September 22, 2020

Via Email (Comments@fdic.gov)

Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, N.W.
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 Mr. Feldman:

Mastercard International Incorporated ("Mastercard") submits this comment letter to the Federal Deposit Insurance Corporation ("FDIC") in response to its request for information on standard setting and voluntary certification for models and third-party providers of technology and other services ("RFI").[1] We would like to express our support for this initiative of the FDIC to promote the adoption of technology by banks. We believe that technological innovation by banks, particularly smaller banks, is crucial to their ability to compete in the financial services marketplace. Our comments below address important aspects of introducing standards and a voluntary certification program for third-party providers of models and technology services to banks, as well as key characteristics for adopting standards and for choosing a Standard Setting Organization ("SSO").

Background on Mastercard

Mastercard is a technology company in the global payments industry. Mastercard operates the world's fastest payments processing network, connecting consumers, financial institutions, merchants, governments and businesses in more than 210 countries and territories. Mastercard does not issue payment cards of any type nor does it contract with merchants to accept those cards. In the Mastercard network, those functions are performed in the United States by financial institutions. Mastercard refers to the financial institutions that issue payment cards bearing the Mastercard brands to cardholders as "issuers." Mastercard refers to the financial institutions that enter into contracts with merchants to accept Mastercard-branded payment cards as "acquirers."

When a cardholder presents a Mastercard-branded payment card to a merchant to purchase goods or services, the merchant sends an authorization request to its acquirer, the acquirer routes the request to Mastercard, and Mastercard routes the request to the issuer. The

[1] 85 *Fed. Reg.* 44,890 (July 24, 2020).

issuer either approves or declines the authorization request and routes its decision back to the merchant through the same channels. Mastercard's role in the transaction is to facilitate the payment instructions among the parties to the transaction and to facilitate the clearing and settlement of the payment transaction between the issuer and acquirer.

Comments

Mastercard strongly urges the FDIC to partner with existing SSOs that are respected and known in the industry to formalize standards for third parties that provide banks with models and technology services and a voluntary certification program for the same. The issues raised by the RFI have relevance for Mastercard as an operator of a payment network in which thousands of U.S. banks participate, as discussed above, and also as a provider of other services to such banks, including data analytics, consulting, cybersecurity solutions, and issuer processing. Examples of these other services include the following:

- With regard to Artificial Intelligence ("AI"):
    - Mastercard ThreatScan, an AI-powered solution that helps banks proactively identify potential vulnerabilities in their payment card authorization systems. The service works alongside an issuer's existing fraud tools, imitating known criminal transaction behavior to identify potential weaknesses and prompt action before fraud potentially occurs.
    - Decision Intelligence, our fraud scoring technology, which scores billions of transactions in real time every day while increasing payment card approvals and reducing false payment card declines.
    - AI and data analytics with cyber risk assessment capabilities that are designed to help financial institutions, merchants, corporations and governments secure their digital assets.
- An e-commerce fraud and dispute management network that enables the sharing of intelligence between merchants and issuers to stop delivery of goods or services when a fraudulent or disputed payment card transaction is identified and to facilitate cardholder refunds (instead of chargebacks).
- Data insights to help customers with anti-money laundering compliance and identification and prevention of other financial crimes.

If the FDIC were to proceed with a voluntary certification program, the FDIC would reduce the barriers for many smaller banks to the use of third-party models and technology services. For service providers to numerous banks, such action also would reduce burdens that result from being the subject of multiple overlapping bank diligence and monitoring processes.

We offer our comments below on portions of five questions raised by the FDIC regarding a voluntary certification program for third-party providers of models and technology services to

banks, the standards that should serve as a basis for the certification program, and important characteristics of SSOs: Questions 13, 14, 15, 17 and 19 from the RFI.

Voluntary Certification Program for Third-Party Providers of Models

Question 13. 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?

Mastercard encourages the FDIC to put in place a voluntary certification program with respect to validation of models that rely on AI, machine learning, and big data processing. Such a program would benefit both banks and third-party providers of models, as discussed in more detail below.

The FDIC Supervisory Guidance on Model Risk Management (the "Model Guidance") contains specific requirements for banks to manage risks associated with third-party models.[2] To satisfy these requirements, banks are likely to require third-party model providers to:

(i) Provide developmental evidence explaining a model's components, design, and intended use, to determine whether it is suitable for the bank's products, exposures, and risks;

(ii) Provide appropriate testing results that show a model works as expected; and clearly indicate the model's limitations, assumptions, and where the model's use may be problematic;

(iii) Conduct ongoing performance monitoring and outcomes analysis with disclosure to bank customers, and make appropriate modifications and updates over time; and

(iv) Provide information regarding any data and assumptions that did not originate from the bank that are used in a model, so the bank can assess the extent to which it is representative of the bank's situation.

The Model Guidance directs banks to evaluate all the foregoing information in order to validate a third-party's model. Moreover, the Model Guidance instructs banks to incorporate third-party models into their broader risk management frameworks as they would their own proprietary models.[3] Additionally, the Model Guidance creates an expectation that banks should have as much knowledge in-house regarding third-party models as possible, in case a third-party provider or the bank terminates a contract for any reason or the third-party provider is no longer in business.[4] The burden on banks, particularly smaller banks, to comply with the Model Guidance is substantial.

[2] FDIC, *Supervisory Guidance on Model Risk Management*, FIL–22–2017 (June 7, 2017).

[3] *See, e.g., id*. at 13.

[4] *Id*. at 14.

In our experience, every bank that uses the services offered by Mastercard that involve models requests considerable amounts of information and documentation from Mastercard and undertakes a significant effort in time and cost to comply with the Model Guidance. An SSO that sets standards for models and a voluntary certification program, by which third-party providers are able to obtain certification of fulfillment with relevant standards, would make the model risk management processes vastly more efficient and less burdensome, expensive, or susceptible to error.

An SSO-driven process would allow the information and the documentation requested of a third-party provider by banks to be provided a single time to a certification organization, instead of multiple times for each bank that uses the service. Moreover, a voluntary certification program should improve model transparency in a manner that should improve the quality of validations. That is, a third-party provider likely will be more willing to provide proprietary information related to its models (*e.g.*, product components or design) to a single certification organization than to every bank customer. This concern regarding revealing proprietary information has become increasingly relevant as models rely more heavily on complex AI.

Ultimately, an SSO/voluntary certification program would result in more banks being able to engage third-party providers of models and would result in more accurate validations. Also, by lowering the compliance costs for third-party providers, more third-party providers would be motivated to develop models for banks. Thus, the FDIC has an opportunity to be a catalyst for a "virtuous cycle" of technology innovation that should inure to the benefit of banks, particularly smaller banks, and their customers.

Voluntary Certification Programs for Third-Party Providers of Technology Services

Question 14. How can the FDIC identify those types of technology or other services, or those aspects of the third-party provider's condition, that are best suited for a voluntary certification program or other standardized approach to due diligence? For example, should such a certification program include an assessment of financial condition, cyber security, operational resilience, or some other aspect of a third-party provider?

In our capacity as a third-party provider of models to banks, we receive regular requests from banks for information regarding our models. In particular, the following topics on which we frequently provide information to our bank customers would be ideal for a voluntary certification program:

(i) Impermissible bias reviews;

(ii) Model monitoring;

(iii) Model governance; and

(iv) Model transparency.

In addition to being a third-party provider of models to banks as discussed above, Mastercard is a third-party provider of technology services to banks more generally. Under its Guidance for Managing Third-Party Risk ("Third-Party Risk Management Guidance"), the FDIC expects a bank's third-party provider oversight program to include monitoring on an ongoing basis of a third party's quality of service, risk management practices, financial condition, and applicable controls and reports.[5] Based on our experience as a long-time provider of technology services, this oversight often takes the form of lengthy and detailed questionnaires on topics related to our operations. The topics covered by these questionnaires that would be ripe for an FDIC-program of standards and voluntary certification include:

(a) Access management;

(b) Business continuity and disaster recovery;

(c) Collection, processing and storing requirements;

(d) Physical security;

(e) Data retention;

(f) Third-party management;

(g) Vulnerability management;

(h) Risk management;

(i) Operational management; and

(j) Human resources and people management.

Such standards and certification would lead to many of the same benefits for banks and third-party providers as we discuss above in the context of models.

The oversight by banks of third-party providers of technology services also covers the topic of cybersecurity. However, this topic already is addressed through a widely-accepted validation process established by the Payment Card Industry Security Standards Council ("PCI Council"). We encourage the FDIC to review the PCI Council approach as an example of the well-designed, well-functioning certification program for third-party providers of technology services, and we discuss our experience with the PCI Council in more detail below.

Standard Setting Organizations and Standards

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

[5] FDIC, *Guidance for Managing Third-Party Risk*, FIL–44–2008 (June 6, 2008).

or challenges would the introduction of an SSO into the standard-setting process provide to IDIs, third-party providers, or consumers?

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?

Question 19. What is the best way to structure a Standard Setting Organization ("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?

Mastercard has participated in, or been associated with, a number of SSOs and similar collaborative bodies as a result of our experience as an operator of a global payment network. We believe the most expeditious path forward for the FDIC to implement a certification program is to designate existing SSOs that are well-regarded within the financial services industry to be the SSOs for the certification program and to use the existing standards of such SSOs to the greatest extent possible. For example, the FDIC should consider the National Institute of Standards and Technology ("NIST"), the PCI Council, and the International Organization for Standards ("ISO"), among others.

By working with existing SSOs that are familiar to banks and third-party providers, the FDIC should be able to develop a program of standards and certifications without needing to undertake the time-consuming process of forming, staffing, and developing from the ground up a new SSO. Moreover, existing SSOs already have developed and published widely accepted standards for several of the topic areas that are addressed in the Model Guidance and Third-Party Risk Management Guidance. The industry is already familiar with these existing standards. By adopting them, the FDIC would enable third-party providers and banks to take advantage of the certification program without having to make significant changes to their current practices.

Our experience with the PCI Council offers an example of the work already done by an SSO that could be valuable to the FDIC. The PCI Council is a global forum that brings together payments industry stakeholders to develop and drive adoption of data security standards and resources for safe payments worldwide.[6] The PCI Council developed a set of security standards, the PCI Data Security Standard ("PCI DSS"), which addresses some aspects of the Third-Party Risk Management Guidance. The PCI DSS consists of twelve technical and operational requirements, including multiple sub-requirements, which contain numerous directives to protect cardholder data and to monitor, test, and maintain a network's security.[7] These standards apply to all organizations that store, process or transmit cardholder data and/or sensitive authentication data, and serve as guidance for software developers and manufacturers of applications and

[6] *See* https://www.pcisecuritystandards.org/about_us/.

[7] *See, e.g.*, PCI Council, *PCI Quick Reference Guide, Understanding the Payment Card Industry, Data Security Standard version 3.2.1* (2018) (the "PCI Reference Guide").

devices used in those transactions.[8] The PCI Council also conducts training and determines qualification for an entity to be a qualified security assessor, an organization that assess compliance with the PCI DSS.[9]

We believe that there is a great deal of existing activity in the standards field that the FDIC can leverage. In our view, it would be a great first step toward developing an FDIC-approved standards and certification program if the FDIC were to publish a mapping of the requirements from its Model Guidance and Third-Party Risk Management Guidance to industry standards developed by the NIST, the PCI Council, and ISO so that third-party providers and banks have an understanding of how compliance with a standard may also satisfy the FDIC's regulatory expectations.

* * *

Mastercard appreciates the opportunity to provide comments to the RFI. If there are any questions regarding our comments, please do not hesitate to contact the undersigned at (914) 249-1871 or Bernadette.Walli@mastercard.com, or our counsel at Sidley Austin LLP in this matter, Joel Feinberg, at (202) 736-8473.

Sincerely,

Bernadette Walli
Counsel, Regulatory Affairs

cc: Joel D. Feinberg

[8] *See, e.g. id.*

[9] PCI Reference Guide at 10.