Via Electronic Submission

September 22, 2020

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

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

Dear Secretary Feldman:

The Independent Community Bankers of America ("ICBA")[1] welcomes the opportunity to respond to the Federal Deposit Insurance Corporation's ("FDIC") request for information ("RFI") that seeks input on whether a standard-setting and voluntary-certification program could support community banks' efforts in partnering with third parties or implementing new models. While there is enormous benefit for community banks to partner with third parties or to leverage new models, there is also tremendous burden associated with these endeavors. ICBA believes that the program contemplated in the RFI could greatly enhance community banks' ability to seek these benefits while mitigating the associated burden.

Many community banks develop partnerships with innovative third parties, such as fintechs, to seek new opportunities, such as the ability to quickly leverage new technologies, forge deeper relationships with their customers and communities, target new markets, and dramatically increase efficiency. However, community banks also face many challenges as a result of these

[1] The Independent Community Bankers of America® creates and promotes an environment where community banks flourish. With more than 50,000 locations nationwide, community banks constitute 99 percent of all banks, employ nearly 750,000 Americans and are the only physical banking presence in one in three U.S. counties. Holding more than $5 trillion in assets, more than $4 trillion in deposits, and more than $3.4 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation and fueling their customers' dreams in communities throughout America. For more information, visit ICBA's website at www.icba.org.

partnerships. Because many of the challenges in partnering with fintechs are seemingly so large and vast, it is easy to understand why some community banks opt to not enter into these partnerships. While not insurmountable, these added burdens can dissuade some community banks from exploring relationships with new third-parties, despite the fact that the benefit might outweigh the burden. By not adopting these new technologies, these community banks may limit opportunities to serve their customers.

The RFI explores potential ideas in response to this dilemma. ICBA applauds the FDIC for approaching the issue in a thoughtful manner that not only solicits and catalogues challenges associated with bank-fintech partnerships, but also contemplates potential solutions to these common challenges.

Overall Discussion and Response to Questions

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? (Question 1)

Before exploring the hurdles and challenges of community bank partnerships with fintechs, it is important to first reiterate why partnering with fintechs is so advantageous for community banks. In a 2017 ICBA Fintech Survey,[2] community banker respondents noted the following benefits that fintech companies offer to community banks:

- **Increased Operational Efficiency and Scale**: Given their nimble nature, community banks are well-positioned to take advantage of the opportunities in the fintech landscape—opportunities that present potential gains in fee income, reductions in risk and fraud, increased efficiency, and improvements to the customer experience.
- **Increased Access to Customers with a Younger Age Demographic**: The baby boomer generation is winding down their earning and spending activity. Over the next 25 years, nearly 81 million U.S. millennials (all of whom came of age after the digital revolution) will dominate the economy. Millennials demand financial services that focus on origination and sales, which are personalized and emphasize seamless/on-demand access to the service from the underlying product. Fintech companies are eager to meet millennials' preferences.
- **Increased Access to Loan Customers in New Markets**: Community banks can work with fintech lenders to provide critical banking services to underwrite consumer, mortgage and commercial loans. This can expand bank access into new markets where

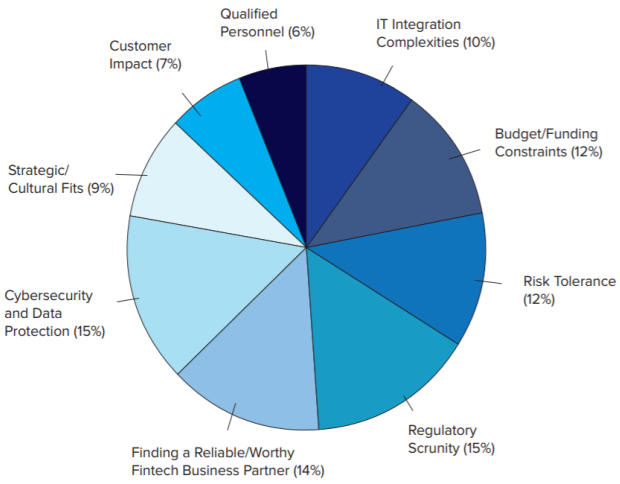
[2] "Fintech Strategy Roadmap for Community Banks," Mar. 2018, ("ICBA Fintech Whitepaper") *available at* https://www.icba.org/docs/default-source/icba/icba-fintech-strategy-roadmap-(03-12-16).pdf?sfvrsn=6a0e7117_4

fintech companies have greater penetration. For example, marketplace lenders or "MPLs," leverage data collection and technology to provide access to credit with little to no physical overhead or distribution network. Small and medium-size banks often partner with MPLs when they do not have the internal expertise or resources to execute an online lending business model.

- **Enhanced Brand Reputation**: Community banks partner with fintech companies to offer new, innovative services. To be successful, banks will need to work with fintech partners to develop marketing and financial branding strategies that carry forward the bank's brand. Customers may demand more universal banking automation and transformed branch experiences, all of which will need to be communicated through a community bank's brand messaging.
- **Enhanced Customer Experience**: Nearly 50 percent of responding community bankers noted the opportunity for enhanced customer experience as the greatest benefit to capitalizing on new and emerging technologies. Community banks are looking to fintech advancement as an opportunity to strengthen customer and community relationships. Technology can act as the great equalizer for community banks successfully traversing the fintech scene given their ability to be nimbler in implementing change.

Yet despite these clear advantages and enormous potential, significant challenges currently inhibit many community banks from engaging in partnerships with fintechs. ICBA has studied these inhibitors to community bank partnerships with fintechs for a significant period of time. The 2017 whitepaper[3] identified some of the most pressing perceived hurdles.

Top Challenges Fintech Partnerships Present for Community Banks



[3] *Id.*

Limited staffing
Some community banks seek partnerships with third parties to gain efficiencies, due to limited staffing or expertise. However, it is the very fact that these banks have limited staff that leads to the difficulty of properly overseeing the third-party relationships that were meant to help alleviate limited staffs in the first place.

Limited experience
Other than limited staff bandwidth, some community banks might not have staff with the requisite skill or knowledge to implement new technologies or to oversee the third parties that implement and adopt these new technologies. There is a lack of knowledge and internal manpower needed to conduct a complete and thorough internal review.

High costs
Costs present another challenge in partnering with a third party, especially if the product or service is particularly unique or novel, or the bank has come to critically rely upon the provider such as a core processor. Compounding these problems, banks might have diminished bargaining power when negotiating with these service providers. Not only can this lead to a bank that is captive to the service provider, but it can also drain monetary resources that could be better allocated to other technology providers that might better serve the community bank. Though service providers will often tailor their pricing based on the bank's asset size or volume of transactions, it is still a major expense.

Integration challenges
Even in circumstances where a bank might be able to search for technology beyond that provided by their core service provider, few third-party products or services are able to integrate flawlessly with the core service provider. While the product or service might work in concept, the difficulties only present themselves when attempting to integrate the fintech software with the core service provider.

Limited information
If a fintech is a new company or early in its life cycle, community banks will struggle to find information on the company that is sufficient to meet regulator and due diligence demands. Trying to assess their financial resilience, experience, referenceable clients, and verify other information referenced in agency third-party guidance is difficult unless they are larger and more established.

Verification of information
Verifying the information that is provided in response to due diligence inquiries is also a challenge, as is on-going monitoring for certain critical third parties that have gotten so large that they can decline to demonstrate compliance or respond to information requests. Some banks have relayed to ICBA that there is a 'take it or leave it' approach, knowing that the community bank will be forced to 'take it.'

Regulatory hurdles

Finally, while initially designed to be an opportunity for banks to demonstrate their due diligence and on-going monitoring of third parties, compliance with third-party guidance and responses to examiner scrutiny have themselves become burdens to partnering with fintechs. To head-off any examiner criticism, community banks will sometimes subject fintechs to a full and thorough dose of due diligence, without regard to criticality, interconnectivity, or other factors that might dictate a less encompassing vetting. Though not directly the fault of examiners, the wariness of examiner scrutiny and the practice in response has become a significant hinderance to the adoption of bank-fintech partnerships. Aside from the actual management of the risk that these partnerships present, simply responding to examiner scrutiny and showing compliance with third-party risk management guidance can be prohibitive. Simply said, it is costly for community banks ensure and demonstrate compliance with relevant regulatory requirements when selecting and monitoring significant service providers.[4]

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

A standard-setting organization ("SSO") and certification could help solve for many, if not all, of the challenges discussed above. Looking to other areas at banks that have utilized standards and certifications can provide insight into their advantages and disadvantages.

For example, the Federal Accounting Standards Board ("FASB") is a well-known SSO that created and maintains the Generally Accepted Accounting Principles ("GAAP") standards. Established in 1973, the Financial Accounting Standards Board ("FASB") is the independent, private-sector, not-for-profit organization that establishes financial accounting and reporting standards for public and private companies and not-for-profit organizations that adhere to GAAP.[5] FASB standards are recognized as authoritative by many other organizations, including state Boards of Accountancy and the American Institute of CPAs ("AICPA").[6]

Recognizing the value of standards and SSOs, the federal banking agencies adopted GAAP as the reporting basis for the Call Report in March 1997. Additionally, the Securities and Exchange Commission has designated GAAP as the designated accounting standard for public companies.[7] As the agencies explained at the time, "the adoption of GAAP for Call Report purposes eliminated the differences in accounting standards among the agencies."[8]

---

[4] Congressional Research Service, "Fintech: Overview of Innovative Financial Technology and Selected Policy Issues," (Apr. 28, 2020), *available at* https://crsreports.congress.gov/product/pdf/R/R46332.

[5] About the FASB, *available at* https://www.fasb.org/jsp/FASB/Page/SectionPage&cid=1176154526495#:~:text=Established%20in%201973%2C%20the%20Financial,profit%20organizations%20that%20follow%20Generally

[6] *Id.*

[7] *Id.*

[8] "Differences in Capital and Accounting Standards among the Federal Banking and Thrift Agencies," Jan. 20, 1999, *available at* https://www.federalreserve.gov/boarddocs/rptcongress/differences/default.htm.

Just as the creation of FASB and the adoption of GAAP standards helped achieve uniformity and a common set of expectations between regulators and the regulated entities, the creation of a fintech SSO that establishes standards for certification could greatly enhance and address the common inhibitors to bank-fintech partnerships.

In contrast to the advantages discussed above, challenges that might not be solved by an SSO or certification include analysis of the documentation in support of certification. Certification that attests to the completion of various audits, questions, or other standards is not sufficient to assess risk. Therefore, it seems unlikely that an SSO would completely alleviate banks' obligations to thoroughly vet third parties. That creates the potential for an additional layer of certification without the benefit of reliance.

Additionally, though third-party services or products can be certified, the ability for those products or services to integrate into the existing banks' platforms might not lend itself to standards or assessment by certification organizations ("COs"). While the systems can be standardized, the systems' configurations are not. Identical systems and who/what the systems talk to can be, and many times are, different, therefore, a canned certification may not be adequate. These determinations would likely need to be made on a case-by-case basis.

> *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? (Question 3)*

Through much anecdotal evidence, ICBA has come to believe that most, if not all, banks have their own version and requirements when assessing third parties. Even if a community bank uses a standard questionnaire, such as the standardized information gathering ("SIG") questionnaire, the bank likely adds unique questions to the questionnaire. While this is arguably a practical response to the uniqueness among community banks, the reality creates a difficult situation for fintechs to manage these very similar, yet different, questionnaires and third-party compliance frameworks.

In response, fintechs pull together documentation resources to comply with similar but different third-party due diligence requirements, resulting in immense redundancies and waste, for both the bank and fintech. Due to the increasing complexity of responding to initial bank questionnaires and managing on-going inquiries of existing bank clients, many fintech have outsourced the responsibility to other parties.

Given that these fintechs are already engaging and utilizing third parties to manage these requirements, the creation of an SSO and CO may integrate well within current practices. In fact, these third parties help the fintechs seek, obtain, and manage reporting requirements associated

with audits and/or certifications, such as a System and Organization Control ("SOC") type 1 and type 2 audits.

The clear benefit of this model would be a shorter 'time-to-market' for fintechs. For example, a fintech that recently participated in ICBA's ThinkTECH Accelerator has explained that undergoing due diligence and initial vetting by potential bank partners is taking 10 months (and counting), whereas finalizing partnerships with non-banks has taken as little as 10 days. Once the initial due diligence requirements are met, though, fintechs have reported that the process is much easier to manage as an on-going process. In an ideal world, certification of compliance with SSO standards would reduce the on-boarding by several months.

So long as regulatory agencies uphold the validity of certificates and put weight in their assessments, SSOs and certifications would make it easier to get new technologies through a bank's internal approval process.

The obvious trade-off, discussed further below, is that fintechs that do not participate in the certification program will be at a competitive disadvantage. Rather than reducing barriers to entry and accelerating the on-boarding process for new stage companies, the certification program could perversely protect incumbent third parties from competition by new entrants if the program is too costly or otherwise burdensome for new entrants, which adversely affects banks looking for diverse products or less costly services.

Additionally, depending on the depth of the analysis, is it possible that earning the certificate would be more stringent than what a community bank would typically require of a fintech. That possibility could serve as a disincentive against a fintech participating in the program, which would undermine the adoption rate of the program. Similarly, if certification is a months-long process, then the fintech might not see the benefit in seeking the certification – it could be quicker and/or easier to simply be vetted by the bank directly.

As the FDIC considers the SSO and certification process, it should address the following questions: What would be the specific process of earning the certification? What is the cost and number of hours required to complete the certification? And how long will it take to receive a response to the application?

Finally, by design, standards homogenize the market. While this certainly has advantages to auditing and reviewing third parties, a homogenized market diminishes the likelihood of diverse products or services. That lack of a diverse marketplace may place bank-fintech partnerships at a disadvantage when compared to other industries or service providers where diversity flourishes.

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

Community bank participation in the standard-setting and certification process would alleviate many of the challenges discussed in response to Question 1, above. In particular, limited staffing, limited experience, and limited information can be ameliorated through the adoption and use of standard-setting and certification. Perhaps most directly, the use of standard-setting and certification could also address regulatory challenges, described below.

Certifications that verify which standards are met can save tremendous amount of time for community banks that have limited staff or resources to dedicate toward due diligence and monitoring. While not a replacement for appropriate oversight, such a solution would allow banks to reallocate staff toward customer-centric operations or obviate the need to hire additional compliance staff. In addition to saving staff time, certifications can provide knowledge and expertise to community banks that might not have the requisite expertise for specific technology. Some community banks may feel more confident with a review conducted by an expert with the knowledge and skill set to complete the review.

There are already multiple versions of vendor management questionnaires for each vertical relationship, many overlapping and proving redundant.[9] The number of questionnaires available for use is continually increasing.[10] If some of these questionnaires or requirements are not eliminated in the face of the SSO or certification, then the process has merely added to the burdens and redundancies.

Aside from staffing challenges, SSOs and certification could recalibrate the asymmetries between community banks and certain fintech providers. As mentioned above, some community banks have claimed that certain third-party service providers are so large that community banks do not have sufficient bargaining power to receive answers or documents in response to basic due diligence questions and requests. If enough smaller community banks collaborate and utilize the services of an SSO, there likely would be enough bargaining power in the aggregate to access that information.

On the opposite end of the spectrum, SSOs can alleviate problems typically present with small or early stage fintechs. In contrast to large fintechs that have the requested information but simply will not share it, these early-stage fintechs *would* share the requested information, but for the fact that they do not have it prepared. The SSO could solve for this by acting as a shared platform on behalf of multiple banks, working with the early-stage fintech to develop the information

[9] *See* UpGuard, "11 of the Top Questionnaires for IT Vendor Assessment," *available at* https://www.upguard.com/blog/top-vendor-assessment-questionnaires; highlighting the 11 top questionnaires for IT Vendor Assessments (California Consumer Privacy Act Questionnaire, Center for Internet Security — CIS Critical Security Controls (CIS First 5 / CIS Top 20); Cloud Security Alliance — Consensus Assessments Initiative Questionnaire (CAIQ); General Data Protection Regulation (GDPR); Higher Education Community Vendor Assessment Tool — (HECVAT / HECVAT Lite); ISO 27001 Questionnaire; Modern Slavery Questionnaire; National Institute of Standards and Technology — NIST SP 800–171; Shared Assessments Group — Standardized Information Gathering Questionnaire (SIG / SIG-Lite); Vendor Security Alliance — VSA Questionnaire (VSA) Payment Card Industry Data Security Standards (PCI DSS) Questionnaire). This is limited to IT Vendors, yet evidence of arguably non-IT related matters are included, such as 'modern slavery.'

[10] *Id.*

sufficient for the SSO's certification. The banks benefit from the efficiencies of shared services, and the early-stage fintechs benefit from having SSO's expert assistance in compiling the information.

While certification and SSO will be advantageous, they will not be a panacea. In addition to requiring on-site and on-staff knowledge and oversight, banks would still need to address integration challenges that are unique to each bank's technology stack.

Of all the potential advantages that SSO and certification hold, its use to ameliorate regulatory burden and examiner scrutiny are perhaps the most promising. While ICBA appreciates that banking agencies are working together to establish consistent expectations for third-party relationships, a community bank's real-world experience in fintech relationships is dictated by an examiner's interpretation of guidance on the matter. A fintech's adherence to standard-setting and receipt of certification could provide the community bank with a safe harbor and enough confidence that the examiner will not pose undue scrutiny toward the bank's partnership with the fintech.

> *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? (Question 5)*

It is inefficient to subject each third-party to the same or similar due diligence and monitoring requirements from thousands of banks.[11] Banks are asking third parties a fairly common set of questions that have been asked and answered numerous times by third parties in response to multiple requests for proposals. It is frustrating for the fintechs, and certainly wasteful for the banks. SSOs and certification could address those inefficiencies.

By demonstrating compliance with SSOs and certifications, banks will be able to evaluate fintechs according to one standard, creating more equitable 'apples-to-apples' comparisons, and fintechs will only have to adhere to one standard, eliminating the bespoke and 'similar but different' scrutiny to which banks currently subject them. In essence, participation in standard-setting would create shared due diligence of potential partners, allowing community banks to gain economies of scale as they pool resources.

> *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?*

[11] See Governor Michelle W. Bowman, "Direction of Supervision: Impact of Payment System Innovation on Community Banks," (Feb. 27, 2020), remarks made at, "Age of Advancement: The Intricacies of a Digital World" 2020 Banking Outlook Conference sponsored by the Federal Reserve Bank of Atlanta, Atlanta, Georgia, *available at* https://www.federalreserve.gov/newsevents/speech/bowman20200227a.htm.

(2) The certified technology?
(3) Potential IDI technology users, particularly community banks? (Question 6)

The current costs for fintechs to receive certifications and audits can be cost-prohibitive, especially for early-stage fintechs that might not yet have a bank partner. For example, the SOC 1 & 2 audit and readiness reports cost approximately $40,000 to $60,000. If the certification or audit to demonstrate compliance with standards is an additional cost, then the contemplated audit and certification will likely become too prohibitive and the adoption rate might be lower than otherwise anticipated. The adoption of SSO and certification will be a cost-*saving* endeavor, and thus, a much more viable option, only if it replaces existing certification and audit mandates.

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)? (Question 7)

As discussed above, the cost associated with this program would be a significant determinant of its success. The current model of many certification programs and audits typically place the cost on the certified entity, whereas banks that rely on those certifications might engage the services of a vendor management firm to assist in the ongoing oversight, with those costs borne by the bank.

The approach to allocating costs in the operation of the SSO could be a similar hybrid approach, where both the fintechs and the banks contribute to the funding. This seems prudent considering both parties will be benefiting from participation in the SSO - fintechs would benefit from the efficiency of adhering to a uniform standard while banks would benefit from time-saved in conducting full-scope due diligence.

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? (Question 8)

A voluntary certification process certainly could undermine innovation by effectively limiting an IDI's discretions regarding models or third-party providers, especially if the community bank wants to work with a third party to build a unique product. Even if it is clear that the certification is voluntary, some community banks might still be uncomfortable in partnering with a fintech that is not certified in order to avoid scrutiny.

Fewer third parties are likely to seek certification if the process is costly, burdensome, or duplicative. This would further limit the pool of third parties that have their certification, and thus, further limit the pool of third parties from which community banks would feel comfortable partnering.

> *What supervisory changes in the process of examining IDIs for safety and soundness or consumer protection would be necessary to encourage or facilitate the development of a certification program for models or third-party providers and an IDI's use of such a program? Are there alternative approaches that would encourage or facilitate IDIs to use such programs? (Question 9)*

Examiners and the supervision process can contribute to an environment where banks are empowered to achieve supervisory goals by simplifying and clarifying the process of third-party service provider selection, due diligence, and monitoring.[12] When examining banks, examiners could spend their time identifying and discussing potential trouble spots rather than conducting rote reviews of third-party relationships that have met agreed-upon standards. This would be beneficial to all parties involved and create a more purposeful examination process.

A critical factor with the certification would be the acceptance of the certification as a form of approval by regulators. If regulators do not accept the certificate, or if examiners add additional due diligence measures because the third party is not certified, the creation of the SSO and certification program would be a step backward and increase burden without providing any benefit.

For this program to work effectively, examiners must rely on the certification as evidence of compliance with agreed-upon standards. Examiners can continue to ensure that the community bank is monitoring the third-party interactions with the bank on a case-by-case basis, but the documentation and other standardized metrics should be beyond reproach.

> *What other supervisory, regulatory, or outreach efforts could the FDIC undertake to support the financial services industry's development and usage of a standardized approach to the assessment of models or the due diligence of third-party providers of technology and other services? (Question 10)*

While federal regulations essentially must be promulgated upon reflection and in response to past activities or events, such as the response to the financial crisis, SSOs may have the opportunity to more nimbly read trends and proactively develop standards *before* they are widely adopted. In fact, setting standards and expectations before wide-spread adoption may prove to be pro-cyclical and trigger wide-spread adoption since many banks rely on guidance or standards before adopting novel technologies.

---

[12] See Governor Michelle W. Bowman, "Direction of Supervision: Impact of Payment System Innovation on Community Banks," (Feb. 27, 2020), remarks made at, "Age of Advancement: The Intricacies of a Digital World" 2020 Banking Outlook Conference sponsored by the Federal Reserve Bank of Atlanta, Atlanta, Georgia, available at https://www.federalreserve.gov/newsevents/speech/bowman20200227a.htm.

Further supporting the development and use of a standardized approach to the assessment or due diligence of third parties, the FDIC could reference and cite the agreed-upon standards when developing guidance and regulations. This would dramatically reduce the compliance time needed to comply to a new rulemaking.

Finally, the FDIC or inaugural SSO might explore whether there are third-party insurance policies that cover community bank damages in the case of certain predetermined events. These insurance policies likely have developed standards that the SSO can leverage and build upon when developing its own standards. The SSO could even cite to the insurance standards or vice versa, resulting in a closed loop system that increases adoption rates.

> *What are the potential challenges or benefits to a voluntary certification program with respect to models that rely on artificial intelligence, machine learning, or big data processing? (Question 13)*

Artificial intelligence and machine learning ("AI/ML") technology is designed to be dynamic with minimal human intervention. Examples include rapid changes in the inclusion or exclusion of variables and data points that might not be adequately projected in advance of the technology's usage of the data. However, rather than focus on the inputs of the models that use AI/ML, SSOs and voluntary certificates could focus on the outputs of those models and standardize the tests that are used to periodically back-test the findings. For example, existing models not relying on AI/ML technology are currently required to undergo periodic back-testing and review. There are certain statistical models that allow for this. Though models using AI/ML technology may require more frequent back-testing, statistical modeling can still be employed to back-test model outputs. The statistical model and the process for overseeing the use of those back-tests could lend themselves well to SSO and voluntary certificates.

> *To what extent would a standards-based approach for models or third-party providers of technology and other services be effective in an environment with rapidly developing technology systems, products, and platforms, especially given the potential need to reassess and reevaluate such systems, products, and platforms as technologies or circumstances change? (Question 16)*

The standards-based approach could be very effective even in rapidly developing areas. If the SSO places responsibility upon the vendor to provide client banks with updates if material changes occur, then the community banks and regulators would be more informed and in better positions to develop responses to those changes. The SSO or CO could serve as a central clearinghouse that receives timely information from certified third parties and transmits that information to all interested parties, including the client banks and regulators.

For example, rather than passively waiting for an annual review or periodic assessment of a third-party's credit modeling, the third-party could actively update the SSO every time it changes

its underwriting model or adopts new information upon which it makes decisions. The SSO would keep a log of these changes and notify the client bank or regulators based on the desired preference. Some banks might want to be notified every time a change to the model is made, whereas other banks might merely want to review the change log on a quarterly basis or only when a material change occurs.

> *What current or draft industry standards or frameworks could serve as a basis for a standard-setting and voluntary certification program? What are the advantages and disadvantages of such standards or frameworks? Do standards and voluntary certifications already exist for use as described herein? (Question 17)*

There is no shortage of standards and frameworks used to vet and monitor third-party partnerships, and ICBA strongly urges the FDIC to assess the existing landscape of existing tools. The success of the contemplated program hinges on replacing or integrating existing standards and frameworks. As noted above, if a certification is a new standard in addition to existing standards and frameworks, then the benefit will be outweighed by the redundancies and costs of an additional standard.

In reviewing the landscape of existing tools, assessments, standards and frameworks, FDIC should at a minimum assess and determine how the following tools and questionnaires could or will be adopted into the SSO: National Institute of Standards and Technology third-party risk management framework; Payments Card Industry standards; SOC 1 & 2; SIG; Cyber Assessment Tool; California Consumer Protection Act questionnaire; General Data Protection Regulation questionnaire; Center for Internet Security; Vendor Security Alliance; and Federal Financial Institutions Examination Council questionnaire.

> *Given that adherence to SSO standards would be voluntary for third parties and for IDIs, what is the likelihood that third-party providers of models or services would acknowledge, support, and cooperate with an SSO in developing the standards necessary for the program? What challenges would hinder participation in that process? What method or approaches could be used to address those challenges? (Question 18)*

Third-party providers would likely support and cooperate with an SSO if the program reduced the redundancies of several banks requesting the same information. Additionally, third parties are likely to be drawn to the program if banks tend to favor partnering with third parties that have been certified by the SSO.

Specifically, third-party providers would be more likely to participate in the program if the potential advantages noted above are available and delivered. Specifically, the program must:

- Decrease costs of partnering with banks
- Increase speed to market
- Eliminate redundancies
- Provide FDIC support of the certification

- Assist in the management of bank inquiries on monitoring activity

What is the best way to structure an SSO (e.g., board, management, membership)? Alternatively, are there currently established SSOs with the expertise to set standards for models and third parties as described herein? (Question 19)

In developing standards and creating an SSO, ICBA believes that the structure should utilize a board structure that serves as the final arbiter of standards and other relevant matters. The board would ideally be a public-private composition with a diversity of experiences. Specifically, ICBA recommends that the contemplated SSO board have representation from each stakeholder community that would benefit or be affected by the SSO, including representation by community bankers, third-party fintechs, and federal and state agencies, such as a representative of the Federal Financial Institutions Examination Council.

In order to create standards that are considered and contemplative, ICBA recommends that the SSO board issue proposed standards with opportunities for the public to weigh-in, regardless of whether those commenters are associated or benefit from the standard-setting and certifications. Finally, the board could utilize a small staff and a body of volunteers that can generate and craft guidance in response to market needs, lending their expertise and perspective to the process.

A model that could be followed is:

1. Identify issues based on requests/recommendations from stakeholders.
2. Determine whether to add a project to the technical agenda based on a staff-prepared analysis.
3. Hold public meetings to discuss the various issues..
4. Draft a proposal to solicit broad stakeholder input.
5. Hold a public roundtable meeting on the draft.
6. Analyze comment letters, public roundtable discussion, and all other information obtained through due process activities.
7. Issues a standards update, describing amendments.

While other SSOs are required to sever connections with firms or the intuitions they serve as a way to foster independence,[13] ICBA does not believe that such a requirement is necessary for the contemplated SSO.

To what extent should the FDIC and other Federal/state regulators play a role, if any, in an SSO? Should the FDIC and other Federal/state regulators provide recommendations to an SSO? Should the FDIC and other Federal/state regulators provide oversight of an SSO, or should another entity provide such oversight? (Question 20)

[13] *Supra*, note 5.

ICBA strongly recommends that the FDIC collaborate with other federal and state regulators in evaluating and, if pursued, creating the SSO. Creating standards is important, but their use and adoption depends on the reliance and faith that other regulatory bodies place on them. In order to gain wide-spread acceptance, representatives from these various agencies will need to provide input on the standard-setting and hold seats on the governing board that serves as the final arbiter.

> *What benefits and risks would COs provide to IDIs, third parties, and consumers? (Question 21)*

As discussed at various points throughout this response, COs can provide numerous benefits for community banks, third parties and consumers. In summary, COs can decrease the costs of partnering with banks, increase speed to market, eliminate redundancies, provide FDIC support of the certification, and assist in the management of bank inquiries on monitoring activity.

Consumers would benefit by the faster introduction of novel technology used by the consumer. If banks do not find more effective and speedier ways to partner with fintechs, then consumers will not have access to technology that could improve their financial lives. By facilitating more bank-fintech partnerships, COs would facilitate broader consumer access to technology.

> *To what extent would COs be effective in assessing compliance with applicable standards in an environment with rapidly developing technology systems, products, and platforms, especially given the potential need to reassess and reevaluate such systems, products, and platforms as technologies or circumstances change? (Question 22)*

Since a certificate would be an analysis of the fintech at a point in time, routine reviews should be conducted on an annual basis, and perhaps more frequently depending on the criticality of the third party. To keep certificates current, third parties could be required to notify COs of significant changes to their operations or models. However, regardless of changes, the certification should be renewed with current information on an annual basis.

> *If COs receive derogatory information indicating that a certified third party or certified model or technology no longer meets applicable standards, should the COs develop a process for withdrawing a certification or reassessing the certification?*
>
> > *(1) If so, what appeal rights should be available to the affected third party?*
> > *(2) What notification requirements should COs have for financial institutions that have relied on a certification that was subsequently withdrawn?*
> > *(3) Should the FDIC or Federal/state regulators enter information sharing agreements with COs to ensure that any derogatory information related to a certified third party or certified model or technology is appropriately shared with the COs? (Question 24)*

COs should have a responsibility to monitor certified third parties for compliance with the agreed-upon standards. If deficiencies or issues of non-compliance are discovered, the SSO should use the clearinghouse mechanism discussed in Question 16 to actively transmit the relevant information to the banks, regulators, and any other interested parties.

If the deficiency or non-compliance is material, COs should have a process for withdrawing certification, but only after an investigation and an opportunity for the third party to respond. The right to appeal can vary with the severity of the action taken by the CO and the potential for harm caused or avoided. Since the validity of the certification will only be as good as the reliability and diligence of the CO, it is imperative that bad actors or deficient providers be removed from the program.

Conclusion

ICBA supports the FDIC's efforts to explore options and solutions to commonly experienced problems facing community banks when partnering with third parties such as fintechs. Though achieving a fully operational SSO, standards, and certification program will take many months, ICBA believes that the endeavor is well worth the effort. Community banks are eager to contribute to its implementation and success. Should you have any questions or would like to further discuss the comments raised in this letter, please do not hesitate to contact me at Michael.Emancipator@icba.org or 202-821-4469.

Sincerely,

/s/

Michael Emancipator
Vice President & Regulatory Counsel