Financial Data and
Technology Association

www.fdata.global/north-america

September 21, 2020

SENT VIA ELECTRONIC MAIL TO: Comments@fdic.gov

**Re: Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services (RIN 3064–ZA18)**

The Financial Data and Technology Association of North America ("FDATA North America") appreciates the opportunity to provide comments to the Federal Deposit Insurance Corporation ("FDIC") in response to its request for information on standard-setting and voluntary certification for models and third-party providers of technology and other services. As a trade association that represents dozens of third-party technology providers to U.S. financial institutions, FDATA North America commends the FDIC for its efforts to improve the ability of smaller banks to implement innovative tools, products, and services.

FDATA North America is encouraged by the FDIC's support of innovative technology and efforts to enable FDIC-supervised banks and savings associations to utilize technology that will provide their customers with tools and services that can be transformative to their financial health. As many of our member companies partner with financial institutions to provide these valuable products and services, FDATA North America members have direct experience working under and complying with third-party partner risk management requirements for FDIC-supervised institutions. This process often includes disparate, and oftentimes lengthy, onboarding and approval processes for each bank with which they partner and recurring audits from each of their bank partners, required by third-party partner guidance, that sees our members provide materially similar information to dozens, and sometimes hundreds, of FDIC-supervised banks each year. FDATA North America is delighted to offer its perspective regarding how to create more efficiency in these partnerships to encourage a more innovative and competitive landscape for smaller financial institutions while maintaining safety, soundness, and consumer protection.

**About FDATA North America**

FDATA North America was founded in early 2018 by several firms whose technology-based products and services allow consumers and small businesses to improve their financial wellbeing. We count innovative leaders such as the Alliance for Innovative Regulation, API Metrics, Betterment, Direct ID, EQ Bank, Envestnet Yodlee, Experian, Fintech Growth Syndicate, Fiserv, Flinks, Interac, Intuit, Kabbage, Mogo, Morningstar, M Science, MX, Petal, Plaid, Questrade, Quicken Loans, TransUnion, Trustly, ValidiFI, VoPay, Wealthica, Xero, and others among 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, Australia, South 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.

As the leading trade association advocating for customer-permissioned, third-party access to financial data, FDATA North America's members include firms that provide technology services to financial institutions to enable innovation and expand financial access and inclusion. Collectively, our members enable tens of millions of American consumers and small business customers to access vital financial services and products, including affordable and safe credit, payment solutions, and accounting and financial management solutions, among many other use cases.

Supporting an innovative ecosystem for the thousands of smaller financial institutions in the United States is integral to consumer financial health and a more modern U.S. financial system. We applaud the FDIC's interest in fostering a more efficient process for community and smaller banks to compete with their larger counterparts to provide better products and services to their customers by encouraging safe and sound innovation. The primary goal of this effort must be to determine how to best streamline the ability for smaller financial institutions to partner with third parties to offer innovative solutions while protecting their customers. Moreover, to realize a more innovative, technology-enabled financial ecosystem, it is critically important that the FDIC ensure that any standards or third-party certifications for third-party providers be implemented in a manner that increases the number of technology firms that may partner with smaller financial institutions, enhancing marketplace competition.

We are pleased to have the opportunity to respond to some of the FDIC's questions based on our collective experience:

**Question 1: Are there currently operational, economic, marketplace, technological, regulatory, supervisory, or other factors that inhibit the adoption of technological innovations, or onboarding of third parties that provide technology and other services, by insured depository institutions (IDIs), particularly by community banks?**

The current, arduous process for third parties to partner with banks undoubtedly inhibits the onboarding of third-party technology partners. Every bank has an individual process, created based on a combination of existing internal capabilities and expertise, its existing technology infrastructure as well 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 similarly are dictated by these criteria. As a result, the more banks that our members partner with, the more time must be spent individually providing materially similar information to each bank (and responsible department) during each individual onboarding, major product update, or annual audit. This process is time-consuming and expensive for both the bank and the third-party and ultimately, due in large part to the commonality among the various requests for information from each bank with which our members partner, the marginal benefit to the safety and soundness of the financial system of each audit or onboarding process is relatively low, especially relative to the cost of third-party partner risk management compliance.

Moreover, the cost, in terms of both time and resources, of the process 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, which ultimately results in fewer, more expensive choices for customers. For small and community banks to survive in an increasingly digital world, they must be able to partner with third parties to offer their customers first-class products and services.[1] Additionally, similarly situated third-party data services also serve the regulatory mission, through "RegTech," which despite a clear theoretical compliance advantage to the institution, may suffer from an inability to integrate across the organization's policies and procedures easily. The best way to ensure all institutions can adequately compete for customer value is to streamline the regulatory expectations related to these partnerships.

The ability to handle customer data safely and securely is paramount in an increasingly data-driven financial ecosystem. Financial institutions are rightly held to an extremely high standard for protecting customer information by both regulators and their clients. Unfortunately, the simplest way small financial institutions may choose to protect customer data is to resist the digital transformation and decline to offer, either in-house or through technology partners, more innovative financial tools or products that rely on customer-permissioned data access. This choice results in less flexibility and fewer product, less competitive offerings for customers.

Community banks and smaller financial institutions that would like to utilize third-party vendors as a cost-effective way to provide digital products and services to their customers must adhere strictly to the FDIC's and other prudential regulators' third-party partner risk management rules, which stipulate that these banks maintain responsibility for managing operational risks associated with these partnerships and are responsible for ensuring that they are operating safely and soundly and meet the same regulatory requirements as if the bank itself was performing the third party's services. This has resulted in an arduous, slow, and expensive process that has

[1] https://www.finastra.com/sites/default/files/documents/2018/02/market-insight_small-banks-big-goals-how-community-banks-can-thrive-through-digital-disruption.pdf

thwarted the deployment of innovative technology tools within the smaller financial institution ecosystem.

As FDATA North America has referenced in previous submissions, the average American adult has nearly 16 different financial accounts spread across more than seven different financial institutions or non-bank financial companies. It has never been more difficult for consumers to manage the totality of their financial wellbeing and failure to offer competitive, data-driven products and services will make financial institutions increasingly less competitive over time as the customers' need for products innovative to deliver necessary and empowering tools increases. As millennials surpass baby boomers as the largest generation[2] and have an ever-increasing demand for high-quality digital products and services that, for a highly mobile generation are not geographically specific nor require in-branch visits, smaller financial institutions will struggle to compete and survive without third-party partnerships. In addition, the steady increase in digital consumption has been accelerated by the COVID-19 pandemic, which has pushed consumers who had not yet begun to utilize digital services to do so, simultaneously spiking the need for data holders to adopt robust data security protocols.[3]

Meeting this demand is a challenge for all financial institutions. Large and small banks face different challenges, and so do their prospective partners and vendors, with both sets of issues closely tied to their regulators' third-party-risk requirements. Regardless of institution size, regulators expect banks to take responsibility for ensuring compliance. To be able to compete, banks must be able to offer these products and services to their customers, and to maintain and manage them well, all while ensuring that they are meeting all 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. For example, in recent years, many larger financial institutions have begun to require data aggregators to execute bilateral data access agreements to continue facilitating the flow of required financial data to fuel the technology tools upon which millions of American consumers and small businesses rely to manage and improve their finances. While these bilateral agreements are intended to provide critical governance in banks' transitions from existing data-gathering technologies to use of application programming interfaces ("APIs"), market participants generally recognize that individually negotiated bilateral agreements are an inefficient means of dealing with customer-permissioned data access. Such agreements lack

[2] https://www.pewresearch.org/fact-tank/2020/04/28/millennials-overtake-baby-boomers-as-americas-largest-generation/

[3] https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/a-global-view-of-how-consumer-behavior-is-changing-amid-covid-19

uniformity, transparency, and insight, which can be challenging and expensive for third-party partners.

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 costs that smaller financial institutions will not 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 regarding API integration due to the substantial expense of building and implementing an API specifically for customer-permissioned data. Our members often hear from small institutions concerned that API implementation for customer-permissioned data access is cost-prohibitive. In addition to the deployment of API technology itself, the process of negotiating a bilateral data access agreement is cost and labor-intensive. For the smaller institutions, often the safest and securest way to offer innovative products and services to customers is by engaging with a third-party who is devoted to offering a high-quality product with the most robust security possible. Unfortunately, however, the direction of the marketplace is making this increasingly cost-prohibitive for many small financial institutions to follow suit. Streamlining, through objective certification programs governed by an objective stakeholder, the ability for smaller financial institutions to work with third parties has the potential to address this issue meaningfully. On the other hand, allowing existing market participants the ability to meaningfully control such a certification process presents a very real risk to competitiveness and more efficient pricing.

Finally, helping to ensure the survival of small and community banks by enabling them to better compete in the innovation space is critical for vulnerable and underserved consumers and small businesses. For example, alternative credit models, many of which are provided by third-party technology partners, are crucial for banks serving customers with less access to financial services or who may need innovative, flexible solutions to meet their specific needs. This is especially true for Americans who may be left out of the traditional financial services system. Fintech has emerged readily into this space - filling the gaps where traditional banking could not reach - and banking partnerships have enabled many customers to have the best of both worlds where in the past, they may have had few, if any, options. If, however, the regulatory process for partnerships continues to be overly arduous and expensive, there will inevitably be less competition in the marketplace as newer entrants cannot afford to compete, and potential smaller banks can no longer compete. From 1986 to 2020, the number of FDIC-insured institutions fell from 18,083[4]

[4] https://crsreports.congress.gov/product/pdf/R/R45518

to 5,116[5] while the number of banks with more than $10 billion in assets rose from 38 to 146[6] , and the share of total banking industry assets held by those banks increased from 28 percent to 84 percent.[7] If smaller financial institutions are not able to offer high-quality, affordable, innovative products to compete with their larger counterparts, it is likely this trend will continue.

**Question 2: What are the advantages and disadvantages of establishing standard-setting and voluntary certification processes for either models or third-party providers?**

A clear deterrent for banks in contracting with third-party providers is fear their regulator may not approve of the partnership.[8] This is especially true for 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. We commend the FDIC for identifying and seeking to address this issue, including under this request for information. A standard-setting and voluntary certification process 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. A certification system could generate tremendous advantages over the current approach by reducing the time, complexity and expense it takes for a financial institution to partner with a third-party provider. To the extent the FDIC pursues a certification system, it must guard against the risk of that the certification created under the process becomes a gate-keeping device that would serve to further protect incumbents rather than to facilitate competition. Additionally, the FDIC must ensure that any certification system serves all FDIC member classes through truly optional participation and ultimately serves to build more competitive products, markets, banks and customer outcomes.

To be successful, a standard-setting or voluntary certification process for third-party providers, particularly in the technology space, must: 1) clearly and publicly articulate to the marketplace the requirements for receiving certification; 2) establish a process that ensures that the cost of receiving certification encourages, and not discourages, new entrants into the marketplace; 3) receive express approval from the appropriate regulatory agencies so that certified third parties and their partner banks will have no doubt about their regulators' comfort with third party/bank partnership; 4) ideally, be approved by multiple federal and state regulatory agencies so that third parties may utilize their certification for banks and financial institutions of all sizes; and 5)

[5] https://www.fdic.gov/bank/statistical/stats/2020mar/industry.pdf
[6] https://www.mx.com/moneysummit/biggest-banks-by-asset-size-united-states
[7] https://www.fdic.gov/bank/analytical/qbp/
[8] https://www.fdic.gov/news/financial-institution-letters/2008/fil08044.html

ensure certification requirements are nimble enough to meet the speed of technological advancements.

Clarity and certainty

The standards should publicly and clearly address the following to create a robust, competitive marketplace: whether a vendor's product or service is effective; whether the service provider and its product or service is in compliance with the laws, regulations and best practices for protecting bank customers and maintaining safety and soundness; and whether the vendor meets minimum data and cyber security requirements, including through earning other certifications such as, for example, a SOC 2 certificate.

To be successful, a standard-setting or voluntary certification process must be designed with bank and non-bank financial companies' customers in mind. For third-party providers, the process must be constructed in a manner that to provides financial institutions the confidence to partner with them under a framework that facilitates a streamlined third-party partner risk management program. For financial institutions, a successful certification process must explicitly receive the approval of the appropriate regulatory authorities. Otherwise, no financial institution will be willing to utilize a streamlined voluntary certification for a third-party partner in favor of existing, cumbersome third-party partner risk management. To achieve this desired outcome, it is critical that the FDIC, and ideally other regulators as well, remain highly engaged in the design of any standard setting or certification process and that the regulators' approval of the process be explicit, and transparent to the marketplace. Once the process is established, the FDIC must make it clear to financial institutions what regulatory requirements any third party receiving certification have in so doing adequately met.

Cost

Cost is a critical component – particularly for new market entrants. Receiving a certification can be an expensive process. For many companies, the process and cost are likely to be justified by the savings associated with not working through multiple, multi-year, rigorous onboarding processes and bilateral agreements associated with partnering with different banks. For a standard-setting or certification process to successfully streamline the partnership process between banks and third-party providers, financial institutions must have a clear understanding of what additional third-party partner compliance requirements they will be subjected to under a regime in which a partner has met the criteria for a voluntary certification. Without this clear market understanding, any certification process is meaningless. Ideally, this could result in encouraging banks to consider engaging smaller technology providers that may offer more competitive products and services than their well-established counterparts. 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.

Gate-keeping risk

Another challenge that will be crucial to avoid is any standard-setting or certification process becoming a bottleneck or gatekeeping protocol that evolves into barriers that protect incumbents. We caution the FDIC to closely consider the appropriate scope and composition of any public/private standards setting or certification organization. To be successful, such an entity must be perceived as unbiased and its requirements must be objective and well understood in order to guard against commercial interests influencing decisions made by the entity. While representation from financial institutions and third parties alike will be integral to the success of such an organization, the process of negotiating the standards must also be balanced between competing stakeholder groups to prevent specific interests from becoming dominant. For

example: members of the Financial Data and Technology Association (FDATA) of North America see competition in data-driven financial services 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 direct severe detriment of consumers. Any certification process must guard against such commercially-driven outcomes.

Interagency engagement and consistency

We implore the FDIC to invite the other agencies to take part in this process. Given the decentralized regulatory environment in the United States, it will be important that the FDIC work closely with the other prudential regulators and the states, and, over time, international regulatory bodies, to ensure that a flexible and inclusive regulatory infrastructure is being created that will foster innovation and stand the test of time. While this does not need to happen in tandem, collaboration between the agencies will be critical to the successful fostering of innovation across industry and we encourage you to work with your fellow regulatory agencies to continue to progress.

In addition, most certification programs have voluntary participation, but compliance with the standards should be mandatory to both receive as well as to maintain certification. We commend the FDIC for focusing on creating a public/private partnership. Any certification program that lacks sufficient input from either is unlikely to work. In addition, creating a public/private approach is a way to build interagency participation that will be critical to long-term success.

Adaptability

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 and streamlined, 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 critical that a certification program not be so inflexible that it becomes quickly outdated and results in an unintentional additional roadblock to innovation. The standards should be designed to use interoperable and flexible technology design at their core, consciously striving to avoid rigid technology that will require major IT updates to adjust it as technology norms change over time.

The future of small and community banks is dependent on their ability to embrace technology and offer innovative digital products to their customers. Financial institutions should therefore be encouraged to experiment and test products while limiting risk. 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. Millions of Americans are dependent on third-party financial tools today, and a regulatory framework that enables innovation is necessary to adapt the U.S. financial services system to the reality of how Americans interact with the financial system and necessary to the survival of smaller financial institutions. We are pleased to see the FDIC take a leadership role among the agencies 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.

**Conclusion**

FDATA North America appreciates the opportunity to provide the perspective of the aggregation and fintech community to the FDIC in response to its request for information on standard setting and voluntary certification for models and third-party providers of technology. As the trade association representing firms that currently partner with many small and community banks 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,

Steven Boms
Executive Director
FDATA North America