July 1, 2021

Via www.regulations.gov

Office of the Comptroller of the Currency
400 7th Street, S.W.
Washington, DC 20219

Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, N.W.
Washington, DC 20551

Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, DC 20429

Bureau of Consumer Financial Protection
1700 G Street, N.W.
Washington, DC 20552

National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314

RE: Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, including Machine Learning; Docket ID OCC-2020-0049 (OCC), Docket No. OP-1743 (Board), RIN 3064-ZA24 (FDIC), Docket No. CFPB-2021-0004 (CFPB), and Docket No. NCUA 2021-0023 (NCUA)

Ladies and Gentlemen:

Mastercard International Incorporated ("Mastercard") submits this comment letter to the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("Board"), the Federal Deposit Insurance Corporation ("FDIC"), the Bureau of Consumer Financial Protection ("Bureau") and the National Credit Union Administration ("NCUA" and, together with the OCC, Board, FDIC and Bureau, the "Agencies") in response to their Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, including Machine Learning (the "Request").[1] Mastercard appreciates the opportunity to provide input on the Request. We recognize the important opportunities that artificial intelligence ("AI") presents to the financial services industry and the need to ensure

[1] 86 *Fed. Reg.* 16,837 (Mar. 31, 2021).

responsible use of AI. In our comments below, we recommend actions that could be taken by the Agencies to (1) streamline oversight of third-party providers of models for banks, savings associations, and credit unions (collectively, "banks") —particularly community banks—and to streamline oversight of service providers; (2) offer some best practices for service providers to manage their AI services; and (3) urge the Agencies to largely rely on the existing regulatory framework, but to take a principles-based approach in adopting any new AI-specific regulations.

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 banks. 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 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 is committed to the goal of responsible AI use and development. AI's potential benefits are enormous but we recognize that the Agencies have a duty to monitor the impacts of AI carefully. This notwithstanding, we believe that changes in technology do not necessarily require changes to regulations, especially where existing regulations are already sufficient. Similarly, given the variability and rapidly evolving nature of AI technology, we believe that regulation is prone to becoming obsolete quickly and a one-sized-fits-all approach can be problematic. We encourage the Agencies to continue their dialogue with industry to figure out how AI technologies can best be deployed in a responsible way and to carefully consider whether regulations may be necessary. In those instances in which the Agencies identify regulatory concerns, we believe that the best approach would be the issuance by the Agencies of principles-based rules or guidance that are conducive to a rapidly changing environment.

We offer our comments below on: (1) third-party risk management of AI service providers, especially in the context of community banks; (2) best practices for AI service providers that could guide the Agencies in setting principle-based expectations for bank oversight of AI service providers; and (3) the reason that existing regulation should already address risks arising from explainability, overfitting and dynamic updating, and cybersecurity.

I. *AI Use by Community Banks and Oversight of Third Parties*

Last year, Mastercard submitted a comment letter to the FDIC urging the FDIC to partner with Standard Setting Organizations ("SSOs") that are respected and known in the financial services industry to formalize standards for third parties that provide banks with models that rely on AI, machine learning ("ML"), and big data processing. We also recommended that the FDIC develop a voluntary certification program for the same. We now encourage all of the Agencies to pursue such an approach. By implementing a voluntary certification program for such models, the Agencies would reduce the barriers for many smaller banks, including community banks, to make use of the models. For service providers of AI models to numerous banks, such as Mastercard, doing so also would reduce burdens that result from being the subject of multiple overlapping bank diligence and monitoring processes.

Specifically, model risk management guidance issued by the Board, the OCC, and the FDIC directs banks to evaluate various information in order to validate a third-party's model (the "Guidance").[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 Guidance directs banks to evaluate all the foregoing information in order to validate a third-party's model. Moreover, the Guidance instructs banks to incorporate third-party models into their broader risk management frameworks as they would their own proprietary models.[3] Additionally, the 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 Guidance is substantial.

---

[2] *See* Board, *Supervisory Guidance on Model Risk Management*, SR 11-7 (Apr. 4, 2011) ("Board Guidance"); OCC, *Supervisory Guidance on Model Risk Management*, OCC 2011-12 (Apr. 4, 2011) ("OCC Guidance"); and FDIC, *Supervisory Guidance on Model Risk Management*, FIL-22-2017 (June 7, 2017) ("FDIC Guidance").

[3] *See*, *e.g.*, Board Guidance at 15; OCC Guidance at 15; and FDIC Guidance at 13.

[4] Board Guidance at 16; OCC Guidance at 16; and FDIC Guidance at 14.

In our experience, every bank that uses the services offered by Mastercard that involve AI models requests considerable amounts of information and documentation from Mastercard and undertakes a significant effort in time and cost to comply with this guidance. 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 review; (ii) model monitoring; (iii) model governance; and (iv) model transparency. 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.

By working with existing SSOs that are familiar to banks and third-party providers, the Agencies 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 Guidance. Examples of existing SSOs that are well-regarded within the financial services industry are the Payment Card Industry Security Standards Council and the International Organization for Standards.

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 Agencies have an opportunity to be a catalyst for a "virtuous cycle" of technology innovation that should inure to the benefit of banks, particularly community banks, and their customers.

II. *Best Practices for AI Service Providers*

In this section we discuss industry best practices to control risks arising from data processing and usage, much of which involves having data management and governance when developing and reviewing a model. These best practices are in many ways similar to the governance, policies and controls expectations that the Board, OCC, and FDIC have set forth in the Guidance for banks to manage risk.

As discussed above, Mastercard encourages the Agencies to apply a principles-based approach to setting expectations for bank oversight of AI service providers. As such, the Agencies should expect banks to conduct oversight of third-party providers of AI in a manner that is appropriate, taking into consideration the size and complexity of the third-party providers. Thus, we do not believe that it is necessary to mandate that banks oversee every AI service

provider for these best practices. Rather, we include these concepts as a reference for the Agencies regarding the types of practices that would help AI services providers—and accordingly banks—reduce risk associated with AI models.

The best practices include the following:

- Implement data management, data governance, quality, and taxonomy programs. It is important to implement standards on managing data assets adequately and consistently across an organization and to understand, measure, and monitor data risks and performance as well as any changes in datasets required for use in advanced AI applications. Organizations should implement related tools, including data quality dashboards and data visualization tools, to enable data assessments.

- Implement AI governance. Organizations should develop and implement strong governance around use of AI that aligns organizational values and principles with AI practices. The governance should include focusing on identification and mitigation of data risks, deliberate steps to minimize data bias and prevent differential outcomes, and include appropriate executive oversight. High-level steps which could be part of AI governance include:

    - *Purpose Evaluation.* Intended purpose of AI is properly framed as a business problem and evaluated for alignment with organizational values and principles.

    - *Data & Use Case Evaluation.* Data used in AI is evaluated for availability, quality and compliance, and assessed in the context of its intended use to ensure fitness for purpose.

        - *Understanding how the data was generated*—having a good understanding of data provenance and data lineage is particularly relevant for large enterprises that wish to use large historical data stores to drive data innovation. Data sources and data collection methodologies should be assessed as part of this step.

        - *Assessing data quality and fitness for purpose against the defined use case*—a critical part of the process is to understand if the input data is fit for the purpose, and make sure it is of high quality and representative of the production population and/or context in which it will be applied. This can include conducting exploratory analysis of the data to understand the existing relationships among input data variables which is essential to uncovering potential data bias.

    - *Model Build and Output/Impact Assessment (prior to deployment).* Models are assessed for risk and developed in line with best practices, as outlined in the governance framework, with each model assessed for quality and bias, explainability, driving factors, and potential impact. Models are also peer-

reviewed. Impact assessment and model maintenance and monitoring procedures are established.

- *Soft Launch and Production Monitoring (post-deployment).* Models are deployed to staging and then production environments where they are continuously monitored (*e.g.*, for issues such as dynamic updating as discussed below in Section III.B) with reports prepared and reviewed with frequency and level of reviews commensurate with the level of established model risk.

III. *Other Topics: Explainability, Overfitting, Dynamic Updating, and Cybersecurity*

As a leader in technology in the financial services industry, Mastercard strongly supports innovation that increases access to financial services for consumers and communities through AI and ML. We appreciate the Agencies considering whether to provide regulatory clarity to help facilitate innovation. If the Agencies do so, we encourage the Agencies not to adopt any specific technical requirements or limitations on the development and use of AI and ML. These technologies are in their formative stages and the potential for unintended disruptions can be significant. As discussed below, we believe that existing regulations currently provide strong protections.

Moreover, the Agencies can facilitate innovation in a way that increases access to financial services while mitigating associated risk by supporting the initiative on self-certification discussed in Section I above.

A. Explainability

Challenges exist to understanding AI outputs, which can commonly arise based on the source of the data or the usage permissions provided by the parties that are involved in obtaining the input data. Consequently, as the Agencies acknowledge, explainability is important to a bank's understanding of the conceptual soundness of an AI approach, because explainability requires an understanding of how a system works. However, a frequent concern is that it may not always be appropriate to share or explain detailed inner workings of a particular system. This is particularly true where such an understanding of how a system reaches its decisions could enable its manipulation (such as with fraud models, the goal of which is to detect and prevent fraudulent transactions), would otherwise allow for actors to "game" the system or could lead to the disclosure of proprietary aspects of a model, such as product components and design. We believe that a balance can be struck between transparency and explainability and protecting the integrity of the system and its output.

The Guidance already achieves this balance. We support the concept of providing transparency to banks regarding how third parties manage their respective systems. The Guidance instructs banks to require that third-party model providers explain model inputs, design, intended use, and testing results, as discussed in Section I above. But the Guidance does not require banks to obtain information that could harm system integrity. Accordingly, we do not believe it is necessary for the Agencies to impose further obligations on banks vis-à-vis their third-party service providers of models. If, however, the Agencies believe that specific

requirements are necessary to enhance explainability, we would be willing to provide input on some techniques that could do so.

B. Overfitting and Dynamic Updating

Overfitting is a common problem in data science. In addition to limitations of a specific method, the data used to train the AI model may be limited, resulting in a program that is only as good as the data from which it learns. For instance, examples with past data may not be representative of future data, data may be abstracted and not representative of the actual data, or data may be only collected under punitive situations (*e.g.*, missed payments) or on a self-reported basis. Best practices to prevent overfitting include adequate testing of model performance on never before seen data, with standard procedures. Moreover, because a model must be trained on data that is fit for purpose and representative of the population to which the model will be applied, in most cases models should not be used on populations that differ from the population for which the model was designed. For example, if a model was developed on country-specific data for use in that country, it may not be suitable for use in another country. Changes in underlying data, context, population or region in which the models are applied should trigger ongoing performance review of the model, which may have to be retrained to address the change.

Moreover, the Agencies recognize the risks associated with models drifting over time—dynamic updating. The risks may be further magnified when financial institutions lack the real-world data (*i.e.*, known answers to model outcomes) they can use to evaluate conceptual model soundness at scale. A common practice in the industry is to use a combination of system monitoring and human involvement in systems as a risk mitigant for systems that are subject to dynamic updating. There are varying degrees of human oversight broadly categorized as: (1) human-in-the-loop – involving the most active level of human involvement in which the human retains full control over the decision-making process that is supported by AI's recommendations; (2) human-over-the-loop—involving some human involvement in which the human may have the ability to override AI's outcome or adjust its parameters to arrive to a different outcome; and (3) human-out-of-the-loop—involving no direct human involvement, with AI having full control over the decision-making process, but with human oversight (*e.g.*, fraud modeling).

When it comes to human-out-of-the-loop systems or other systems that involve dynamic updating, there should be continuous monitoring of AI systems and data, as set forth above and commensurate with the level of risk in the systems and data, configured to alert and prompt human reviews according to predefined parameters. The process for monitoring such systems should also involve systematic production and review of monitoring reports, with frequency and level of detail in monitoring reports and their reviews commensurate with the level of risk in the system. Any notable changes in the data or model performance should be observable, should be reviewed, and should be acted on promptly.

Thus, in our experience, the risk mitigants for overfitting and dynamic updating involve testing and ongoing performance reviews, which are part of the information that banks are expected to obtain from third-party providers of AI models under the Guidance, as discussed in Section I above. When complemented by strong internal governance processes and controls, these checks and balances serve to counteract these risks associated with AI. Accordingly, the

Agencies should not impose further obligations on the banks beyond the Guidance to address these risks.

C. Cybersecurity Risk

Cyber criminals continue to view banks as key targets for cybersecurity attacks. The attacks increasingly rely on more sophisticated methods and technologies to penetrate networks. However, the risks posed to AI by cybersecurity attacks are not necessarily different than those posed to businesses more generally.

The Gramm-Leach-Bliley Act ("GLBA"), and its implementing regulations issued by the OCC, Board, FDIC and NCUA, already require banks to implement and maintain an information security program that is appropriate to their size and complexity, the nature and scope of their activities, and the sensitivity of any customer information at issue. Moreover, the general third-party risk management guidance from each of those four Agencies expressly references information security or GLBA compliance as topics for which banks are expected to oversee their service providers.[5] Service providers to banks that are non-bank financial institutions under the GLBA, such as Mastercard, are also directly subject to the same standard as banks under the Federal Trade Commission's Safeguards Rule. Finally, several state privacy laws also require businesses to ensure that they have taken reasonable and appropriate security measures to protect consumer information.

Given the breadth of coverage of these existing laws intended to mitigate the risks associated with cyber attacks, we urge the Agencies not to impose further obligations on banks with respect to their service providers. Further regulation specific to AI is not necessary.

* * *

[5] *See*, *e.g.*, Board, *Guidance on Managing Outsourcing Risk*, SR 13-19 (Dec. 5, 2013) ("Financial institutions have a responsibility to ensure service providers take appropriate measures designed to . . . comply with section 501(b) of the [GLBA]."); OCC, *Third-Party Relationships: Risk Management Guidance*, OCC Bulletin 2013-29 (Oct. 30, 2013) ("Ensure the contract addresses compliance with specific laws . . . including provisions that outline compliance with certain provision of the [GLBA] (including privacy and safeguarding customer information) . . . ."); FDIC, *Guidance for Managing Third-Party Risk*, FIL-44-2008 (June 6, 2008) ("The financial institution's board of directors and senior management should understand the nature of these risks . . . . Transaction risk is the risk arising from problems with service or product delivery. . . . Weak control over technology used in the third-party arrangement may result in threats to security and the integrity of systems and resources."); and NCUA, *Evaluating Third Party Relationships*, Supervisory Letter No. 07-01 (Oct. 2007) ("Typically, at a minimum, third party contracts should address the following . . . [c]ompliance with regulatory requirements (*e.g.*, GLBA, Privacy, BSA, etc.) . . . .").

Mastercard appreciates the opportunity to provide comments to the Request. If there are any questions regarding our comments, please do not hesitate to contact the undersigned at (914) 249-1582 or Tina.Woo@mastercard.com, or our counsel at Sidley Austin LLP in this matter, Stan Boris, at (202) 736-8227.

Sincerely,

Tina Woo
Senior Managing Counsel
Regulatory Affairs

cc: Stanley J. Boris