http://www.fdata.global/north-america

September 23, 2021

Chief Counsel's Office
Attn: Comment Processing
Office of the Comptroller
of the Currency
400 7th St. SW, Suite 3E-218
Washington, DC 20219

Ms. Ann E. Misback
Secretary
Board of Governors of the
Federal Reserve System
20th Street and Constitution Ave. NW
Washington, DC 20551

Mr. James P. Sheesley
Assistant Executive Secretary
Attn: Comments-RIN 3064-ZA26
Federal Deposit Insurance Corporation
550 17th St. NW
Washington, DC 20429

Re: Proposed Interagency Guidance on Third-Party Relationships: Risk Management
Agency/Docket Numbers:
Docket No. OP-1752
Docket ID OCC-2021-0011
RIN:3064-ZA26

The Financial Data and Technology Association of North America ("FDATA North America") appreciates the opportunity to submit comments to The Board of Governors of the Federal Reserve System ("the Board"), the Federal Deposit Insurance Corporation ("FDIC"), and the Office of the Comptroller of the Currency's ("OCC") proposed interagency guidance and request for comment regarding managing risks associated with third-party relationships.

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, Envestnet Yodlee, Experian, Fiserv, Flinks, Interac, Intuit, Inverite, Kabbage, Mogo, Morningstar, M Science, MX, Petal, Plaid, Questrade, SaltEdge, Trustly, ValidiFi, VoPay, Wealthica, and Xero, among others, as our members.

http://www.fdata.global/north-america

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.

Overview

As the leading trade association advocating for customer-permissioned, third-party access to financial data, FDATA North America's members include firms with a variety of different business models. Collectively, our members enable more than one hundred million consumers and SMB customers to access 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: it depends on the ability of a customer to actively permission access to some component of their own financial data that is held by a financial institution.

We have long advocated for a customer-centric open finance regime in the United States with appropriate regulatory oversight to ensure consumer and SMB protection. Such a framework should, in our view, include supervisory oversight of financial data aggregators by the Consumer Financial Protection Bureau ("CFPB") under its statutory authority granted by Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank"). Our vision of a well-designed open finance system also includes minimum governance requirements for third-party financial technology applications, clear lines of regulatory jurisdiction and supervisory expectations for all industry stakeholders, and a transition away from existing reliance on complex bilateral data access agreements which are both opaque to the end user and collectively result in an unlevel playing field for consumers and SMBs.

FDATA North America welcomed President Biden's issuance in July 2021 of an Executive Order on Promoting Competition in the American Economy, which included a provision directing the CFPB to finalize a rulemaking under its Dodd-Frank Section 1033 authority. This rulemaking, when finalized, will provide a legally binding financial data right for financial institution customers and will create an open finance regime in the United States. We applauded this order as a critical step forward in the development of an open finance system for the United States, and are now respectfully urging the agencies, in this and other future policy reform efforts, to ensure coordination across the federal regulatory system towards the open finance framework that a Section 1033 rulemaking will establish.

Several FDATA North America members are subject to federal supervision as technology service providers to large financial institutions, and all of our members have operational

similarities to insured depository institutions due to their close and long-standing bank relationships. As third-party service providers to large financial institutions, they are subject to vendor due diligence, are required to be compliant with third-party risk management guidelines issued by the prudential regulatory agencies, are audited regularly by their bank partners and are subject to myriad state laws and regulations.

Though the proposed guidance is directed toward insured depository institutions, it directly impacts third-party service providers which we represent and, by extension, their customers. Therefore, we submit to the agencies the following answers to the relevant questions included in the agencies' proposal.

B. SCOPE:

3. In what ways, if any, could the discussion of shared due diligence in the proposed guidance provide better clarity to banking organizations regarding third-party due diligence activities?

Supporting an innovative market for the thousands of smaller financial institutions in the United States is integral to competition, improved consumer and SMB financial outcomes, and a more modern U.S. financial system. We applaud the agencies' interest in fostering development of partnerships between insured depository institutions and third-party service providers and suggest that the primary goal of this effort must be to determine how to best streamline the ability for smaller financial institutions in particular to partner with third parties to offer innovative technology-based products and services while protecting their customers.

The development of bank partnerships with third-party providers now faces two major barriers: fear by an institution that one of its regulators may not approve of the partnership and, particularly for smaller financial institutions, the significant resources required to onboard and maintain a third-party partner in a compliant manner. This is also the case for financial technology providers since their offerings are relatively new and, in some cases, regulatory expectations for the types of services they provide may not yet be formalized or uniformly interpreted.

A cohesive, multiagency Third-Party Risk Management Guidance has significant potential to help streamline this process, but to be successful in promoting competition while ensuring continued customer protection, it must be approached thoughtfully. Properly devised guidance must also guard against the risk of becoming a gate-keeping device that would serve to stifle competition.

This is a concern our members see in the marketplace today. Competition in data-driven financial services can be stifled by financial institutions that override customer direction to share their financial data. These restrictions range from broad attempts to directly limit third parties'

access to data despite customer authorization (outside of individual instances of suspected fraud or unauthorized access); degradation of data sharing that effectively thwarts customer-directed access to financial data; and targeted blocking of sharing specific data fields, in way that effectively renders competing services useless. In each of these cases, as evidence shows, competition in data-driven financial services is being substantially inhibited to the severe detriment of consumers and SMBs.

Due to these market dynamics and to promote continued innovation, it is critically important that the agencies ensure clear, objective standards regarding the risk management requirements associated with financial data sharing are set for regulated financial institutions that enter into partnerships with financial technology companies. The objective should be centered on increasing partnerships between financial technology firms and financial institutions, including clarifying areas where regulatory uncertainty inhibits institutions from engaging in partnerships. Bolstering the ability of financial institutions to confidently partner with third parties will drive healthy competition in the marketplace and help ensure the best possible outcomes for customers in terms of cost, quality, and security.

C. Tailored Approach to Third-Party Risk Management

7. In what ways, if any, could the proposed guidance be revised to better address challenges a banking organization may face in negotiating some third-party contracts?

The current, arduous process for third parties to partner with banks inhibits the onboarding of third-party technology partners. Every bank has its own unique process, created based on a combination of existing internal capabilities, expertise, and technology infrastructure, as well as those of any entities it has acquired, and regulatory requirements under the agencies' third-party partner risk management guidance. The scope and tenor of recurring third-party audits are similarly dictated and vary from institution to institution by these criteria. The best way to ensure all institutions can adequately compete for customer value is to streamline regulatory expectations related to these partnerships. Financial institutions are rightly held to an extremely high standard for protecting customer information by both regulators and their customers, and FDATA North America believes that well-designed open finance frameworks must include similar standards for third-party data aggregation platforms that provide the critical infrastructure powering the financial technology marketplace.

The more insured depository institutions that our members partner with, the more time must be spent individually providing materially similar information to each institution during onboarding, major product updates, or regular audits. This process is time consuming and expensive for both parties, due in large part to the commonality among the various requests for information from each bank with which our members partner, and the marginal benefit to the safety and soundness of the financial system, especially relative to the cost of third-party partner risk management

compliance, is minimal. Moreover, the cost, in terms of both time and resources, of onboarding and maintaining a relationship with a third-party technology provider often stymies the ability of smaller financial institutions and financial technology companies to engage in partnerships, limiting technology adoption for both financial institutions and customers.

Due to lack of clear regulatory guidelines, liability, and responsibility in this marketplace, many larger financial institutions have begun requiring financial data aggregators to execute bilateral data access agreements to continue facilitating the flow of customer-permissioned data that is needed to fuel the technology tools upon which millions of American consumers and SMBs rely to manage and improve their finances. While these bilateral agreements are intended to provide governance in banks' transitions from existing data gathering technologies to the use of application programming interfaces ("APIs") under the agencies existing third-party risk management supervisory expectations, market participants generally recognize that individually negotiated bilateral agreements are an inefficient means of dealing with customer-permissioned data access. Such agreements lack uniformity, transparency, and insight, which can be challenging and expensive for third-party partners. Moreover, an approach that relies on every U.S. financial institution executing a bilateral data access agreement with every data aggregation platform will result – and already is resulting – in an uneven playing field in which some customers have more data rights than others based on the terms and conditions of an agreement their bank executed with a data aggregator, to which they have no visibility.

In the absence of these API agreements, and particularly at smaller financial institutions, many of the aggregators can only access permissioned consumer data on behalf of a fintech through credential-based authentication. As we discuss later in this submission, these arrangements do not absolve the bank of oversight requirements, as they are still expected to protect their consumers and SMBs and to maintain a third-party relationship with the consumer-permissioned access entity.

Several of FDATA North America's member organizations that have executed data access agreements with large financial institutions report that the negotiations can take as long as three years from inception to execution and often require intensive legal and technical costs that smaller financial institutions likely cannot bear, thereby discouraging the adoption of new technology and user services. This presents a significant challenge to smaller financial institutions that will struggle to keep pace with larger banks nationwide.

The substantial expense of building and implementing an API specifically for customer-permissioned data in a manner compliant with existing regulatory expectations imposes an undue burden on smaller institutions. A revised regulatory approach wherein aggregation platforms' connectivity to bank-held data, whether through API or other means, is supervised by the agencies, along with a corresponding simplified set of expectations for the bank itself under such arrangements, has the potential to meaningfully improve adoption of financial technology

partnerships in the marketplace. As noted, these relationships are materially different than other third-party relationships the bank may hold, given that they occur at the request of a joint customer between the bank and financial technology platform, and not in a direct transactional relationship between the institution and the aggregator.

Moreover, the CFPB's forthcoming Section 1033 rulemaking will impose significantly more rigor on the relationships between aggregators and their clients. In tandem, these two regulatory developments – supervision by the agencies of the bank-aggregator relationship and supervision by the CFPB of the aggregator-fintech relationship – would exert enhanced regulatory oversight over the third-party financial technology system while easing the existing gridlock in the marketplace caused in large part by the third-party risk management expectations the agencies project onto financial institutions.

D. Third-Party Relationships

10. What revisions to the proposed guidance, if any, would better assist banking organizations in assessing third-party risk as technologies evolve?

As technology evolves, it is important that any certification process be structured so that its utility lasts over time and that recertification processes are straightforward, streamlined and supported by clear monitoring and reporting requirements. The prudential regulators are all familiar with the challenge of trying to regulate rapidly changing technology without stifling innovation. It is essential that any new standards are not so inflexible as to quickly become outdated, unintentional roadblocks to innovation. The standards should be designed to support interoperable and flexible technology at their core, consciously striving to avoid rigid technology that will require major IT updates to adjust as technology norms change over time. The most important element of any revisions to the proposed guidance for the third-party technology providers that we represent is the notion that any evolution in supervisory expectations must provide clear instructions about exactly what types of documentation can be provided to fully satisfy a bank examiner. Unambiguous, objective requirements that leave little room for interpretation by regulated entities results in a more efficient, uniformly applied onboarding process for third-party technology firms that partner with banks, as well more straightforward regulatory obligations for financial institutions.

The guidance can establish this necessary clarity by publicly and clearly addressing the following: whether a providers' product or service is effective; whether the service provider and its product or service follows the laws, regulations, and best practices for protecting bank customers and maintaining safety and soundness; and whether the third party meets minimum data and cyber security requirements, including through earning other certifications.

11. What additional information, if any, could the proposed guidance provide to banking organizations in managing the risk associated with third-party platforms that directly engage with end customers?

As discussed earlier in this submission, a regulatory regime in which the prudential regulators are responsible for overseeing the relationships between insured depository institutions and third-party data aggregators, and the CFPB is responsible for overseeing the relationships between third-party aggregators and their customers would provide the certainty and uniformity necessary to foster a safe and competitive marketplace. Critically, this coverage would ease the burden on the banks themselves and eliminate the uncertainty that banks often use to block or restrict third-party, permissioned access to customer financial data. The existing regulatory regime lacks this clear delineation of responsibility, providing only vague guidelines that allow for many forms of interpretation, some of which can and are being used to thwart the wider promulgation of innovative technology tools that can meaningfully improve customer financial wellbeing.

To balance the free flow of commerce with the ever-growing need for data security, FDATA North America has consistently advocated for the CFPB to undertake a supervisory role over data aggregations firms. Since the Dodd-Frank Act provides jurisdiction over consumer and SMB data access rights to the CFPB, any successful interagency effort on third-party risk management must include careful consideration of this Section 1033 authority, its jurisdictional impact, and most importantly, a detailed analysis of how it intersects with any guidance issued by the prudential regulators. Once again, the outcome of any such regulatory structure must allow for healthy growth of new market entrants and competition.

The prudential regulators should retain supervisory authority over the relationship between insured depository institutions and data aggregators, while the CFPB, upon finalization of a regulation under Section 1033 of the Dodd-Frank Act, supervises the relationships between aggregators and third-party service providers. This bifurcated approach will best leverage the existing technical expertise of each agency and its staff, align with the spirit of U.S. banking laws, and maintain clear lines of jurisdiction.

G. Information Security

17. What additional information should the proposed guidance provide regarding a banking organization's assessment of a third party's information security and regarding information security risks involved with engaging a third party?

We strongly urge the agencies to build a regulatory regime in which data aggregators are all covered under Federal Financial Institutions Examination Council supervision as Technology Service Providers to large financial institutions. This coverage should establish a baseline for data, cyber, and information security practices as well as risk management and governance for

these firms. Doing so will also provide enhanced regulatory oversight and relieve banks from current regulatory expectations to interpret and apply existing regulatory third-party risk management requirements that do not fit the consumer-permissioned data sharing model. Critically, this approach also will prevent additional justifications for restricting customer-permissioned data access.

Regulated aggregation firms, or application providers relying on financial account data aggregators, would under this construct be responsible for governance over the customers on their platforms in accordance with the supervisory regime established by the CFPB under Section 1033 of the Dodd-Frank Act. In FDATA North America's view, this framework represents a logical construct for implementing Section 1033 of the Dodd-Frank Act under which customers would have full use over the totality of the non-proprietary data their financial institution holds on their behalf, and financial institutions would have the assurance that the aggregators providing data connectivity are supervised and regulated.

FDATA North America also strongly supports the creation of federal data privacy standards by Congress that are consistently applied to all market participants and designed and implemented with the customer's best interests in mind. As increasing numbers of financial services customers interact with their providers on mobile devices, it is unreasonable to expect a customer to have to consider, when they access a financial application, which data privacy or data protection regime applies to that tool. It is important to acknowledge the rapid pace of technological innovation and to ensure that a data privacy regulatory framework does not become an unnecessary hindrance to customers' ability to benefit from new and innovative products and services. Therefore, flexibility must be introduced into any such privacy regime to ensure that consumer protections implemented can evolve and improve over time.

Even a perfectly designed third-party risk management framework will still see the potential for bad actors to access customer data, regardless of security controls. This truth is underscored by the fact that even the largest, most complex, most highly regulated financial institutions in the U.S. have been victims of cybercrime in recent years. A key component of a well-designed open finance system therefore is a requirement for shared responsibility across the system in the event something goes wrong. Thus, assuring the consumer or SMB that, in the event they have sustained harm because of a data breach, the party responsible for the breach will be responsible for making the customer whole should be a foundational component of both the agencies' third-party supervisory expectations and the Bureau's forthcoming rulemaking implementing Section 1033 of the Dodd-Frank Act. While this is a self-evident requirement, accomplishing this outcome will require modernization of existing rules and statutes that currently apportion responsibility for consumer protection in the event of a consumer loss.

Many of those rules and statutes have shared jurisdiction across multiple regulatory agencies, most notably including Regulation E. We respectfully encourage the agencies to modernize

Regulation E to provide for a system under which the impacted holder of a customer's data is ultimately responsible for making them whole in the event of financial loss related to a data breach stemming from fraudulent account access. In tandem with the other recommendations included in this submission, modernization of Regulation E holds the potential to significantly address barriers to customer-permissioned data access in the marketplace today.

H. OCC's 2020 FAQs

18. To what extent should the concepts discussed in the OCC's 2020 FAQs be incorporated into the guidance? What would be the best way to incorporate the concepts?

While we support the joint agency proposal to create uniform guidance on this issue, we are concerned that the OCCs 2020 FAQs have increased the complexity of bilateral data access agreement negotiations.

Our members have often seen banks using their existing supervisory responsibilities to justify ad-hoc restrictions to data access, since the existing supervisory strategy merely provides guidance, while ultimately leaving banks with the responsibility for ensuring third-party compliance. In common scenarios where a bank restricts data access to a third party under the guise of safety and soundness concerns, the third-party provider is entirely beholden to the bank's stated interpretation of regulatory expectations. Unfortunately, the OCC's 2020 FAQs have not remediated this market dynamic and have created an environment in which the largest financial institutions are in a position of increased control over whether and how their customers will have the ability to share access to their financial data.

Regardless of institution size, the current regulatory regime puts the onus on banks to take responsibility for ensuring compliance with regulatory expectations and gives them significant latitude to decide what data elements to allow their customers to share, with which third parties, and how. To be able to compete, all banks must be able to offer these products and services to their customers while ensuring that they are meeting regulatory requirements - particularly keeping sensitive customer information safe and secure. The largest banks are most readily able to meet these demands both by developing products themselves and by driving, through the influence of their market share, how the marketplace engages with third parties.

Therefore, we offer that the simplest solution to this problem would be to remove the interpretive role banks play today in this space through the creation of a regulatory structure in which prudential regulators supervise and retain full responsibility for interactions only between banks and data aggregators, while the CFPB, upon finalization of a rule under Section 1033 of the Dodd-Frank Act, is similarly responsible for supervising the relationship between data aggregators and third-party providers, and by extension, the end users.

http://www.fdata.global/north-america

This end-to-end coverage could effectively eliminate the legal grey area which is currently stifling the growth and innovation of third-party financial tools to the detriment of US consumers. Once again, we urge the agencies to heed the letter and spirit of the recent Executive Order on competition and ensure that any policy changes resulting from the development of this guidance do not interfere with the goals set out in the Order.

Conclusion

The future of third-party financial technology providers is dependent on their ability to work with insured depository institutions to offer innovative digital products to their customers. To facilitate the most market competition and consumer choice, financial institutions should be encouraged to partner with innovative third-party technology providers nnder clear supervisory guidelines. Any presumption by regulators that whatever a financial institution is already using is inherently better or safer than what they could have by partnering with a third-party technology provider stifles innovation and thwarts more fulsome financial access and inclusion.

Millions of Americans are dependent on third-party financial tools today, and a regulatory framework that enables innovation is necessary to the survival of smaller financial institutions and their partners. We are pleased to see the agencies seeking to drive forward innovation and better enable all financial institutions, regardless of size, to partner with third-party service providers to competitively offer innovative products and services to their customers.

FDATA North America appreciates the opportunity to provide the perspective of the aggregation and fintech community to the agencies on their proposed risk management guidance for third-party providers of technology. As the trade association representing firms that currently partner with many banks of all sizes to provide critical financial wellness tools to millions of Americans, we believe that streamlining the ability for banks to partner with third-party providers will be critical to the survival of small and community banks in the United States and to the financial wellness of their customers.

Sincerely,

[redacted]

Steven Boms
Executive Director