharing in the United States currently occurs via screen scraping, the report's failure to clearly define this key technology leaves a significant hole in its coverage of open banking.

Furthermore, to ensure continued access to financial data for consumers and small businesses, "screen scraping" will have to continue until direct access methods are significantly robust to support the needs of end users. An FDATA survey in 2019[2] determined that hundreds of millions of United States accountholders would lose access to at least one critical data field on which a use case they currently used relief if the system switched entirely to APIs overnight. We feel that this omission creates a significant deficit in this paper's utility and its understanding of the current open banking marketplace in the United States.

This section also neglects to mention that third-party services which rely on data aggregation, such as financial planning applications and "dashboard" services that present consumers with consolidated financial profiles, would also greatly benefit from open banking; it is not just payment services using "the flow of debits and credits" that stand to benefit. By creating this narrow definition, the authors have inadvertently excluded a plethora of major open banking use cases that do not involve money movement. To wit: the latest data from the UK highlight the consistent value of non-payment related open banking use cases to consumers: of the 327 approved third-party providers in the UK, 234, or 71 percent are AISPs.[3]

Additionally, the authors' proposed definition of "open banking" states that "opening and sharing of data forces banking entities to make *proprietary* data available…" when in fact Section 1033 of Dodd-Frank provides that consumers' financial data belongs to the consumer. The data that is made available to end users in an open banking environment is not at all proprietary to the data holder: it belongs to the end user. While this may seem like a minor distinction, it is, in fact, a critical one. The notion that transaction data created by customer financial activity belongs to the consumer or small business and not the data holder is the foundational basis for open banking, and we suggest that this report must clarify this important

[2] FDATA NA 2019: "Opportunities in Open Banking"
[3] Open Banking UK: "August Highlights 2021"

point. For reference, FDATA NA has defined "proprietary data" as data that a data holder cannot be reasonably expected to allow their customers to share, which does not include data elements that are already required to be disclosed to the customer, such as fees and interest rates.

Section 2

Line 337 attempts to describe an open banking use case of debt collection; however the wording of this statement "using open banking, a debt collector can look into the accounts of the person and try to generate payment" is actually describing a case of data *mining*, which is qualitatively distinct from customer-permissioned data *sharing*. This wording could confuse policymakers and end users into thinking that open banking will weaken the individual agency and privacy consumers and small businesses have over their data in open banking regimes. FDATA NA has long stressed that customer permissioning is the keystone principle of open banking, and therefore use cases that do not wholly rely on customer permission are not within the scope of open banking. We do not and have not endorsed any business practice that makes use of consumer financial data without explicit and limited consent.

Section 4

We agree with the assertion on line 373 that the adoption of open banking in many countries will occur through a hybrid approach between both government and private actors. This statement further highlights the urgent need for the CFPB to finalize its Section 1033 rulemaking, as even a partial governmental mandate or set of standards can drive significant progress in this space-particularly given the complex barriers described in our overview.

This description of the UK's approach to open banking on line 446 is a critical point and aligns with our position on the importance of technology-neutrality which does not inherently require the use of APIs. Although we do support a gradual transition to this method of data sharing, it is worth noting again that the vast majority of customer-permissioned financial data sharing in the United States currently occurs via screen scraping, not APIs.

The assertion found on line 763 is unfounded in stating that "in view of the narrow scope of Section 1033, the CFPB's ability to establish an open banking system through regulatory authority remains unclear." In fact, Section 1033 of Dodd-Frank sufficiently authorizes and provides clear instructions to the CFPB to create a legally-binding consumer financial data right, which is the cornerstone for any open banking regime. Evidence for this authority was solidified in July 2021 when President Joe Biden signed an Executive Order directing the CFPB to "commencing or continuing a rulemaking under section 1033 of Dodd-Frank to facilitate the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new, innovative financial products." The language of this section of the order strongly suggests that Section 1033 sufficiently authorizes the CFPB to facilitate development of an open banking system in the United States.

Further, in its 2020 ANPR on Section 1033, the CFPB poses questions to the public that indicate its confidence in the expansive authority provided by the statute. While we have urged the CFPB to remain technology-neutral in this rulemaking, we feel that the establishment of a customer data right will be significant leap forward in the development of a United States open banking regime and clear the way for market participants to build out the infrastructure necessary to complete it.

The 2018 report from the United States Treasury Department cited in this report contains similar assertions as to the broad scope of the authority Congress granted to the CFPB under Section 1033. Page 33 of the report describes the conflicting views of the coverage of Section 1033, but "recommends that the Bureau affirm that for purposes of Section 1033, third parties properly authorized by consumers, including data aggregators and consumer fintech application providers, fall within the definition of "consumer" under Section 1002(4) of Dodd-Frank for the purpose of obtaining access to financial account and transaction data." FDATA NA is aligned with this recommendation and concurs that the definition of "covered persons" under Dodd-Frank is broad enough, when combined with Section 1033, to provide the CFPB with the scope necessary to facilitate development of a United States open banking regime.

The liability considerations described around line 767 are indeed a significant barrier to open banking and modernization of the United States payment infrastructure. One of the biggest points of contention faced by financial institutions and third-party providers in the negotiation of data access agreements is precisely this liability- the determination of which entity is responsible for making a customer whole when funds are improperly transferred. As such, this remains one of the largest barriers to the development of open banking in the United States. Thankfully, just prior to publication of this report, the CFPB in December 2021 published on its website updates to its Frequently Asked Questions relating to the Electronic Funds Transfer Act ("EFTA") and its implementing Regulation E, over which the CFPB has partial authority.

Critically, the FAQs state that unauthorized transfers now include situations when a consumer is fraudulently induced into sharing account access information with a third party, or when such credentials are obtained from a third party through fraudulent means such as computer hacking- and applies the preexisting Regulation E Error Resolution requirements to such situations. Though less impactful than formal regulatory action, this clarifying material helps advance a modern liability framework in the digital payments system, and by extension, the forthcoming structure of open banking in the United States.

We therefore believe that the CFPB's existing positions on Regulation E, combined with the Section 1033 are sufficient to provide it the necessary authority to jumpstart development of a United States open banking system. By creating clearly defined lines of legal responsibility and regulatory oversight, the CFPB can make strides in helping the industry overcome these thorny legal barriers which have stubbornly hindered progress. The key point is that these standards

must be the same for each financial institution in order to realize the basic principle of open banking that all users must have equal access to their financial data.

Due to the recent the publication of the updated FAQs, this report understandably does not mention them; however, we feel that these updated FAQs are significant to the topic of this report and suggest that any later version include their mention and discussion.

Conclusion

The future of the customer-selected financial technology providers we represent is dependent on their ability to work with customers to offer innovative digital products. As FDATA NA eagerly awaits the finalization of the CFPB's rulemaking under Section 1033 of Dodd-Frank, we encourage the authors of this paper to undertake the revisions outlined in this letter to more accurately reflect the current state of open banking in the United States.

Thank you in advance for your consideration of our perspectives.

Sincerely,

Steven Boms,
Executive Director