September 22, 2020

Via electronic submission

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

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

To whom it may concern,

The Alliance for Innovative Regulation, AIR, appreciates the opportunity to submit comments in response to the FDIC's Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services.

AIR is a nonprofit organization co-founded in 2019 by Jo Ann Barefoot, former Deputy Comptroller of the Currency, to help catalyze and shape modernization of the financial regulatory system for the Digital Age. We produce thought leadership, convene gatherings for learning and problem-solving, and conduct tech sprints and proof of concept projects to develop and demonstrate digital solutions to regulatory challenges. Last month we released a seminal paper in the form of a Request for Comments, titled A Regtech Manifesto: Redesigning Financial Regulation for the Digital Age. This year we are exploring development of a public/private initiative called the Regulatory Design Project to develop open source standards that can facilitate transition to a digital, interoperable financial regulatory system, in order both to improve outcomes and reduce costs.

We commend the FDIC's focus on this issue, which we believe to be one of the most critical challenges facing community banks and, by extension, the financial wellbeing of their diverse customers and communities.

The RFI has been published at a time when AIR, itself, is actively exploring the concept of developing third party certification standards and becoming a Standards Setting Organization (SSO), and potentially a Certifying Organization (CO). Our logic tracks closely with that of the FDIC in examining this idea, which we view as having the utmost urgency.

Arguably the greatest challenge facing small banks is the difficulty of keeping up with new technology. It impacts these banks in two ways.

First, bank customers today expect cutting edge technology in the financial services they use, just as they do in everything else. They expect an easy and enjoyable user experience (UX). They expect mobile and online services to be intuitive to navigate and effective in performing tasks or delivering answers. They expect services to be instantly available. They expect them to be increasingly affordable. All of this is particularly true of millennial consumers, who now comprise the largest generation in history and who are entirely digitally-native. Serving them well requires the ability to leverage technology that is constantly evolving. Like other industries, banking is digitizing -- converting information and processes into digital formats that are capable of making things work better, faster and cheaper, all at once. Large banks are well along in this journey, as are many nonbanks that now offer financial services. Small banks will be at a competitive disadvantage if they cannot keep pace.

Second, banks today need better technology in order to manage their own operations and costs, including the regulatory compliance costs that account for a very substantial share of their cost of doing business. It is well documented that smaller banks bear a disproportionately high compliance burden in comparison to their larger competitors. Here again, the most promising leveling factor is better technology.

Few small banks are in a position to develop cutting edge technology in-house. Instead, they need to be able to draw upon and partner with technology vendors that can provide what they need. To meet customers' rising expectations, they need to be able to work with fintech firms that can enhance capabilities in areas like customer onboarding or credit underwriting. To meet their compliance needs they need access to regtech vendors that can perform regulatory tasks better, more quickly, and at lower expense.

We at AIR believe that the future of community banking rests on whether these two technology challenges can be solved, quickly enough to keep most small banks competitive and profitable.

We believe there are two primary impediments to this modernization. One is the reliance of most small banks on traditional core IT technology that is aging and makes it difficult for new solutions to "plug in" to existing infrastructure. The second is the difficulty community banks face in vetting and working with fintech and regtech vendors and partners. This second factor is driven in part by regulatory rules and sensitivities, but is also broader, impacted by the intrinsic difficulty of evaluating young technologies that lack long track records. A well-designed standards and certification program, developed with input from the FDIC and other regulators, could solve much of this vendor problem and open the door for innovation by smaller banks.

Solving this latter dilemma is central to the questions being raised in the FDIC's RFI. As the RFI notes, changing the third party risk process could "allow community banks to engage with third

parties, including fintechs, permit FDIC supervision resources to be used more efficiently and effectively, and reduce costs of doing business for financial institutions and providers of data."

Below are our thoughts on some of the questions raised in the RFI. Many of our comments are most relevant for regtech compliance vendors, but apply also to fintech firms seeking to serve or partner with banks, and also to vendors offering models such as for loan underwriting. The barriers for all three types of relationships -- fintech partners, regtech vendors, and providers of models -- are similar.

We have mainly addressed the RFI's "Scope" section, i.e. Questions 1-10, although many of our comments touch on the later sections as well.

Question 1: Factors inhibiting adoption of third party technologies

As noted above, major factors inhibit adoption of new technology by community banks. Among these, the two most serious are small banks' widespread reliance on rigid core IT and regulatory third party risk requirements imposed by regulators. The latter is a barrier due both to the cost of going through the due diligence process and to banks' fears of regulatory criticism if they, in effect, try something new.

The costs are very considerable for both the bank and the third party. Since many fintech and regtech firms are offering point-solution tools, it often is not worth it to the bank to undertake a time-consuming vendor review process. Similarly, many technology vendors are young, smaller firms that do not have the resources to spend months -- sometimes more than a year -- navigating a bank's review of their tools. It is also extremely inefficient for these firms to navigate bank due diligence processes one by one. A certification process could solve most of this problem, as well.

We recognize that the RFI does not address changes that might be needed in the current third party risk standards, but it is worth noting that these were generally written before the new technology available today. Banks often ask questions that are not relevant for young firms that were "born digital," even though these firms may offer superior technology. The breakthrough technology used by fintech and regtech firms today is leveraging the profound changes that have occurred in computer programming in just the past ten years. For example, many bank questionnaires still ask for responses that reflect assumptions about mainframe IT as the normal paradigm, such as seeking information on the provider's server security. Banks also ask for information like several years of audited financial statements, which young and small firms may not have.

If the FDIC or an SSO decides that young firms should not be able to be bank vendors and partners, they should do so in recognition that small banks will almost inevitably fall behind the technology curve as a direct result. Large banks can produce and adopt these technologies on

their own. Small banks will not be able to compete if the system cannot enable them to do so as well.

Questions 2, 3 and 4: Pros and cons of standard-setting and voluntary certification

As noted, AIR is itself becoming a standards-setting body because this approach can solve tremendous problems in the system as it stands today.

Interagency uniformity: The current third party risk standards have extensive overlap among regulatory agencies, but this may not continue as agencies move to modernize their requirements in light of new technology. Interagency coordination on new standards, rules and guidance is a complex process, but uniformity and consistency are extremely important to making these processes efficient for third party vendors and model providers. By creating an external platform for collaboration, it may be possible to move more quickly and efficiently in working on multi-agency standards and to assure consistent outcomes.

It should be noted that this uniformity could also be extended internationally over time. This would give US community banks easier access to solutions developed by vendors and partners from other countries, many of which have very advanced technologies.

Balanced input: We believe that the best regulatory standards reflect participation by both the public and private sectors. Again, a neutral platform at a nonprofit can help assure that standards meet regulators' needs and expectations, while also assuring that they are fully responsive to the practical needs and limitations of the industry -- both the banks and the third party providers.

Flexibility: By moving the standards-setting process onto a neutral platform, regulators can create a process that can be designed to be far more nimble than can most regulatory change procedures. Almost by definition, an independent party will be able to learn more quickly about needed changes in standards, to develop updates, and to smooth out obstacles to adoption.

Compatibility: A related issue is that a specialized SSO is more likely than a regulatory agency to be able to recognize practical issues in designing standards that will be compatible with constantly-evolving technology at both banks and vendors.

Question 5: Specific challenges to be addressed

As discussed further below, a voluntary standards and certification program would have the potential to solve many current problems. These include how banks can determine whether the vendor's solution works; whether the vendor technology is compliant and secure; and potentially whether the vendor has sufficient capacity to serve the bank's needs. On the vendor side, it can help solve the problem of having to navigate numerous similar but separate diligence reviews and the lengthy elapsed time involved in each review before reaching the contract stage.

Another specific difficulty in the current system is that rules impede a bank's ability to test potential vendor solutions, by barring institutions from paying for vendor services until after the diligence process has run and the parties have entered into a purchase contract. For complex tools, it can make sense for banks to have vendors create a "sandbox" environment customized to the bank's individual data formats and workflows. Most large banks develop sets of anonymized or synthetic data for this purpose, but many small banks can not readily do so. Particularly for small vendors, the costs of undertaking this customization without a contract can be prohibitive.

This problem could be solved by allowing payment specifically for this kind of testing scenario, with the vendor walled off from any access to the bank's systems during the test period. It could also be solved by having an SSO create certification protocols for determining that the offered services are sound.

Question 6: Cost-reduction

Development of voluntary standards would definitely enable reduced costs for all the parties. In the current system, every bank must duplicate the efforts of other banks in vetting vendor technology, and conversely, every vendor must repeat its diligence-related efforts with every bank that considers its services. Bank vendor questionnaires cover largely the same material, but do so in different formats, which means the vendor essentially starts from scratch with each new bank prospect. With an SSO process, vendors could be vetted once and certified for use by banks, and banks would be relieved of most of the burden of conducting the reviews. This would capture major gains in cost savings.

The process would also produce downstream cost savings over and above the reduced costs of vendor review. As noted earlier, streamlining the vendor review process would greatly reduce the disincentives for banks to adopt these new technologies, and that adoption will in many cases generate further savings by reducing manual labor, inefficient workflows, mistakes, and compliance errors. These problems are widespread today due to old technology and collectively contribute to the high operating and compliance costs borne by small banks.

Question 7: Challenges, costs and benefits of a voluntary certification or standards program, including allocation of costs

As we have laid out elsewhere in this comment, the benefits of such a program could be very substantial in both enabling community banks to take advantage of newer and better technology and in reducing their costs and risks in vetting it. Again, we think enabling small banks easily to acquire cutting edge technology through vendors and partners is probably necessary for their viability as a sector.

Regarding challenges, one is the major risk of chilling innovation, which will be discussed below under Question 8. Other challenges include the following (some of which touch on the questions raised in the RFI numbered 11 to 30, which we have not addressed individually):

Existing vs. new SSO: One key is whether to leverage an existing standard-setting organization or set up a new one. While expanding the scope of an existing body could leverage its instructure and standard-setting knowledge, we think any SSO for this purpose must take a "digitally-native" approach to it, rather than starting with assumptions grounded in legacy practices and data structures. We would lean to starting something new. As noted earlier, AIR is itself exploring taking on a role of this kind, driven in part by this logic.

Makeup and design of an SSO: We think this SSO would need active participation by both regulatory agencies and industry. Their two perspectives are each essential, since the standards would need to satisfy the regulators but also be readily, efficiently implemented by industry. A model might be the standards-setting body for the Worldwide Web, the Worldwide Web Consortium, or W3C. It sets standards for the web and has membership drawn from businesses, nonprofit organizations, academia, governmental bodies, and individuals. It is funded by member dues as well as grants and has established governance and processes to enable a vendor-neutral standards-setting system. We recommend that the FDIC undertake a study of potential models that looks at existing bodies in and outside of the realm of finance.

Elements to certify: An SSO process should consider the scope of the standards and certification process. Banks want to know whether the prospective vendor or partner's solution works as promised; whether the vendor or partner meets requirements for data security; whether the vendor or partner is compliant with applicable laws and regulations and has the needed skills and capacity to continue to comply; and whether the vendor or partner is robust -- well managed, well-capitalized, and sustainable. The FDIC should consider whether the SSO program should solve for all of these or only for some. The standards involved are quite different, in terms of evaluating technology versus evaluating factors like business capability.

Certification process: It is not clear to us whether the ideal model would be to have both standards-setting and certification handled by one organization or instead to create a decentralized certification process.

One instructive model here is the way SOC 2 cybersecurity standards are set and certified. The standards are set by the American Institute of CPAs (AICPA), which sets standards for data protection based on five "trust service principles"— security, availability, processing integrity, confidentiality and privacy. SOC 2 certification reviews are then performed in a decentralized manner by experts who are qualified to do them. This rigorous process enables certified organizations to gain the confidence of customers, investors and others.

In fact, having a SOC 2 certification is an example of a standard that an SSO should consider requiring for vendors that want to work with banks in matters involving sensitive data.

Technology-based certification: A certification program should be designed to enable much of the evaluation to be done electronically. For example, Github offers vulnerability and security screening of code that it hosts. Methods such as this can reduce the time and cost involved in companies achieving certification.

Maintenance: Standards can be easier to set up and disseminate than to update and maintain as the world around them changes, and especially as technology evolves. As discussed elsewhere in this comment, there would be significant risk of the standards becoming obsolete and/or devolving into anti-competitive gatekeeping.

Funding: One could envision standard-setting being funded through member fees, grants, and potentially government contributions. A distributed funding model would help counter the risk of the program becoming dominated by its primary funders.

Open Source: Any standard-setting process should seek to incorporate open source code as a basis, so that any regulator, regulated firm and vendor will be able to use, vet and build upon the foundational elements. This will not prevent participants from building proprietary code on top of the open code, but will help the system accelerate adoption, move toward interoperability, and reduce the need for ecosystem participants, including regulators, to "reinvent the wheel" over time throughout the system.

Voluntary adoption: We strongly agree with the FDIC's framing of this challenge in terms of creating standards for voluntary adoption.

Risk tiering: A principle that should guide standard-setting for bank third parties is the degree of risk involved in the

Question 8: Risk of undermining innovation

Creation of voluntary standards and voluntary certification processes would create a risk of undermining innovation in a number of ways.

First, as noted in the RFI, the certification process might become interpreted, by banks and perhaps by examiners, as a de facto requirement. This would have to be actively managed through examiner training and communication to the industry.

Second, standard-setting has a tendency to become a gatekeeping exercise. The FDIC would have to manage against the risk that vendors would tend to dominate a standards-setting process and use it to impede new competitors entering the market. Similarly, there would be a risk that banks involved in standard-setting would have a tendency to use the process to limit their own competition, by trying to make the standards difficult for competitors to adopt.

Third, standard-setting always raises a risk of locking in obsolescence. Stories abound of standard-setting efforts that have involved very lengthy development -- so lengthy that the standards were already obsolete before deployment. Similarly, standards tend to be built for existing technology and then have difficulty being reinvented for new technologies. They can evolve from initially solving problems to, over time, creating them.

These challenges are becoming ever-more acute due to the pace of change and emergence of mold-breaking technologies in the digital age.

Question 9: Supervisory changes to address safety and soundness and consumer protection

We believe banks will have to become adept at using modern digital technology, both to maintain safe and sound performance and consumer protection. As the industry begins to adopt superior digital technologies, banks that fail to do so will increasingly fall below regulatory expectations.

We urge the FDIC to take the following steps:

Encourage new underwriting models: A key area is use of new models and new kinds of data in credit underwriting. Evidence is mounting that use of these new models is both highly predictive of loan performance and is also more inclusive than are traditional models, in ways that can advance regulatory goals such as those expressed in the Community Reinvestment Act. For example, the nonprofit FinRegLab (for which I chair the board of directors) has conducted research validating the promise of cash-flow underwriting in fostering sound and inclusive finance.

The FDIC and other agencies should study these new underwriting techniques, issue clear guidance on how banks can assure that the models they use are compliant, and actively encourage adoption of sound and inclusion models that meet these expectations. The FDIC and other agencies have already encouraged this kind of exploration, but will need to sustain and enhance that effort.

Provide safe harbors if new regtech detects old problems: Another supervisory adjustment should focus on the risk that superior new regtech tools may discover noncompliance that was not detected by older ones. A key example is anti-money laundering. Here too, the FDIC and other agencies have encouraged testing and use of new regtech solutions. However, the industry still expresses concern about whether regtech adoption will be acceptable to examiners. A specific concern here is the possibility that these newer techniques will uncover financial crime that was missed by older tools, and that banks could face regulatory and enforcement penalties for past activities.

We urge regulators to state clearly that they will not penalize past activity that occurred while the bank was using compliance tools that were considered, at the time, to be effective. Similar issues could arise in areas of credit discrimination or UDAAP, if new monitoring tools find patterns that were not evident in the past, and where there is no indication of intentional bad practice.

Permit banks to pay vendors for experimentation: Another recommendation is to actively encourage banks to conduct testing of prospective regtech and fintech vendors and partners and, as noted earlier, to permit banks to pay for small-scale customized trials even before they select the vendor involved for deployment of its technology.

Treat reliance on old and less effective technology as an unsafe practice: We believe bank supervisors should adopt an active and sustained program of encouraging banks to adopt digital-age vendor technologies. As compliance and prudential performance improve as a result, regulators should treat use of older, less effective technology as an unsound practice and/or inadequate consumer protection. While this pressure should be introduced gradually, it will probably be needed to help the industry undertake the cost of the needed technology conversion without individual banks facing short term competitive disadvantages as they do so.

This should be akin to the agencies requiring banks to continue to upgrade their information security technology to keep up with cybersecurity threats.

Question 10: Other supervisory, regulatory or outreach efforts

Bank supervisors face a novel and difficult challenge -- how to move faster. Technology is changing the financial system at exponential rates, while regulatory processes are built to move deliberatively, at linear speed. This creates rising risk that government policies will lag behind the reality in the market. It also means, for community banks, that regulatory and supervisory policy will prevent them from keeping up with competitors, by impeding their ability to engage with vendors and partners that have young digital technology solutions for them. Both regulators and banks will need to find ways to move faster in order to be effective in the digital age.

Other steps should include:

Migrating the system's regulatory technology to a platform architecture: The FDIC and other agencies should actively foster a shift of the regulatory technology infrastructure in banking from the current vendor-dominated "walled garden" design to a platform architecture that enables modularity and "plug in" solutions that will automatically be compatible with the bank's systems via API's, without the need for integration.

Education and support of community banks: We recommend that the FDIC and other agencies work actively with the industry trade associations to help equip community banks with the needed education to make these kinds of changes.

Experimentation: Innovation of all kinds requires trying out new approaches, in an environment where failure is permitted and can be studied, but cannot do any harm. We encourage the FDIC to create a robust program of experimentation of its own on both fintech and regtech.

The agency should also encourage banks to do the same and should assure that regulations and examiner culture do not impede their ability to do so, as long as experimentation is done in a contained, safe space on a small scale.

Interagency and industry collaboration: We urge the FDIC to work closely with the other bank regulatory agencies to address this full spectrum of challenges facing community banks.

One key to accelerating regulatory change for the digital age is to intensify cross-silo collaboration, and especially to bring technology people to the table when supervisory and regulatory decisions are being made.

AIR has issued a Regtech Manifesto that lays out the case of why regulatory activities must convert to digitally-native design; what such a system would look like; and how to migrate to it from today's analog system.

In conclusion, again, we commend the FDIC for the visionary questions laid out in its RFI and will be pleased to be helpful in any way we can.