September 21, 2020

By Email Submission to Comments@FDIC.gov

Robert E. Feldman, Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

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

Dear Mr. Feldman:

The **Wall Street Blockchain Alliance ("WSBA")**, a 501(c)(6) non-profit trade association based in New York City, and the Value Technology Foundation ("VTF"), a 501(c)(3) non-profit think tank based in Washington, DC, appreciate the opportunity to submit our collective thoughts and commentary in response to certain questions raised in the *Federal Deposit Insurance Corporation (FDIC) Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services*, published in the *Federal Register* on July 24, 2020 ("RFI").[1] In particular, members of the **WSBA Legal Working Group ("LWG")**, comprising over 120 attorneys from across the United States, all with deep experience in securities law and the emerging ecosystem of digital assets and blockchain, have been instrumental in the creation of our responses below.[2]

* * * * *

The RFI states that the FDIC would like to achieve certain key objectives and poses a number of questions relating to the achievement of those goals. The goals include:

- Promote the efficient and effective adoption of technology at FDIC-supervised banks and savings associations (financial institutions);

- Facilitate the supervision of technology usage at these institutions without increasing costs or regulatory burden;

- Consider a standard-setting and voluntary-certification program to support financial institutions' efforts to implement models and manage model risk by certifying or assessing certain aspects of the models themselves, and

[1] https://www.fdic.gov/news/press-releases/2020/pr20083a.pdf.

[2] The comments in this letter do not necessarily represent the views of any individual or corporate member of the WSBA Legal Working Group or any individual VTF sponsor.

- Conduct due diligence of third-party providers of technology and other services by certifying or assessing certain aspects of the third-party providers' operations or condition.

Below is a statement of some of the questions the FDIC posed and our responses thereto. We also offer constructive observations at the end of this document for the FDIC and a potential standard-setting organization ("SSO") to consider in deciding what standards are appropriate for recommendation.

* * * * *

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

Response:

Yes, we believe all of these factors collectively inhibit the broad adoption of innovative technologies by IDIs, especially community banks. As the FDIC notes in the RFI, community banks often lack the requisite resources to undertake sufficient and timely due diligence and risk reviews to assess and deploy vendor models and technology solutions offered by financial technology companies ("fintechs") and other third-party service providers. As a result, there are opportunity costs for community banks that may defer their deployment of innovative models and technology services that would enhance the efficiencies and effectiveness of the business of banking.[3] We also note that IDIs face a number of barriers to broad acceptance of cryptocurrencies, crypto-related services, and distributed ledger and blockchain technologies to modernize their own bank offerings and business models, such as:

- Lack of clarity and certainty on the legal and regulatory status of tokens as securities or cryptocurrencies;
- Lack of regulatory clarity on the ability of IDIs to offer cryptocurrency custody services for their customers, which was addressed for national banks and Federal savings associations in recent interpretive guidance issued by the Office of the Comptroller of the Currency ("OCC");[4]
- Lack of broadband internet access in rural and certain urban areas, which inhibits the ability of community banks located in such areas from offering internet banking and payment applications to their customers in affordable, reliable, safe and inclusive ways.
- Lack of specialized tools to handle the complexity of data relating to cryptocurrencies, such as decimal precision (e.g., 20+ digits to the right of the decimal).

[3] RFI at 44891.

[4] See OCC Interpretive Letter No. 1170 (July 2020).

As we noted above, community banks may face disproportionate barriers to adoption of new technologies to upgrade their legacy technology infrastructures. To address such barriers, we see merit in streamlining their onboarding processes, particularly their use of certified Backend as a Service (BaaS) providers. This would enable community banks to outsource the running and maintaining of servers to third parties, which would free up their capacity for frontend or client-side development.

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

Response:

In our view, the main advantages of standard-setting are consistency and efficiency for FDIC-supervised banks and savings associations ("financial institutions"). Financial institutions would be able to rely on a consistent set of standards to facilitate more efficient due diligence assessments and risk reviews of innovative models developed by fintechs and other third-party providers of models without having to "reinvent the wheel" each time they conduct due diligence and risk reviews. We believe the development of clear and voluntary standards through a consensus-driven process among public and private sector stakeholders would yield well-informed standards that financial institutions could integrate into their own due diligence processes. We agree with the FDIC's suggestion for an SSO to manage the process, provided the SSO participants can work efficiently under an agreed schedule for developing standards that would not conflict with existing standards and rules. As technology changes at a rapid pace, the SSO's standards will need sufficient flexibility for technology-neutral applications.

The need for sufficient flexibility highlights an inherent disadvantage of any standard-setting process. Once standards are set, they may not accommodate the assessment of evolving innovations, and thus would have the unintended consequence of inhibiting financial institutions from adopting new and innovative models. We believe that a prospective SSO and the FDIC can overcome this disadvantage by collaborating to formulate standards that reflect regulatory and market needs; update and tailor third-party guidance for partnering with fintechs;[5] and develop principles-based and performance-based requirements that accommodate rapid updates in technology.

Regarding voluntary certifications, we believe their main advantage for financial institutions is enhanced efficiency. Financial institutions would be able to make more targeted assessments of models and third-party technology providers that conform to certification standards, because they would know ahead of time who is "certified" to engage or partner with. Efficiencies would be further enhanced for financial institutions when they can rely on certifications rather than using their own resources to conduct full-scale due diligence and on-boarding assessments.

[5] We agree with Federal Reserve Governor Michelle Bowman on the need for tailored due diligence guidance and standards for banks to assess potential fintech partners. See Remarks by Michelle W. Bowman, Member, Board of Governors of the Federal Reserve System, "Direction of Supervision: Impact of Payment System Innovation on Community Banks," at "Age of Advancement: The Intricacies of a Digital World" 2020 Banking Outlook Conference sponsored by the Federal Reserve Bank of Atlanta, Atlanta, Georgia, on Feb. 27, 2020 ("*I also believe our guidance should explain what due diligence looks like for a potential fintech partner, because the standards applied to other third parties may not be universally applicable*.").

On the other hand, we note the FDIC's concerns in Question 8 about potential disadvantages associated with a voluntary certification process. We believe the main disadvantage of voluntary certifications could be their potential to create concentrations of service providers or disproportionate over-reliance on a few certified vendors and models. This could create inadvertent barriers to entry for certain fintechs and new third-party service providers, resulting in competitive distortions and concentration risks.

Question 3: What are the advantages and disadvantages to providers of models of participating in the standard-setting and voluntary certification process? What are the advantages and disadvantages to providers of technology and other services that support the IDI's financial and banking activities of participating in the standard-setting and voluntary certification process?

Response:

We expect that model providers would benefit from the following advantages by participating in the standard-setting and voluntary certification process:

- *Efficiencies in developing a model that conforms to known standards and qualifies for certification* - Model certification has the potential to facilitate more streamlined due diligence, risk assessments, selection, on-boarding and use of models by IDIs. The resulting savings in time and resources would benefit both the model provider and the IDI.
- *Competitive and comparative advantages* - Providers of certified models would have competitive and comparative advantages over providers of models that lack certification based on the IDI's third-party risk management program. More specifically, certified models would minimize operational risk to the IDI and its customers because minimum standards to address and mitigate risks would be factored into the design of the model, such as compliance risk, transaction risk, risks from cyber-attacks, power outages, and other risks. An IDI may also be able to minimize its legal liability risk by on-boarding certified technology.
- *Selection preferences by IDIs* - To meet its obligations to manage third-party model risks, an IDI may prefer to select and use a certified model. A vendor or provider of an uncertified model may not meet minimum standards of risk mitigation to protect consumer privacy and customer data and records. Uncertified models may not be designed to adequately address other compliance and transaction risks to the IDI and thus would not pass muster under examiner scrutiny.

We note that certification may pose a disadvantage for existing model providers whose current models may not conform to newly developed standards. They may face significant costs to make the necessary adjustments to their models to achieve certification.

For fintechs and other providers of technology, they stand to benefit from similar due diligence and on-boarding efficiencies, as well as competitive advantages and selection preferences that we noted above for model providers. In our view, a distinct advantage of their participation is the opportunity to become stakeholders in the standard-setting process and to help inform the standards by which their technology offerings of products and services will be assessed. As stakeholders in the standard-setting process, fintechs and other technology firms would offer insights on technology solutions to meet emerging market needs for innovations in banking. Their insights would also inform the development of appropriate standards to facilitate evolving technologies. They may also gain

insights from participating in the standard-setting process that inform the design and functionality of their product and service offerings. More specifically, their participation could help them refine or update their technology offerings, such as meeting bank regulatory compliance needs or adapting their offerings to achieve interoperability with existing banking infrastructure and technology systems at financial institutions.

The main disadvantage of standard-setting and voluntary certification for fintechs and other technology firms is the risk that the developed standards do not accommodate their new innovation ideas, both now and in the future. For some fintechs, they may also find that the costs of achieving voluntary certification are prohibitive for their stage of business funding and operations. In such cases, they would face the risks of being uncertified and therefore, less desirable for IDIs to engage and partner with from a resource and risk management perspective.

To address this disadvantage, we suggest that the FDIC could issue a Request for Proposal (RFP) to vendor providers to develop a certification utility in partnership with the FDIC. The Certification Utility could be managed by a representative group of financial institutions, with a pricing model that would benefit both the financial institutions and participating vendors. For example, the International Swaps and Derivatives Association, Inc. (ISDA) set up a utility service for pricing feeds to ensure that all relevant banks and asset managers use the same data. ISDA implemented this utility service in partnership with, and an investment from a third-party provider after a thorough RFP process.

Question 4: What are the advantages and disadvantages to an IDI, particularly a community bank, of participating in the standard-setting and voluntary certification process?

For an IDI, we believe the main advantages of participation include:

- Cost savings from the efficiencies of applying consistent standards in their due diligence and selection of vendors;
- Understanding the latest technology to keep the IDI, whether a community bank or a larger financial institution, at the leading edge of emerging technologies, thus attracting more customers with new and innovative products and services;
- Information sharing from the thought processes and business experiences of others who have identified potential risks from importing and deploying outsourced services into the IDI's business model.

With respect to potential disadvantages, we see none that are material, especially for smaller, less-resourced community banks. Consistent standards and certified technology would only make community banking easier and more competitive.

We note that many IDIs seek to create greater efficiencies for their organizations by finding technological solutions to their back and middle office processes that have been traditionally manual, paper intensive, and/or required human interaction or intervention. One of these areas relates to client onboarding. One article reports that just 8% of a typical IDI's account opening activities can be done remotely, and just 36% of them say they can open a basic checking account remotely without in-

person human interaction.[6] Increasing this figure is especially important in light of the continuing COVID-19 pandemic, decreasing bank margins, and the adverse consequences of lapses in operational controls. In our experience, emerging best practices for client onboarding solutions include those that:

- Automate customer data entry and verification of humans, as well as entities, without the need for in-person interaction;
- Allow for scanning of the full variation of features needed to onboard clients via facial recognition technology;
- Perform automated onboarding and customer verification with commensurate high success rates;
- Conduct automated sanctions screening, watchlist filtering, and online searches of adverse media and other data sources that can support automated or human-assisted customer due diligence and onboarding decisions in an accurate and reliable way;
- Integrate third-party technology for required Anti-Money Laundering (AML) and "Know Your Customer" (KYC) checks as part of customer due diligence.

IDIs are also increasingly considering or engaging in partnerships with smaller fintech companies to gain market share over payment gateway companies and cashback agencies.

Question 5: Are there specific challenges related to an IDI's relationships with third-party providers of models or providers of technology and other services that could be addressed through standard-setting and voluntary certification processes for such third parties?

(1) Are there specific challenges related to due diligence and ongoing monitoring of such third-party providers?
(2) Are there specific challenges related to the review and validation of models provided by such third parties?
(3) Are there specific challenges related to information sharing or data protection?

Response:

Reliance on a single third party for inputs into an IDI's service model presents risk that the IDI may become reliant on that third party for essential functions relating to its business. Contingency planning is necessary to account for such risks, including (a) contractual protections, (b) continued use rights in the event of failure by the third party, and (c) building to open technological standards so that other service providers can fulfill any operational voids.

Updating their infrastructure in sync with the third-party providers could potentially impose significant technological and operational costs on these banks.

Hence, as noted above, the potential creation and implementation of centralized utility services for community banks could help to reduce the cost and risk of such reliance.

[6] https://thefinancialbrand.com/98218/digital-account-opening-bank-credit-union-dao-onboarding-covid-19/

Questions 6: Would a voluntary certification process for certain model technologies or third-party providers of technology and other services meaningfully reduce the cost of due diligence and on-boarding for:

(1) the certified third-party provider?

(2) the certified technology?

(3) potential IDI technology users, particularly community banks?

Response:

Yes, we believe that a standard-setting and voluntary certification process would meaningfully reduce time and costs related to due diligence and preparing responses relating thereto for both the potential IDI technology users, particularly community banks that lack experience or resources, and the third-party provider seeking to respond to the requests. Potential IDI technology users, particularly community banks, would also benefit from third-party technology utilities that are designed to conform to FDIC regulatory requirements to which IDIs are subject. This would also facilitate the FDIC examination process of IDIs with third-party relationships. Thus, we believe standard-setting and a voluntary certification process present a compelling business case for all interested parties. However, the process of obtaining certification for model technologies and other third-party technology services may involve some upfront costs and investment for fintechs and other third-party providers that may be more expensive than uncertified technology.

Question 7: What are the challenges, costs, and benefits of a voluntary certification program or other standardized approach to due diligence for third-party providers of technology and other services? How should the costs of operating the SSO and any associated COs be allocated (e.g., member fees for SSO participation, certification fees)?

Response:

Benefits from a voluntary certification process exist for the service providers, as it sets minimum standards towards which they can build. They can then differentiate with add-ons, such as additional security features, increased accuracy for onboarding, etc., which ultimately lead to a more favorable customer experience.

In addition, a standardized approach to due diligence of third-party providers would offer the benefit of published best practices that financial institutions could use to evaluate and assess risks from onboarding service providers and vendors into their value chains. Examples taken from some vendor questionnaires, sourced from our members and colleagues, include:

- Statement of contingency plans for contractual *forces majeures* (*i.e.*, acts of God), such as weather, electrical power outages, pandemics, and other unforeseen or uncontrollable events;
- Standards for cybersecurity protections;
- Disclosure of past security breaches and remedial protocols;
- Business continuity plans that address events posing a significant risk of disrupting functionality or operations;

- Disaster recovery / planning processes; identifying disaster categories;
- Employee background checks for "Know Your Employee";
- Controls to ensure that data files and libraries are backed up to ensure availability of such files and systems;
- Assessment of intellectual property (IP) rights comprising Software as a Service (SaaS) solutions to be delivered (*i.e.*, the degree to which the vendor owns the IP or bundles the IP from others);
- Patent infringement liabilities;
- Document software development life cycle methodology with traditional Systems Development Life Cycle (SDLC) methodologies and/or Agile methodologies;
- Description of change management process;
- Prioritization of clients using a tiered support model;
- Financial statements - audit process of the vendor;
- Source code escrow management in case of vendor business failures;
- Software upgrades that are in line with the firms' strategic roadmap and contractual obligations;
- Response to patches for software issues and other troubleshooting;
- Quality process for User Acceptance Testing (UAT) and integration testing;
- Support agreement infrastructure;
- Primary and secondary data centers / method of delivery;
- Management of operational risk with redundancy for all critical processes and system components;
- Establishment of automatic fail-over (back-up process) mechanism for all critical processes;
- Demonstration of minimal (no) diminution in service in disaster recovery mode;
- Description of critical controls, including system access, network security, data protection and more.

Question 8: Would a voluntary certification process undermine innovation by effectively limiting an IDI's discretion regarding models or third-party providers of technology and other services, even if the use of certified third parties or models was not required? Would IDIs feel constrained to enter into relationships for the provision of models or services with only those third parties that are certified, even if the IDIs retained the flexibility to use third parties or models that were not certified?

Response:

IDIs would likely choose those that are "certified" for risk management purposes and the expectation that examiners may view certified third parties or models more favorably than uncertified third parties or models. This may effectively constrain IDIs in their selection process. However, we believe there are potential benefits of an incentive-based model for voluntary certification. For example, third parties could seek certification of their software processes by different standards, such as Capability Maturity Model (CMM)[7], SDLC, or other existing software industry standards, to build credibility in the marketplace. If financial institutions give technology vendors an incentive in the form

[7] https://en.wikipedia.org/wiki/Capability_Maturity_Model

of a return on investment (ROI) to obtain voluntary certification, we anticipate that vendors would offer better quality of service and products for use in the banking technology ecosystem.

Question 21: What benefits and risks would COs provide to IDIs, third parties, and consumers?

Response:

COs function as an independent vetting process which indicates that a service provider has satisfied the minimum standards to offer inputs into the IDI's process. For example, the American Institute of Certified Public Accountants (AICPA) has published standards for audits relating to Service Organizational Controls ("SOC"). These controls are a set of technical standards defined and maintained by the AICPA.

AICPA SOC reports are reports of reputable accounting firms and relate to the internal controls of providers of outsourced services. The reports assess the risks for purchasers of outsourced services. SOC 1 audits evaluate those risks from the perspective of the internal controls and financial reporting of the service provider. AICPA SOC 1, Type 2 attestation evaluates the service provider's design and testing of controls, and reports on their operational effectiveness over a period of time (typically six months). SOC 2 controls relate to information and IT security measured by reference to five Trust Services Categories, *i*.e., security, confidentiality, information privacy, processing integrity and availability.[8]

Such SOC audits are essential for institutions that purchase outsourced services where they have to rely on the output for purposes that have great significance, such as financial reporting or court proceedings. The rigors of the SOC attestation process help protect users from defects in data and the gathering thereof. As a best practice, some purchasers of outsourced technology services will not entertain quotations from service providers that do not have current AICPA SOC type 2 reports.

Using the above as an example, CO's provide several benefits to IDIs, third parties, and consumers, including but not limited to reporting on the reputation and reliability of vendors, adherence by vendors to possible standards for date and client confidentiality, security, privacy, process integrity and more.

Conversely, a CO is only as beneficial as the members of the organization and its ongoing support of certification criteria work to be. Hence, there is a potential risk of loss of relevance as regards to emerging technologies, a falloff in market reputation and credibility due to stagnate relevance, inability to service the growing certification needs of those seeking such certification and more. As with all certification organizations, critical mass of market acceptance and usage is important to minimize such risks.

[8] For additional information on SOC certifications, see: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html

Question 25: Are there legal impediments, including issues related to liability or indemnification, to the implementation of a voluntary certification program that the FDIC, other Federal/state regulators, third-party providers, and IDIs should consider?

Response:

Broadly speaking, we collectively do not believe that there are direct legal impediments related to the implementation of a voluntary certification program that the FDIC, other Federal/state regulators, third-party providers, and IDIs should consider. Indeed, in many instances at both the operational and technological levels, properly implemented voluntary certification programs could offer the opportunity for firms to strengthen, in practical terms, the quality of their compliance. In turn, this could offer the possibility of more efficient and effective compliance due to such voluntary certification programs.

That said, it bears emphasizing that the proposed use of standards for banking industry models and a voluntary certification program would not eliminate or reduce the ultimate legal liability and responsibilities of a financial institution's board of directors and management for ensuring that the use of third-party models and technology services in the provision of bank products and services complies with applicable laws, regulations, and internal policies.[9]

Concluding Thoughts

We applaud the FDIC's issuance of the Notice and Request for Information as part of the FDiTech initiative to promote the efficient and effective adoption of technology at FDIC-supervised banks and savings associations. Blockchain and cryptoassets continue to drive change, innovation, disruption, and the development of new products and services in the banking and financial services industries, as well as in many other segments of the economy. We look forward to discussing our thoughts and comments with the FDIC and welcome the opportunity to assist the FDIC in any way to address the issues raised in the aforementioned Request for Information.

Respectfully Submitted,

[redacted]

Ron Quaranta
Chairman and Chief Executive Officer
Wall Street Blockchain Alliance
New York, New York 10036

[9] See FDIC's FDiTech publication, "Conducting Business with Banks: A Guide for Fintechs and Third Parties", February 2020, at p. 2 ("Bank management remains ultimately responsible for identifying and controlling risks and activities conducted by or through their bank, whether these risks and activities arise directly or through an outside party."). Available at: https://www.fdic.gov/fditech/guide.pdf.

[redacted]

Jason Brett
Chief Executive Officer
Value Technology Foundation
Washington, DC 20005

Contributors

Mr. Roger M. Brown - Head of Tax and Regulatory Affairs, *Lukka*

Ms. Sonia Goklani - Chair *WSBA Tech & Product Working Group*
CEO, ClearTrack - Derivatives Clearing, Blockchain Fintech

Ms. Whitney Kalmbach - Chief Operations Officer, *Value Technology Foundation*

Ms. Joshua Ashley Klayman, Esq. – Member of the WSBA Board, Chair - *WSBA Legal Working Group*

Ms. Laura Harper Powell, Esq. – Former Senior Legal Fellow, *Value Technology Foundation*

Disclaimer – The views, thoughts and opinions expressed in this Request for Information response are those of the Wall Street Blockchain Alliance and the Value Technology Foundation. Numerous Contributors (including the Contributors listed above) who provided their expertise in their fields of work as it relates to these comments offered invaluable contributions; however, these comments do not necessarily represent the views, thoughts, or opinions of their employers, organizations, working groups, or any other groups or individuals.