American Bankers Association
Building Success. Together.

Krista Shonk
Vice President & Sr. Counsel
Regulatory Compliance and Policy
Phone: 202-663-5014
E-mail: kshonk@aba.com

September 22, 2020

Robert E. Feldman
Executive Secretary
550 17th Street, NW
Washington, D.C. 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

Dear Mr. Feldman,

The American Bankers Association[1] is pleased to comment on the FDIC's Request for Information (RFI)[2] seeking feedback regarding the potential creation of a public/private standard-setting partnership and corresponding certification program to help reduce the cost, inefficiencies, and uncertainty related to bank onboarding of third-party service providers. Specifically, the RFI requests input on whether a public/private partnership could support banks' third-party risk management efforts by certifying or assessing certain aspects of a third-party's products or models or by evaluating a third-party provider's operations or condition.

ABA appreciates the FDIC's willingness to address some of the hurdles, duplication, and costs associated with managing third-party risk. Increasingly, a bank's ability to compete in the marketplace will depend on its ability to leverage the expertise of third-party service providers. Banks that are unable to adopt new technologies or partner with new third parties will not be able to provide the products and services that customers expect. Unfortunately, the due diligence necessary to onboard a prospective vendor is costly, inefficient, and time consuming for both banks and service providers. These burdens exist for all institutions, but are particularly acute for community banks.

We are encouraged that the FDIC recognizes the strategic importance of third-party relationships and that Chairman McWilliams has made fostering innovation a top priority for the agency.[3] In particular, we appreciate the FDIC's willingness to explore strategies for reducing the friction and duplication associated with third-party onboarding and oversight.

---

[1] The American Bankers Association is the voice of the nation's $21.1 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $17 trillion in deposits and extend nearly $11 trillion in loans.
[2] 85 Fed. Reg. 44890 (July 24, 2020).
[3] As Chairman McWilliams said in the FDIC's July 20, 2020 press release, "we have to remove unnecessary regulatory impediments that banks must overcome when developing and deploying new technologies." https://www.fdic.gov/news/press-releases/2020/pr20083.html

Summary of Comments
We discussed the RFI with CEOs, senior executives, model risk professionals, and third-party risk management practitioners from banks with a wide range of asset sizes and business strategies. Our members believe there are efficiencies to be gained from standardizing certain aspects of the due diligence process and that certification may help to highlight those vendors who take seriously issues such as cybersecurity, disaster recovery, and consumer protection obligations.

However, our members questioned whether a standard setting and certification mechanism would be compatible with products or firms that are truly innovative. In particular, they were skeptical about whether it is feasible to articulate a standard that would result in certification of a vendor product that is truly pioneering and unproven. For this reason, we encourage the FDIC to refine the potential objectives of a public/private partnership to distinguish between technology in the general sense and technologies that are cutting-edge.

With this important distinction in mind, our comments identify multiple features of a public/private partnership that would be worthy of additional exploration and discussion, including:

- Establishing multiple tiers of review ranging from a baseline of due diligence information to standardization and certification of specific components or elements of a vendor's product or processes.

- Identifying and standardizing the foundational due diligence that banks should collect and review for specific types of providers and services. Once vetted through the certifying organization, this information would provide a ready resource on which banks could rely and build without beginning a vendor or product review from scratch.

- Concentrating on existing service providers, rather than emerging firms and technologies. A public/private partnership could use regulator data to identify vendors and products with significant market share and develop standards and certifications for those entities and services.

In addition, a public/private partnership must provide value to banks, service providers, and regulators that is distinguished from and exceeds existing standard-setting mechanisms. Our members recommend the following to encourage bank participation in a public/private partnership:

- All federal banking agencies would participate in the public/private partnership.

- Regulators would be active standard-setting contributors, not just passive observers.

- Regulators would provide clear, written, and unambiguous assurances that banks may rely on information and findings provided by a certifying organization.
- Banks of all sizes would be able to participate in the public/private partnership and avail themselves of the benefits of certification.
- If an unanticipated event (such as a cyber or compliance breach) were to occur, continued certification would be conditioned on the third party meeting a specified timeline for appropriate mitigation response.
- Certification would be voluntary; it would not be perceived as a prerequisite to doing business with a third party.
- The certification process would be completed within a defined time period; policymakers would not attempt to hold up a certification for a particular public policy purpose.
- The public/private partnership would focus on areas of greatest need, recognize where the market is already meeting needs, and strive not to duplicate or displace existing standards-setting organizations.

The creation of a public/private partnership would be a complex undertaking requiring significant expertise and commitment. Additional study and analysis is warranted prior to moving forward, including an evaluation of sensitive governance issues and the exploration of potential funding streams. We appreciate that the FDIC issued this RFI, which offers stakeholders the opportunity to offer early feedback on these important issues.

I. Refine the Objectives of a Potential Public/Private Partnership

When evaluating the concept of a public/private partnership, a key question is: what problem(s) might a standard-setting organization (SSO) and corresponding certification be able to solve? While standard-setting and certification will not address all of the industry's third-party risk management challenges, we believe that a public private partnership has the potential to reduce some of the inefficiency, duplication, and regulatory uncertainty associated with onboarding and overseeing third parties.

However, as a practical matter, the standard setting and certification process may not be compatible with products or firms that are truly cutting-edge and innovative. For example, a public/private partnership would have to be sufficiently nimble and able to stay ahead of technological change, which frequently outpaces bank regulation. Yet, regulators participating in an SSO might be hesitant to articulate a standard that would lead to a certification of a vendor product or practice that is pioneering and unproven. Similarly, regulators participating in the SSO might deem newer financial technology firms as insufficiently mature for certification.

We also believe there is a risk that certification of new technologies could have the unintended consequence of deterring innovation. For example, it is possible that banks looking to deploy a particular technology or product may choose to partner only with firms that have been certified. Likewise, examiners could take a similar view and discourage banks from entering into relationships with uncertified firms.

While standardization and certification may not improve adoption rates and speed to market for technologies that are new and unique, we *can* envision multiple ways that a public/private partnership might decrease costs and inefficiencies while enhancing banks' management and oversight of their third parties. Possibilities include the following:

A. Create Tiers of Review

Banks might benefit from a public/private partnership that provides multiple tiers of certification (e.g., Level 1, 2, 3, etc). For example, and as described in more detail below, a Level 1 review might set a standard for the types of due diligence information required for certain categories of providers or services and then collect and validate the information provided by a third party.

A Level 2 review might assess, test, and certify that specific components of a product or technology adhere to prescribed standards established by the SSO. This type of review would focus on narrow elements or pieces of a vendor's solution, such as model validation.

Banks from a wide range of asset sizes report challenges in being able to look into the "black box" of a vendor model and perform the same level of validation that the bank would conduct on the models that it develops internally. In many cases, vendors have been unwilling to share detailed model information because they deem it to be proprietary. While we do not know whether vendors be willing to share this information with an independent certifying organization, model validation would be a particularly useful feature of a public/private partnership that could improve a bank's understanding of third-party models while increasing speed to market. Our members are also intrigued by the potential for a public/private partnership to develop standards for qualitative models that include a judgment component on which banks rely when making underwriting or other business decisions.

A Level 3 certification could go beyond specific elements or components of a vendor's product and evaluate a service provider's overall processes for model development, risk management, underwriting, fraud detection, etc.

By addressing multiple pain points associated with third-party risk management, this differentiation between levels of review and certification could provide value to banks. In addition, it would facilitate an incremental approach to standing up an SSO and certifying organization.

B. Build a Foundation of Due Diligence Information

As mentioned above, banks would benefit from a Level 1 review that would provide a foundation of due diligence information pertaining to a particular vendor or product upon which a bank could build.

Under this approach, the SSO could identify a baseline of information that banks should collect and review for defined categories of providers and services.[4] Once collected and vetted, this information would provide a ready resource on which banks could rely without beginning a vendor or product review from scratch. This approach should reduce the time and effort that banks devote to the "paper chase," thereby allowing bank staff to focus on unique aspects of the relationship or product as well as the third party's actual performance.

Standardization and certification of standard due diligence information would have several benefits, including:

- Creating a set of vetted due diligence documents that give banks confidence that the information provided is accurate and correct;
- Decreasing bank and vendor cost and resource demand;
- Providing certainty regarding the depth and sufficiency of due diligence collection and analysis;
- Providing an accessible and affordable due diligence option for community banks;
- Helping banks to more quickly onboard new third parties and assisting with ongoing due diligence of existing third parties;
- Freeing resources to allow bank staff to focus on innovation and risk analysis; and
- Enhancing vendor understanding of bank regulation and regulatory expectations pertaining to vendor oversight.

In addition, we believe that a Level 1 certification would provide a much needed roadmap to help start up firms understand and navigate due diligence expectations. To date, the banking agencies have not issued joint, interagency guidance on third-party risk management. The level of detail in existing guidance varies from agency to agency, particularly as it relates to due diligence expectations for these firms. We urge

[4] For example, due diligence standards could include but would not be limited to: information security, privacy, data validation, data purchasing and handling, data retention and destruction, business continuity planning/disaster recovery, financial health, fraud and AML controls, marketing, hiring, scalability of the vendor/whether the vendor has adequate infrastructure to support the load, interoperability and ability to speak a common language.

the agencies to issue third-party management guidance on an interagency basis, including a discussion of relationships with young, financial technology companies (fintechs).

Often, fintechs are less mature and do not have robust internal controls or audited financial statements—all of which seem to be incompatible with a formalized certification process. However, a public/private partnership could smooth the path for banks to do business with such companies by providing a due diligence standard that these firms can follow and use in preparation for conducting business with a bank. As the firm matures, it could apply for different levels of certification for specific pieces or components of its product or processes.

Finally, we note that developing consensus on the due diligence standards will be *critical*. While this approach would help banks vet third parties more quickly by eliminating much of the duplicative document collection and review that exists today, banks may want (and in some cases may need) to conduct due diligence and analysis that exceeds the baseline information, depending on their specific use of a product or technology and on an institution's individual risk management practices. Striking a balance will be critical. Otherwise, service providers will be in the position of responding to both banks and the SSO. There is also a risk that certified providers will view themselves as "bulletproof" and will decline to provide additional information to individual banks.

C. Review Existing Service Providers/Products

Another approach might be for a public/private partnership to focus on existing service providers, rather than emerging firms and technologies. A public/private partnership could use regulator data to identify vendors and products with significant market share and develop standards and certifications for those entities and services.

For example, a small number of mobile app developers provide services to the banking industry. However, in 2020, mobile apps are not considered pioneering technology. Establishing standards and certifications for mobile app technologies and/or providers could alleviate much of the duplicative effort associated with conducting ongoing due diligence and oversight associated with these firms, thereby freeing up resources for banks to focus on innovative third-party relationships.

Another example involves core processors. While it may be difficult to certify the broad suite of a core processor's products, our members strongly support continued conversations to explore the development of standards and certifications for targeted elements of a core's product offerings. Core processors are major bank vendors. Standardizing targeted aspects of initial due diligence and ongoing oversight of these firms would provide a significant relief for our member banks. And, considering that the regulatory agencies already examine core providers, we anticipate that the development of such standards would be highly achievable.

II. Provide Adequate Incentives

Establishing and maintaining an effective framework will require the dedication of substantial time and financial resources. Therefore, it is critical that the certification be a friction-reducing step that provides meaningful value; creating a standard that adds another level of third-party oversight or increases the complexity of third-party management will not achieve the goals of this initiative.

A. Regulators Must Be Active Standard Setting Contributors

For a standard-setting and certification mechanism to be successful, regulators will need to be full contributors to the standard setting process, not just observers. Their involvement would distinguish the public/private partnership from other standard setting organizations that exist today and would incentivize banks and service providers to participate in the public/private partnership and certification process.

Finally, we note that standing up and maintaining a standard-setting and certification mechanism would be a large and complex undertaking that would benefit from being conducted on an interagency basis. Buy-in from all of the agencies would enhance the credibility and reliability of the standard and corresponding certification.

B. Clarify the Meaning of Certification

For a certification to provide maximum value, regulators should give clear and unequivocal assurances in amended third-party guidance statements and exam procedures that banks may rely on information and findings provided by a certifying organization. Regulators should expressly state that banks may rely on such certification in lieu of collecting and analyzing due diligence information independently. Failure to provide (and reinforce with examiners) these unambiguous assurances would miss an opportunity to leverage collective industry expertise in order to improve the quality of third-party risk management and meaningfully reduce cost and duplication of effort.

We acknowledge, however, that there are circumstances in which banks may need to conduct additional due diligence and analysis of a firm or technology, for example, if the bank's use of that product exceeds the scope or tier of a particular certification. Additionally, we recognize that any certification or due diligence information would represent a third-party's condition, features, internal controls, and compliance status as of a specific point in time. As a result, we understand that banks have an obligation to monitor the product, technology, and performance of the service provider. However, banks should be able to rely on updated information gathered via certification updates in order to help perform this task.

C. Provide Visibility Into Issue Management

One way to incentivize banks to participate in a public/private partnership would be to provide transparency into findings uncovered during the certification process. Presumably, if a firm or a technology does not "pass," any issues would need to be remediated before the firm can earn the certification. Knowing what the gaps were and when and how they were addressed would enhance banks' overall understanding of the service provider by providing important visibility into the provider's issue management practices. One way to provide such transparency might be to describe how the technology/technology provider compares to a baseline (i.e., does the provider or technology meet or exceed minimum baseline standards?)

D. Improve Incident Response

Another way a certifying organization could provide value is to encourage service providers to provide more timely incident response and appropriate mitigation. We are living in an age of rapidly evolving threats and vulnerabilities, and, compliance with applicable laws and regulations is as complex as it has ever been. Rather than automatically withdrawing a certification if a compliance or security breach occurs, continued certification could be conditioned upon the third party meeting a specified timeline for providing an appropriate mitigation response. Such an approach might incentivize certification holders to remediate issues in a timely manner, particularly for small and midsize banks.

E. Certification Must Be Truly Voluntary

According to the RFI, banks could choose to conduct business with entities that are not certified. This is an important feature that must be preserved. We are concerned that certification could be perceived as a pre-requisite to doing business with a third party. Regulators must specify that is not the case.

There may be a number of reasons that a service provider may elect not to go through the certification process or may choose to not renew its certification. The certification process may be too slow, too expensive, or insufficiently agile to keep up with a vendor's changing offerings. It is also possible that product demand may be insufficient for a service provider to justify going through the certification process. Banks, not regulators, should determine whether to limit their partnerships to certified third parties. Institutions exploring doing business with an uncertified provider would simply conduct their own due diligence in full, just as banks do today.

F. The Certification Process Must Be Timely

Finally, for the certification process to be useful, there must be assurances that it will be completed within a defined period of time, absent unusual circumstances. Regulators should not be permitted to hold up a certification for a particular policy purpose.

III. SSO and the Certifying Organization

A. Obtain Adequate Expertise

Both the SSO and the certifying organization must be staffed with highly qualified individuals with the requisite technical skills. For example, staff must have the skills to develop standards and test model accuracy, fairness, use, and conceptual soundness. They must also have the expertise to conduct data testing and test model implementation. These skills are highly specialized and are in high demand in the marketplace.

B. Acknowledge Existing Standards

The financial services sector and trade associations (including ABA) have a distinguished history of providing leadership in the development of standards. Through participation in organizations such as ISO and X9, banks play a key role in anticipating and supporting standards needed by the marketplace. In the electronic payment space in particular, the industry has been forward-leaning in creating roadmaps, specifications, and other key information that promotes innovation across the ecosystem. Among those organizations that have successfully iterated for decades on collaborative standards-setting are EMVCo (managed by the leading payment brands) and the Payment Card Industry Security Standards Council LLC (PCI).

The specialized expertise of EMVCo and PCI in their respective domains of competence has resulted in a proliferation of compatible products available to banks and end-users. These organizations must ensure that crucial interests such as data security and reliability are carefully tended to, and their actions reflect these imperatives. It is important that any new standards organization focus on areas of greatest need, recognizing areas where the market is already meeting needs, and strive to not duplicate or displace existing standards-setting organizations.

C. Address Governance, Participation, and Control

The creation of a public/private partnership would be a complex undertaking requiring significant expertise and commitment. Prior to moving forward, additional study and analysis of various governance issues is warranted, including an evaluation of the potential for certain groups to wield outsize influence and the need for a dedicated funding stream. After the goals and objectives of the contemplated third-party public/private partnership are refined, we would welcome the opportunity to provide perspective regarding potential governance matters.

IV. Conclusion

We reiterate our appreciation for the FDIC's willingness to devote time and resources to exploring ways to improve the efficiency and quality of third-party management. There is still much conversation to be had on this subject, and we look forward to continuing the dialogue with our member banks and the bank regulatory agencies.

Should you have any questions regarding ABA's views, please contact the undersigned at kshonk@aba.com.

Sincerely,

Krista Shonk
Vice President & Sr. Counsel
Fair & Responsible Banking
Regulatory Compliance and Policy