October 18, 2021

Via www.regulations.gov

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

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

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

RE: Proposed Interagency Guidance on Third-Party Relationships: Risk Management; Docket No. OP-1752 (Board), FDIC RIN 3064-ZA026 (FDIC), Docket ID OCC-2021-0011 (OCC)

Ladies and Gentlemen:

Mastercard International Incorporated ("Mastercard") submits this comment letter to the Board of Governors of the Federal Reserve System ("Board"), the Federal Deposit Insurance Corporation ("FDIC"), and the Office of the Comptroller of the Currency ("OCC" and, together with the Board and the FDIC, the "Agencies") in response to their Proposed Interagency Guidance on Third-Party Relationships: Risk Management (the "Proposal").[1] Mastercard appreciates the opportunity to provide input on the Proposal.

We recognize the importance the Agencies place on banks managing risk associated with third-party service providers ("service providers"). In our comments below, we recommend actions that could be taken by the Agencies to improve the final guidance issued by the Agencies and make the diligence and oversight processes implemented by banks more efficient for themselves and for their service providers.

[1] Proposed Interagency Guidance on Third-Party Relationships: Risk Management, 86 *Fed. Reg.* 38,182 (Bd. Of Governors of the Fed. Reserve Sys., Fed. Deposit Ins. Corp., Office of the Comptroller of the Currency July 19, 2021).

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 has thousands of issuers and acquirers in the United States, and Mastercard is a service provider to all of them. We are familiar with the Agencies' existing third-party risk-management guidance and the ways in which banks interpret the guidance and implement their third-party risk-management practices. We have colleagues dedicated specifically to responding to diligence and monitoring requests from banks. In fact, we have received approximately 17,490 requests from banks in 2021 alone related to the banks' risk management process, such as a bank's third-party questionnaire, evidence of controls, and other risk assessments—many of which are duplicative of each other. We recognize the importance of banks managing their risks and overseeing service providers, and we commend the Agencies for jointly proposing a standardized set of guidance on the topic. However, we believe that the Agencies should modify the Proposal to make it more practical for both banks and service providers, and we offer our comments based on our experience as a service provider to many banks.

Specifically, we have identified a number of topics in the Proposal with respect to which the Agencies should clarify their expectations or alleviate the burdens on banks and service providers. Our comments address: (1) promoting collaboration of banks to meet expectations for managing third-party relationships; (2) promoting reliance on reports, certificates of compliance, and independent audits, and introducing a voluntary self-certification regime for service providers; (3) clarifying expectations for contractual negotiations between banks and service providers; (4) clarifying expectations for bank oversight of subcontractors to service providers ("subcontractors"); and (5) creating special standards that apply to bank oversight of data aggregators.

I. *Collaboration of Banks to Meet Expectations for Managing Third-Party Relationships*

The Proposal would permit banks to "use the services of industry utilities or consortium, including development organizations, consult with other banking organizations, or engage in joint efforts for performing due diligence to meet its established assessment criteria."[2] We applaud the Agencies' inclusion of collaboration as a means for banks to carry out due diligence. To this end, we encourage the Agencies to provide additional information regarding acceptable forms of collaboration and we request that the Agencies expand the discussion of collaboration to cover the ongoing monitoring function in addition to the due diligence function. In particular, it would be helpful if the Agencies incorporated into final guidance the language of FAQ No. 12 of the Frequently Asked Questions issued by the OCC to supplement Bulletin 2013-29[3] ("FAQs"), which provides details regarding the manner in which banks may collaborate and also permits collaboration with respect to both due diligence and ongoing monitoring. For example, FAQ No. 12 helpfully explains that:

> Banks may take advantage of various tools designed to help them evaluate the controls of third-party service providers. In general, these types of tools offer standardized approaches to perform due diligence and ongoing monitoring of third-party service providers by having participating third parties complete common security, privacy, and business resiliency control assessment questionnaires. After third parties complete the questionnaires, the results can be shared with numerous banks and other clients. Collaboration can result in increased negotiating power and lower costs to banks during the contract negotiation phase of the risk management life cycle.[4]

The benefits of collaboration are obvious. From the perspective of the banks, collaboration lowers costs and saves time by making use of economies of scale. This is particularly valuable to smaller banks that may have limited resources. From the perspective of a service provider, collaboration by banks reduces the number of duplicative inquiries from prospective bank customers and frees up resources to be used more productively.

However, banks are unlikely to collaborate in the performance of diligence or ongoing monitoring unless the Agencies more clearly endorse collaboration in the final guidance. The statement in the Proposal that the use of collaboration and external services "does not abrogate the responsibility of . . . management [of a bank] to handle third-party relationships in a safe and sound manner and consistent with applicable laws and regulations"[5] has the effect of discouraging banks from collaborating unless the Agencies accompany the statement with a clear

---

[2] *Id.* at 38,189 (internal footnote omitted).

[3] OCC, *Third-Party Relationships: Frequency Asked Questions to Supplement OCC Bulletin 2013-29*, Bulletin 2020-10 (Mar. 5, 2020).

[4] 86 *Fed. Reg.* at 38,200.

[5] *Id*. at 38,189.

endorsement of reliance on collaborative efforts. FAQ No. 12 includes similar, discouraging language: "[l]ike products and services may, however, present a different level of risk to each bank that uses those products or services, making collaboration a useful tool but insufficient to fully meet the bank's responsibilities . . . ."[6] Based on our experience, we are concerned that banks will read sentences such as the above-quoted ones as creating doubt regarding whether they are in fact permitted to rely upon the results of collaborative arrangements even after they determine that such arrangements are appropriate for their particular risk management needs. The result, we believe, will be banks continuing to undertake their own independent diligence efforts and ongoing monitoring, rather than pursuing collaborative arrangements.

The Agencies should make clear in the final guidance that banks may rely upon collaborative arrangements to meet expectations for due diligence and ongoing oversight of third-party relationships so long as they have concluded that such arrangements are consistent with safe and sound banking practices taking into account their use of the third-party services. Doing so would enable banking organizations to leverage their collective resources in managing third-party relationships, creating an opportunity for banking organizations of all sizes to effectively manage their risk in a more cost effective manner.

II. *Reliance on Reports, Certificates of Compliance, and Independent Audits*

Mastercard supports the Agencies' position in the Proposal that banks may rely on third-party audits or assessments in conducting diligence and performing ongoing monitoring of service providers. For example, the Proposal states that banks may "determine whether the third party's internal audit function independently and effectively tests and reports on the third party's internal controls" and "[c]onsider any conformity assessment or certification by independent third parties related to relevant domestic or international standards."[7] The Agencies should incorporate into the final guidance the more detailed language on this topic from FAQ No. 14, which generally permits banks to rely on reports, certificates of compliance, and independent audits provided by third parties. Moreover, Mastercard requests that the Agencies consider other alternatives on which banks may rely for service provider risk management.

The third-party risk-management obligations imposed currently by the Agencies and that would be required by the Proposal place significant burdens on banks. For example, the Proposal would require banks to evaluate the effectiveness of a service provider's own risk management, including a service provider's policies, processes, and internal controls; understand a service provider's change management processes; and determine whether a service provider's internal audit function independently and effectively tests and reports on its internal controls.[8] The quantity of information and level of analysis that the Proposal would require is extreme for a service provider relationship and more akin to the level of diligence that companies undertake for a significant corporate acquisition. Smaller banks lack the resources to conduct the level of third-party oversight that would be required under the Proposal by themselves. Absent an ability

[6] *Id.* at 38,199.

[7] *Id*. at 38,190.

[8] *See id.* at 38,189-38,191.

to rely on third party audits and assessments, the consequence of adopting the Proposal in its current form would be to create a two tier regime in which large banks are able to engage service providers with ease and smaller banks need to limit their use of service providers to conserve resources. This would lead to a concentration of innovative product offerings (for which technology service providers are essential) in a limited number of larger banks to the detriment of bank customers.

Allowing the use of third-party audits or assessments will help level the playing field within the banking industry. However, the Proposal needs to send a clear message to banks regarding the permissibility of doing so. In this regard, the Agencies should not include in the final guidance language that may discourage banks from using third-party information. For example, the Proposal directs banks to consider "reviewing [SOC] reports and whether these reports contain sufficient information to assess the third party's risk or whether additional scrutiny is required through an assessment or audit by the banking organization or third party at the banking organization's request."[9] SOC reports are widely used, and their purpose is well known in the industry; so long as a bank has the compliance expertise to understand the results set forth in the SOC reports, it should be able to rely on service provider SOC reports without needing to evaluate whether a SOC report is a suitable piece of information to assess a service provider's risk. FAQ No. 14 embodies this concept of banks having the requisite expertise to understand the reports when it advises that "[t]he person reviewing the report, certificate, or audit should have enough experience and expertise to determine whether it sufficiently addresses the risks associated with the third-party relationship."[10]

In the spirit of minimizing the burden on banks in responsible ways, we encourage the Agencies to expressly permit banks to rely on information filed by public companies that is required by law. In particular, filings with the Securities and Exchange Commission (*e.g.*, 10-Ks, 10-Qs, 8-Ks) are likely to contain information of value to banks in conducting due diligence and ongoing monitoring that need not be verified by a bank's own inquiries to a service provider. This strikes us as a simple, reliable, and efficient method for banks to obtain information about service providers.

Finally, we offer some other third-party arrangements that the Agencies should consider permitting banks to rely upon in their risk management efforts—certification using industry standards, third-party audits using industry standards, and examination by the Agencies themselves.

First, we have advocated in other recent comment letters to the Agencies for the Agencies to partner with Standard Setting Organizations ("SSOs") and implement a voluntary certification program for third-parties, and we reiterate those comments in response to the Proposal.[11]

---

[9] *Id.*at 38,190.

[10] *Id*. at 38,200.

[11] *See* our comment letter to the Agencies and the National Credit Union Administration, dated July 1, 2021, in response to the Proposal 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) and our comment letter

Partnering with an SSO that sets standards for common aspects of service providers' businesses on which banks seek information and a voluntary certification program, by which service providers would be able to obtain certification of fulfillment of relevant standards, would make the risk-management processes vastly more efficient and less burdensome, expensive, or susceptible to error. It would also reduce the barriers for many smaller banks, including community banks, to potentially make use of innovative technologies offered by service providers. An SSO driven process would allow the information and the documentation requested of a service provider by banks to be provided a single time to a certification organization, instead of multiple times for each bank that uses the service. Each service provider could then in turn provide its certification to the banks.

By working with existing SSOs that are familiar to banks and service 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. 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 service providers. Also, by lowering the compliance costs for service providers, more service providers would be motivated to develop technology to be used by 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.

If the Agencies are unwilling to permit certification, they could still allow banks to rely upon reports from independent auditors that apply industry standards in conducting audits of service providers. The most common example would be to allow banks to rely upon external audits conducted by firms that apply Generally Accepted Accounting Principles, which are the accounting standard for public companies in the United States and established by an SSO, the Financial Accounting Standards Board. The largest auditors themselves are also separately subject to oversight by Public Company Accounting Oversight Board. Thus, mechanisms are in place to ensure the accuracy of audit reports.

We also encourage the Agencies to permit banks to consider as part of their overall service provider risk management analysis that service providers are subject to examination by the Agencies under the Bank Service Company Act and that larger service providers are generally subject to regular examinations from the Agencies. For Multi-Regional Data Processing Servicers such as Mastercard, banks should be able to use the Report of Examination issued by the Agencies as a factor in their oversight of the service provider.[12]

---

to the FDIC, dated September 22, 2020, in response to the Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services; RIN 3064–ZA18.

[12] We recognize that a service provider may not share its Report of Examination with a bank (or any third party) because Reports of Examination are confidential supervisory information.

III. *Contractual Negotiations*

The Proposal includes a detailed list of contractual provisions and contracting factors (which describe contract provisions) for bank agreements with service providers. While the Agencies have identified many important risk management elements, it is impractical to expect all enumerated provisions and factors to be included in all cases. Further, such an expansive list overemphasizes the role of contractual negotiation and provisions in an effective risk management program. As such, we urge the Agencies to (1) reduce the list of provisions to prioritize those that the Agencies deem to be most important to an effective risk management program, or (2) expressly recognize in the final guidance that banks may enter into contracts that do not include all of the recommended provisions listed in the Proposal. In doing so, the Agencies should adopt in the final guidance the concepts in FAQ No. 5. FAQ No. 5 recognizes that there are circumstances in which banks have limited negotiating power with service providers and sets forth additional steps for banks to take to manage risk.

The Proposal uses language regarding bank contracting obligations that is open to interpretation and in many instances is understood by banks to be prescriptive. By its terms, the Proposal generally does not mandate that banks include particular language in service provider contracts. For example, the Proposal states that a bank "typically considers the following factors, among others, during contract negotiations with a third party . . ."[13] or that a bank should "[c]onfirm that the contract sufficiently addresses" various issues.[14] But, because we routinely negotiate agreements with banks as counterparties, we know that banks often insist on including many terms in agreements on the basis that the Agencies expect banks to have those terms. This approach often is pursued by banks regardless of how disproportionately burdensome or impractical a provision may be from the service provider's point of view.

The Proposal would perpetuate this problem. For example, the Proposal states that a bank should determine whether a contract "[i]ncludes a provision that enables the banking organization to terminate the relationship in a timely manner without prohibitive expense."[15] Banks will read this as a mandate, yet this type of termination-for-convenience provision is inappropriate in many types of agreements, including agreements in which services are customized or situations in which a bank's agreement with a service provider is one facet of a multi-party arrangement.

Another example is the obligation that banks "[p]rovide that the contract requires compliance with laws and regulations . . . ."[16] Although this paragraph of the Proposal later refers to monitoring "the third party's compliance with applicable laws,"[17] we are concerned,

---

[13] 86 *Fed. Reg.* at 38,188.

[14] *Id*. at 38,191.

[15] *Id*. at 38,193.

[16] *Id*. at 38,192.

[17] *Id.*

based on our experience, that banks will interpret this obligation without reference to whether a law is applicable to the services provided to a bank under an agreement with a service provider. We encourage the Agencies to narrow the scope of this obligation so that bank agreements with service providers require service providers to comply with laws and regulations that are applicable to the actual services provided to the bank.

If the Proposal is not revised to address this concern, banks will insist that the Proposal dictates specific contract provisions and each bank will have its own view on what the Agencies require. This will be particularly problematic for network service providers. For a network like Mastercard that has thousands of bank participants, it is impossible to negotiate a bespoke agreement with each bank. Standardized network agreements enable networks to ensure equal treatment of participants and operational protections for all participants, for example, through default rules that take effect in the event of the failure of a participant. Networks like Mastercard need uniform contract terms to operate an efficient, effective, and secure network.

Accordingly, we ask the Agencies to cull the list of specific contract provisions set forth in the final guidance to those that the Agencies consider to be the most important from a third-party risk management perspective. Alternatively, if the Agencies decide it is important to keep the full list of contract provisions, the Agencies should explicitly state that banks do not have to include all provisions in every contract. In either case, the Agencies should incorporate into the final guidance the relevant concepts from FAQ No. 5, which recognizes that there are circumstances in which banks have limited negotiating power with service providers and sets forth additional steps for banks to take to manage risk.

The Agencies assert in the Proposal that an effective third-party risk management program must cover the entire life cycle of a bank's relationship with a service provider and that contracting is only one part of this life cycle. The expansive list of recommended contractual provisions in the Proposal disproportionately inflates the role of contractual negotiations. Streamlining the Proposal's discussion of contractual negotiations would result in the intended balance for banks to manage the life cycle holistically.

IV. *Subcontracting*

The Proposal would require banks to conduct diligence on, and exercise oversight of, subcontractors to service providers. Service providers stand between the banks and the subcontractors in this arrangement and necessarily bear the burden of passing through obligations to the subcontractors that are expected by banks. As with the contractual negotiation issue discussed above, however, the Agencies should recognize that it may be impractical in all situations for service providers to be able to obtain rights for banks vis-à-vis the subcontractors.[18]

[18] Another challenge service providers face with bank oversight of subcontractors is that banks often contractually require consent rights or notice for a service provider's use of a subcontractor. In discussing contractual provisions, the Proposal provides that if a service provider is permitted to use a subcontractor, a contract between a service provider and a bank should "address when and how the third party should notify or seek approval from the banking organization . . . ." 86 *Fed. Reg.* at 38,193. For service providers like Mastercard that work with a large number of banks and a large number of subcontractors, giving each bank a consent right over, or notice of a change of, subcontractor could have adverse effects on the service provider, the bank, and other banks that use the service provider if the service provider is not able to

Thus, we ask that the Agencies acknowledge such limitations and relax the obligations on banks with respect to oversight of service provider subcontractors.

The Proposal states that banks must:

> Evaluate the third party's ability to identify, assess, monitor, and mitigate risks from its use of subcontractors and to provide that the same level of quality and controls exists no matter where the subcontractors' operations reside. Evaluate whether additional risks may arise from the third party's reliance on subcontractors and, as appropriate, conduct similar due diligence on the third party's critical subcontractors . . . .[19]

Conducting "similar" due diligence on subcontractors could require a bank auditing or obtaining information from a subcontractor. However, service providers may lack the leverage to insist on such provisions in their agreements with subcontractors and thus may not be able to facilitate a bank's diligence and oversight of the subcontractor.

As discussed above, FAQ No. 5 recognizes circumstances in which a bank has limited negotiating power and sets forth alternative methods of managing risk. We believe it would be appropriate for the Agencies to also incorporate FAQ No. 5 in the context of diligence and oversight of subcontractors. Given the limitations faced by service providers in connection with their subcontractor relationships, banks and service providers both would stand to benefit from greater flexibility with regard to bank diligence and oversight of subcontractors. For example, banking organizations should be permitted to take into consideration the existing risk management practices of the service provider as a proxy for the banking organization's own risk management practices.

V. *Applicability of Risk Management Practices to Data Aggregators*

Data aggregators serve a distinct role in the financial services ecosystem that distinguishes them from traditional service providers, and the Agencies should modify the Proposal so that the final guidance reflects this distinction. In this regard, FAQ No. 4 is a good starting point, but we offer the additional information below for the Agencies in adopting standards for data aggregators.

As FAQ No. 4 acknowledges, "[a] data aggregator typically acts at the request of and on behalf of a bank's customer without the bank's involvement in the arrangement."[20] FAQ No. 4 also recognizes that "[i]n many cases, banks may not receive a direct service or benefit from [aggregator] arrangements," and that regardless of the structure of the aggregator arrangement, "the level of due diligence and ongoing monitoring should be commensurate with the risk to the

---

efficiently replace subcontractors to keep itself operational. We believe that the Agencies can alleviate this challenge by acknowledging in the final guidance that banks are not required to incorporate a notice or approval provision in all service provider agreements.

[19] 86 *Fed. Reg.* at 38,191.

[20] *Id.* at 38,197.

bank"[21] (which is usually very little risk). As such, banks should not be required to utilize the full set of guidance for risk-management practices as they would with a traditional service provider.

As the Proposal recognizes, a bank typically is not receiving a direct service or financial benefit from a data aggregator.[22] As a result, a data aggregator poses less risk to the bank than the risk posed by traditional service providers. In a traditional service provider arrangement, a bank is dependent upon a service provider to provide some function that the bank would otherwise provide on its own, and a failure of the service provider could represent a business risk to the bank. This is not true for data aggregators because they do not perform essential business functions for the bank; rather, they act on behalf of the bank's customers. Accordingly, bank diligence and oversight of data aggregators should not focus on topics such as performance and disaster recovery. Instead, diligence and oversight should be limited to information security and ensuring that data aggregators have appropriate safeguards to protect the consumer financial information that they handle, as discussed in FAQ No. 4.[23]

The Agencies should not interpret our comment in any way to propose restricting a consumer's right to access financial data.[24] Data aggregators have enabled consumers to exercise this right of access to financial records, and we emphasize the importance of consumers continuing to have such access even if banks do not always have direct arrangements with data aggregators and apply a different third-party risk management standard to data aggregators than they do to traditional service providers.

* * *

Mastercard appreciates the opportunity to provide comments to the Proposal. 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,

[redacted]

Tina Woo
Senior Managing Counsel
Regulatory Affairs

cc: Stanley J. Boris

---

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *See* 12 U.S.C. § 5333.