From: Steve Stevens <Steve.Stevens@x9.org>
Sent: Monday, September 21, 2020 8:18 PM
To: Comments
Subject: [EXTERNAL MESSAGE] ASC X9: FDIC RIN 3064-ZA18
Attachments: FDIC-RFI-Questions SS-Final.pdf

Mr. Robert E. Feldman,
Attached, please find X9's reply to the FDIC's Request for Information titled "Standard Setting and Voluntary certification for Models and Third-Party Providers of Technology and Other Services". Please contact me if you have any questions.

Best regards,
Steve Stevens
Executive Director of ASC X9
275 West Street, Suite 107
Annapolis, MD 21401
Office: 410-267-7707
Web: www.x9.org

Overview:

On July 24, 2020, the Federal Deposit Insurance Corporation ("FDIC") published a Request for Information ("RIN") 3064-ZA18 in the Federal Register/Vol. 85, No. 143. Comments are due by September 22, 2020. The RIN is for a possible FDIC program titled "Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services". The RIN has 24 total questions of which 9 are relevant to the Accredited Standards Committee X9 Inc. ("X9") and X9 has provided comments to those questions below. This reply is being emailed to comments@fdic.gov. If you have any questions, please contact Steve Stevens at steve.stevens@x9.org.

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

Response 1: The lack of standards could act to inhibit adoption of new technology or the onboarding of third parties. Without any guidance, such as a standard and/or a certification program, community banks are left to their own devices to determine if new technology meets regulatory requirements. While this is true for all IDIs, smaller IDIs do not have the resources that large IDIs have regarding the evaluation of new technology so they may be reluctant to adopt new technology. A standard and certification program would provide at least a minimal level of guidance and assurance regarding new technology making it somewhat more likely they might adopt new technology. The more support provided by the regulators in the standard and certification process, the more likely small IDIs might feel comfortable adopting new technology.

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

Response 2: Standards can establish minimum requirements for products marketed to IDIs. These requirements would both protect the IDIs from possible attack by requiring basic security elements and when appropriate, guaranteeing the products meet all rules and regulations applicable to the products. A certification program would validate that the product meets the requirements in the standards. The certification program would reduce the overhead on the part of both the third-party providers and the IDIs by eliminating the need for each IDI to perform a detailed review of the requirements found within the standards for each product. Just the elimination of a review of the basic elements for each product by each IDI would be an improvement and save costs to both parties. The certification program would be voluntary so providers do not have to participate if they believe the program is not designed for their product or put another way, their product is outside of the technology and products covered in the standard.

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

member fees for SSO participation, certification fees)?

Response 7, Part 1: The first challenge is to develop an open consensus standard that accurately captures the elements required to meet due diligence requirements and that satisfies the needs of the IDIs. Next a certification program will have to be established to determine if submitted products and services meet the requirements of the standard. This will require full time staff and the associated overhead. One option is to contract with an existing certification organization to perform the certification program and thus pay only the incremental costs to the organization.

Part 2: The cost of both the SSO and the CO is usually born by the participants/customers. For the SSO, this would be members of the SSO that participate in the development and maintenance of the standard. For the CO, the costs are covered by charging for each certification issued. The SSO and CO perform separate functions and for a number of reasons would most likely be performed by two different and independent entities.

Question 15: If the FDIC partnered with an SSO to set standards for due diligence and assessments of models or third-party providers of technology and other services, what considerations should be made in choosing the SSO? What benefits or challenges would the introduction of an SSO into the standard-setting process provide to IDIs, third-party providers, or consumers?

Response 15: Any SSO chosen for this work should be certified by a higher organization, such as ANSI, and held to certain levels of due process and conduct. These requirements should include an open consensus development process that is transparent, balanced, accessible and responsive to the requirements of the various stakeholders. Having a SSO take over setting the minimum requirements to meet due diligence would eliminate the need for the IDIs and third-party providers to duplicate this function every time a new product or service is used. Using an SSO should lower the overhead and thus the cost to implement new products and services plus provide a more reliable and consistent application of the rules.

Question 16: 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?

Response 16: It is very rare for a technology, product or solution to remain unchanged for a long period of time. For the most part, standards have always had to face and adapt to changing landscapes. However, some aspects of a technology do remain the same even as other parts change. For example, over the last 30 years, the algorithms used to encrypt data have gone through many changes as technology has changed, but the requirement to provide a level of security for the data being encrypted has remained unchanged. In some cases, it may be possible to standardize the desired result and allow the technology that provides the solution to

change. In other cases, the standard will have to be updated when the technology changes. ANSI provides a mechanism that can be used for standards that cover an area that has frequent changes in technology. Standards like this are setup to be under "Continuous Maintenance" which has a shorter development period to provide a quicker response to changes in technology or requirements.

Question 17: 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?

Response 17: ANSI provides a framework to establish a SSO. The requirements for the SSO are specified in the ANSI Essential Requirements, available on the ANSI web site. SSOs must pass an audit every five years to maintain their accreditation. ANSI has over 100 accredited SSOs and has been in the standards business for over 100 years. The advantages of using an ANSI accredited SSO are well documented. They provide an open, consensus driven, balanced, transparent process for developing standards and well-established rules for due process. On the negative side, reaching consensus with a diverse group of participants is not always a fast process. Having a single party that dictates what goes in a standard is always faster but it does not always serve the best interest of the users.

Question 18: 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?

Response 18: Part 1: With any new voluntary program there is always some reluctance to spend money to participate when the ROI is not certain. Both IDIs and third parties have good reasons to participate as long as both parties participate. Some catalyst may be required to achieve the desired level of participation. One possible catalyst could be the creation of a limited safe harbor for the IDIs if they select products or services that are certified to meet the standard. This would create a demand for the certified products and cause to third parties to participate. This would also cause both IDIs, third parties and the FDIC to want to participate in the standard's process.

Part 2: The major hinderance in participation in the standard development process is cost. Cost can be measured in both membership dues used to operate the SSO and the cost of providing subject matter experts to develop and maintain the standard. A non-profit SSO, such as X9, is driven to control costs and provide as many channels as feasible for companies to participate.

Question 19: 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?

Response 19: The best way to structure a SSO is to separate the business activities from the standards activities. This provides for the optimum use of subject matter experts. Participation by SMEs is key to drive a successful end-2-end process. Most ANSI SSOs follow this model. This is the model X9 uses.

Question 20: 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?

Response 20: The FDIC and other regulators have to play a role in the development and maintenance of the standard. At the end of the day, it is the regulators that have to be satisfied that any standard or certification program meets their requirements. A standard that fails to meet regulatory requirements would be harmful to the industry and the participants and a waste of time and resources. A mature, accredited SSO does not need oversight on how to develop a standard; that process will already exist. The SSO will need participation from regulators in the form of subject matter expert engagement and input. Additionally, the SSO will need people from these groups with the insight and experience to lead the work efforts. SSOs provide a framework and structured environment for the experts/regulators to come together and develop a useful standard and certification program.