veriff

September 22, 2020

VIA EMAIL to comments@fdic.gov

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

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

Dear Mr. Feldman:

Veriff appreciates this opportunity to respond to the Federal Deposit Insurance Corporation's ("FDIC") request for comments in response to its Request for Information ("RFI")[1] on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services. As technology performs an ever-increasing role in the delivery of financial services provided by financial institutions, it is important that financial institutions, especially smaller institutions that lack highly developed internal technology capabilities, have confidence in technology providers both for satisfying operational requirements and regulatory expectations.

Since it was founded in 2015, Veriff, headquartered in Tallinn, Estonia, has become a leading global provider of identity verification services. Our verification process supports over 8,000 government issued identification documents from over 190 countries in 35 languages. We have an established presence in the EU and a growing presence in the Americas, including the United States. Veriff clients include leading digital companies in finance, payment systems, e-commerce, the "sharing economy", government agencies, and social media. Identities of customers, employees, and other users are verified for our clients. We believe that our global presence and exposure across multiple sectors offers a unique perspective that helps United States financial institutions and regulators understand and apply emerging technologies.

---

[1] 85 Fed. Reg. 44890 (available at: https://www.govinfo.gov/content/pkg/FR-2020-07-24/pdf/2020-16058.pdf).

Technology and IDIs

There are many types of firms that offer technology beneficial to the financial services industry. At Veriff, we believe that some of the best technology solutions may be offered by emerging companies that have developed innovative methods to address long-standing issues.

Adoption of technological innovations can pose many challenges for an IDI, particularly at community banks. Technology can be costly. IDI management may face many issues that preclude proper consideration of technological innovation. IDIs, particularly community banks, may not have an effective process for evaluating technology-based solutions. These challenges often delay the adoption of technology by IDIs.

Further challenges face smaller, emerging providers of technology. The largest IDIs with the greatest financial resources are pre-disposed to select only those technologies offered by large, established vendors. This corporate culture minimizes or eliminates the contribution from emerging companies to technological innovation at IDIs.

The FDiTech initiative has the potential to address some of these barriers and challenges. As a result, a broader array of providers will be able to serve a broad range of the IDI spectrum.

Standards and Certifications - Advantages and Disadvantages

A set of standards and certification framework can play a role in advancing the adoption of technology by IDIs - if executed properly. A common set of standards can offer a useful guide to technology providers who develop technology services and a reference point for IDIs seeking to adopt technology. Consumers and regulators will have confidence that IDIs adopting technology consistent with these standards are adhering to safety and soundness expectations. These standards can also help emerging providers gain credibility when seeking to provide services to all IDIs from the largest to the community banks.

As the request recognizes, standard setting and certification frameworks could limit innovation, restrict participation in this market, and possibly increase costs associated with adopting technology. To prevent or at least mitigate these undesirable consequences, standards should be appropriate for the technology and have the ability to accommodate innovation offered by emerging companies. Certification frameworks should be accessible to all market participants. Guidance allowing self- certification where appropriate can also mitigate these undesirable consequences.

Standard Setting Organizations (SSOs) and Certification Organizations (COs) have some particular advantages that should be encouraged and disadvantages that should be addressed. IDIs are not technology companies, and technology companies are not IDIs, so these organizations can offer a forum where stakeholders can collectively identify issues and develop guidance for solutions. This activity can encourage development and adoption of technology by a broad number of IDIs from a wide choice of vendors. The FDIC initiative and resulting guidance should encourage this outcome. But regulatory and supervisory initiatives should not result in exclusionary actions that limit choices, increase costs, and stifle innovation. Again, flexible standards and certifications appropriate to the technology and its intended use can mitigate this adverse outcome.

Due diligence and on-going monitoring processes could see positive impacts from standards and certification frameworks, benefitting IDIs, particularly community banks, and technology providers, particularly emerging companies. Standards provide IDIs with a measurement tool to determine if a technology will meet relevant requirements. Without standards, IDIs do not necessarily know how to evaluate the technology offered or whether it will address the operational or regulatory objective. Time and money consumed by IDI management and outside consultants will be greatly reduced allowing more rapid adoption of the solution. As new regulations continue to be announced, this is an important consideration.[2] Standards and certifications can also address Third Party Risk Management (TPRM) expectations established by supervisory regulators.[3] Due-diligence and on-going audit and monitoring burdens required by TPRM frameworks may be lessened by the implementation of standards and certifications principally as a result of lower costs and reduced time requirements.

With technology, there are data privacy and data protection issues. All stakeholders in the financial system have an interest in maintaining the privacy of and protecting personal data. Where appropriate, standards requiring adherence to privacy and protection legal frameworks and certifications that attest to this adherence will benefit these stakeholders by assuring that data is protected to the greatest extent possible.

Considerations For Establishing Standard Setting Organizations and Certification Organizations

The universe of third-party providers of technology and other services for IDIs is vast and diverse, ranging from firms that provide specialized solutions to very specific requirements to firms that offer services to support virtually all of an IDI's operational and compliance needs. Some firms may focus on the financial services sector while other firms serve multiple sectors. Different types of SSOs with different levels of cooperation with the FDIC and other Federal and state regulators should be considered. And since IT providers have different business models, and in many cases provide services for multiple business sectors, SSOs and their organization should reflect these differences in a way that balances objectives of this initiative with the business environment that creates and provides these services. Often, the cost structure of such organizations could be a barrier to the adoption of technology whether by imposing high costs that (1) limit accessibility to smaller IDIs or (2) discourage emerging companies from developing products for IDIs. These concerns should be considered when evaluating the structure of an SSO.

Different forms that an SSO could take include a new independent organization created to set standards for a service, a standard setting framework created within an existing organization, and private initiatives promoted by existing organizations and businesses. Instead of promoting a single SSO solution for standard

---

[2] *See, e.g.*, Anti-Money Laundering Program Effectiveness, 85 Fed. Reg. 58,023 (Sept. 17, 2020) (seeking public comment on potential regulatory enhancements to the Bank Secrecy Act and other anti-money laundering regulations). As new regulations are issued in response to these initiatives, technology can have an important in meeting their mandates.

[3] *See* Third-Party Relationships: Risk Management Guidance (OCC Bulletin, OCC 2013-29, Oct. 30, 2013) and Third-Party Risk: Guidance for Managing Third-Party Risk, FDIC, Financial Institution Letter No. FIL 44-2008.

setting and certification, different types of organizations reflecting the diversity of the technology sector should be considered.

There is a long history of privately organized SSOs in many sectors including technology and finance. For firms that provide a comprehensive suite of IT services, a new SSO may be appropriate, but an SSO serving large scale firms will very likely be inappropriate for providers of specialized or unique services. A large scale SSO may be more likely to focus on the needs of larger IDIs and less on the challenges faced by community banks. Alternatively, existing organizations may consider forming sections or task forces to set standards and certify providers. For example, the American Bankers Association or the Independent Community Bankers of America could take this initiative. Remembering that the goal of this initiative is to encourage adoption of technology in order to mitigate risks and reduce costs, standard setting initiatives by new or existing organizations should not burden IDIs or providers with excessive costs or burdens that discourage IDIs from adopting or providers from developing new technologies.

Other than new SSOs and standard setting functions within existing organizations, private firms may also provide standard setting services. Consulting firms, for example, may be engaged by a provider to design a system of standards to measure the performance of the provider's service.

Scope of Regulatory Participation

Input on the role of the FDIC, other Federal regulatory authorities, and state regulatory authorities was also requested. Any role for regulators must be within the scope of their regulatory authority, which may limit the degree of approval a regulator may confer on standards or upon an SSO. The request recognizes that adherence to the guidelines is voluntary. But guidance within the scope of their authority will be helpful in attaining the goals of this initiative. While this guidance may not be able to describe specific parameters or standards that the technology provider must meet, this guidance can describe considerations to guide the design of the service and the IDI's evaluation of the provider. For example, statutes require financial institutions to maintain Know Your Customer policies and procedures that are consistent with the size of the institution and the scope and nature of its business. Any regulatory guidance to SSOs should be consistent with this flexibility. Since there is a diverse array of stakeholders that would be impacted from this initiative, guidance recognizing this flexibility would benefit all of these stakeholders. Regulatory guidance to SSOs should recognize that different IDIs have different needs and capacities to implement technology. Guidance recognizing that community banks have different needs and resources than systemically important financial institutions will encourage adoption of the technology and help provide a level playing field for all IDIs. Similarly, the guidance should recognize that there is not a direct correlation between the level of resources to stay abreast of regulatory demands and the capacity to develop technologies that further this initiative. The regulatory cooperation with SSOs should not have the effect of preventing smaller technology providers from developing solutions for IDIs and discouraging IDIs from adopting technology from smaller providers.

Defining the scope of a voluntary certification program depends heavily on the type of technology or service that is being certified. Existing Third Party Risk Management expectations which require IDIs to take into consideration the financial condition and operational resilience of a third-party provider already apply to any third party technology provider of technology. But a certification framework should take into consideration that leading technology service providers are often new firms whose financial conditions do not resemble those of established firms. Many smaller firms have been able to demonstrate operational resilience through participation in independent auditing and testing such as the System and Organization Control ("SOC") framework set forth by the American Institute of Certified Public Accountants and executed by independent, third-party auditors. Recognition, even in examination handbooks, that SOC audits support an IDI's due diligence would be one method to encourage adoption of new technologies offered by new technology providers. This or other rigorous auditing could in many instances meet the objectives of a voluntary certification program.

Conclusion

It is encouraging to see the FDIC's interest in promoting IDIs' adoption of technology. Successful adoption of technology can help IDIs improve operational soundness and improve financial strength through cost reductions. A proper balance of reasonable guidance and flexibility will greatly contribute to the success of this effort. With world-class identity verification capabilities, Veriff looks forward to becoming part of the financial services IT landscape.

Sincerely,

Gregory Vint

Legal Counsel, Veriff OÜ