October 18, 2021

Via Electronic Mail

Ann E. Misback, Secretary
Board of Governors of the Federal Reserve System
20th and Constitution Avenue, NW
Washington, DC 20551
Re: Docket No. OP-1752
Email: regs.comments@federalreserve.gov

James P. Sheesley, Assistant Executive Secretary
Attention: Comments-RIN 3064-ZA26 Legal ESS
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
Re: FDIC RIN 3064-ZA26
Email: comments@FDIC.gov

Chief Counsel's Office
Attention: Comment Processing, Office of the Comptroller of the Currency
400 7th Street, SW
Suite 3E-218
Washington, DC 20219
Re: Docket ID OCC-2021-0011

Re: Proposed Interagency Guidance on Third-Party Relationships

Ms. Misback, Mr. Sheesley, and the Chief Counsel's Office:

The Consumer Bankers Association (CBA)[1] appreciates the opportunity to submit comments in response to the proposed interagency guidance and request for comment[2] (Proposed Guidance) issued by 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) (collectively, the Agencies).

[1] CBA is the only national trade association focused exclusively on retail banking. Established in 1919, the association is a leading voice in the banking industry and Washington, representing members who employ nearly two million Americans, extend roughly $3 trillion in consumer loans, and provide $270 billion in small business loans.
[2] Proposed Interagency Guidance on Third-Party Relationships: Risk Management, 86 Fed. Reg. 38,182 (July 19, 2021).

CBA applauds the decision by the Agencies to harmonize guidance on risk management policies and procedures for third-party relationships. CBA strongly approves of the Agencies' efforts to afford banks flexibility in tailoring their third-party risk management programs to each unique relationship. CBA supports the Agencies' decision to model the Proposed Guidance on the OCC's 2013 guidance. Although Board-supervised and FDIC-supervised institutions may not be as familiar with the OCC's 2013 guidance, that guidance provides the most useful starting point for outlining the obligations of banks with respect to their third-party relationships.

Though harmonization of and flexibility in risk management guidance are helpful and important components of the Proposed Guidance, some changes are necessary. The Agencies should adjust the scope of the final guidance so that it is applicable to third-party relationships related to critical activities, rather than applicable to all third-party relationships, and clarify that whether a third-party relationship is critical or not is a determination made by the bank itself. The Agencies should also specify that fourth-party relationships, customer relationships, and bank-to-bank relationships are not subject to the requirements of ongoing monitoring, due diligence, and contractual requirements under the final guidance. The Agencies should also clarify how existing FAQs from each agency will apply during the transition to the final interagency guidance, and expressly commit to interagency pronouncements for future FAQs. Finally, the Agencies should modernize regulatory third-party risk management guidance beyond the Proposed Guidance by ensuring the final guidance affords banks flexibility in their risk management programs specific to their relationships with data aggregators.

I. Harmonization of Standards across the Agencies is Necessary but Further Regulatory Coordination is Required

The harmonization of risk management standards across the Agencies is necessary and important because it sets uniform risk management standards regardless of regulator, thereby facilitating compliance. Currently, the inconsistencies in the guidance among the Agencies complicates the ability of banking organizations to efficiently and effectively manage risks related to their third-party relationships, particularly in situations where two agencies may have overlapping authority. For example, the Board's 2013 guidance is limited to "service providers," which is defined as "all entities that have entered into a contractual relationship with a financial institution to provide business functions or activities."[3] The OCC's 2020 FAQs, however, applies more expansively to "third-party relationships" which are defined as "any business arrangement between the bank and another entity, *by contract or otherwise*,"[4] a broader pool of entities than covered by the Board's 2013 guidance. The FDIC's 2008 guidance applies to "all entities that have entered into a business relationship with the financial institutions,"[5] but does not specify whether non-contractual relationships are included. These variations in guidance may require a bank to expand its risk management efforts to more third-parties than required by the bank's primary regulator in order to comply with the guidance of a prudential regulator with backup supervisory authority; this adds an additional burden of requiring banks to determine whether there is a discrepancy in the scope

[3] SR Letter 13-19 / CA Letter 13-21, "Guidance on Managing Outsourcing Risk," 1 (Dec. 5, 2013, updated Feb. 26, 2021).
[4] OCC Bulletin, 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29" (Mar. 5, 2020) (emphasis added).
[5] FIL-44-2008, "Guidance for Managing Third-Party Risk" (June 6, 2008).

of applicable guidance from regulators and to implement risk management efforts for third-parties that the bank otherwise would not engage in such efforts for. Harmonization decreases the risk that banks' third-party risk management efforts may be sufficient for one regulator but not for another. The net result of harmonization is that banks have an opportunity to redirect resources from meeting divergent guidelines toward promoting efficiency and benefiting consumers.

While harmonization across the Agencies is important, also integral is coordination between the Agencies and the Consumer Financial Protection Bureau (the Bureau) so that the Bureau does not impose guidance inconsistent with the Agencies' final guidance. The Bureau has not joined the Agencies in this harmonization effort, and although the Bureau is not one of the prudential banking regulators, many banks are subject to the Bureau's compliance bulletins and policy guidance related to banks' business relationships with service providers.[6] Future Bureau guidance could potentially differ from the Agencies' harmonized guidance, which would result in two distinct sets of third-party risk management guidance with which banks would be required to comply. As such, CBA recommends that the Agencies work with the Bureau now and before the Bureau issues any future compliance bulletins or policy guidance related to banks' third-party relationships to ensure uniformity across policies.

II. The Flexibility Generally Reflected in the Proposed Guidance Should Be Incorporated in the Final Guidance

CBA supports the flexibility the Proposed Guidance generally provides for planning, due diligencing, contracting, and implementing and managing risk management efforts for third-party relationships. No two third-party relationships are identical; banks have a variety of relationships with third parties for numerous different purposes, ranging from information technology services to accounting to delivery of support services. Accordingly, no guidance or risk management standards can contemplate all circumstances and environments in which a third-party relationship may exist and need to be properly managed. The final guidance issued by the Agencies must avoid overly prescriptive standards and encourage flexibility. Flexibility is a necessity for allowing the industry to grow and innovate, while simultaneously engaging in meaningful risk management policies tailored to the unique relationships and their unique levels of risk. Overly prescriptive standards would quash the ability to appropriately tailor risk management efforts to reflect the actual relationship between the bank and a third party. This flexible approach aligns with guidance that the Agencies have provided to community banks on conducting due diligence on fintech companies.[7]

The Proposed Guidance appropriately provides examples of sound risk management policies without being prescriptive, but for the sake of clarity the final guidance should go further and explicitly state that the final guidance focuses on general considerations and does not mandate specific risk management actions. The Proposed Guidance lists actions or policies in connection with sound risk management banking organizations "typically" engage in but does not explicitly state a bank "should" engage in a specific action or policy. This importantly provides banks

[6] CFPB Compliance Bulletin and Policy Guidance, 2016-02, Service Providers (Oct. 31, 2016).
[7] OCC Bulletin 2021-40, "Third-Party Relationships: Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks" (Aug. 27, 2021).

flexibility in structuring their risk management efforts based on the size, complexity, and risks of the parties, and the final guidance should include similar language.

Because flexibility in third-party risk management policies is important, the Agencies should avoid including prescriptive language in the final guidance like that found in the OCC's 2020 FAQs. For example, FAQ 10 specifies that "[t]he board (or committees thereof) should approve the policies and procedures to address how critical activities are identified."[8] This language obligates either the board or a committee to approve specific policies and procedures, whereas the day-to-day operations may mean there is a department of the bank better suited to undertaking such approvals. This demonstrates that prescriptive language generally would limit the ability of banks to practically and most efficiently pursue their third-party risk management efforts. To the extent the Agencies decide to include any of the FAQs in the final guidance, the prescriptive language should be edited to adopt the more permissive language found in the Proposed Guidance.

The final guidance should adopt the approach in the Proposed Guidance allowing the board of directors to delegate approval of contracts involving critical activities and oversight of the bank's overall risk management processes to an appropriate committee reporting to the board, but go beyond the Proposed Guidance and FAQ 26 to also allow the board to delegate these responsibilities to senior management an appropriate department within the bank. Due to the volume of third-party relationships banks enter into that may impact a critical activity, it is impractical for the board of directors to oversee each relationship and approve individual contracts. In acknowledgment of the operational reality for many institutions, these responsibilities should be delegable not just to an appropriate committee, as contemplated in the Proposed Guidance, but also to senior management or an appropriate department within the bank to promote further flexibility.

III. The Final Guidance Should Provide Banks with Flexibility to Determine Necessary Risk Management Efforts for Third-Party and Fourth-Party Relationships

CBA agrees with the Agencies that "[n]ot all relationships present the same level of risk to a banking organization,"[9] and encourages the Agencies to reinforce banks' flexibility by adopting an approach which expressly allows banks to evaluate the criticality of a third-party relationship and apply the final guidance to that relationship as appropriate based on the bank's own risk-based program. The final guidance should also recognize that fourth-party risks can be managed through effective third-party risk management. Further, the final guidance should also expressly not extend third-party risk management obligations to bank relationships with customers, which are already excluded from classification as a "third-party business arrangement."[10] The final guidance should also contain language recognizing that relationships with other banks are less risky to banks than other third-party relationships.

The definition of "third-party relationship" under the Proposed Guidance is broad, encompassing both contractual and non-contractual relationship, and as a result the Agencies should state in the

[8] Proposed Interagency Guidance on Third-Party Relationships: Risk Management, 86 Fed. Reg. 38,182, 38,199 (Jul. 19, 2021).
[9] *Id*. at 38,187.
[10] *Id*.

guidance that banks may apply aspects of the final guidance as appropriate based on the bank's determination of the criticality of a third-party relationship and the risks associated with that third-party relationship. The definition of a "third-party relationship" under the Proposed Guidance is "any business arrangement between a banking organization and another entity, by contract or otherwise."[11] The term "business arrangement" is meant to be interpreted broadly.[12] Under this definition, banks would effectively be required to treat every business relationship as a relationship subject to the risk management principles, including non-vendor third parties. The final guidance needs to build on the flexibility the Proposed Guidance affords banks, as the economic and legal realities of these relationships will vary among third parties. To this end, rather than specifying which activities are "critical activities," as the Proposed Guidance does, the final guidance must go further and allow each bank to determine for itself whether an activity performed by a third party is a "critical activity" and then implement aspects of the final guidance as appropriate in the bank's determination. The Proposed Guidance defines "critical activities" as those that are significant bank functions or other activities that could cause a banking organization to face significant risk if the third party fails to meet expectations, that could have significant customer impacts, that require significant investment in resources to implement the third-party relationships and manage the risk, or that could have a major impact on bank operations if the banking organization has to find an alternate third-party or if the outsourced activity has to be brought in-house.[13] However, this definition does not afford a bank sufficient discretion based on its experience in determining whether an activity performed by a third party is a "critical activity." Banks are in the best position to determine the criticality of their third-party relationships and to scale the nature of their risk management activities appropriately. Rather than listing activities that are "critical activities," as the Proposed Guidance does, the final guidance should state that "critical activities" are those that are identified by the bank as "critical" to its significant functions. The final guidance should also acknowledge there may be circumstances in which a bank will not have the bargaining power to contractually impose obligations on a third party to manage risk; in these circumstances, banks should have the discretion to determine whether to proceed with the third-party relationship or not.

CBA also urges the Agencies to abandon the Proposed Guidance's recommendation that banks conduct due diligence on a third party's critical subcontractors, and instead expressly state in the final guidance that banks can address risks posed by fourth parties through their third-party relationship risk management efforts and do not need to due diligence the fourth parties themselves. In many instances, third parties may use subcontractors, but these subcontractors are not in contractual privity with the bank, nor will these subcontractors typically provide banking services to the bank or to the bank's clients. The Proposed Guidance suggests that banks obtain information regarding legally binding arrangements between the third party and sub-contractors and evaluate these contracts.[14] It would be infeasible for banks to evaluate all subcontracting agreements of all third parties with whom banks have relationships. Not all subcontractors of the third party may be relevant to the bank's relationship with that third party. For example, a bank

[11] *Id*. at 38,186.
[12] *Id*. at 38,185. The OCC's 2020 guidance, which is currently in effect and which the Agencies are contemplating incorporating into the final guidance, is similarly broad, providing that a "business arrangement" is synonymous with a "third-party relationship" and can exist even in the absence of a written contract or monetary exchange.
[13] *Id*. at 38,187.
[14] *Id*. at 38,191.

should not be obligated to review a third party's agreement with that third party's janitorial services. The final guidance should state that banks need to only exert risk management controls over fourth parties providing critical banking services, based on the bank's determination of the risk the fourth party poses. The final guidance should also state that any risk arising from critical fourth-party relationships can be managed contractually between the bank and the third party, and that the bank can review the third party's requirements and procedures to ensure that the third party is properly managing fourth-party risk.

Finally, the definition of "third-party relationship" in the final guidance should include an explicit exclusion of customer relationships and a recognition that bank-to-bank relationships are less risky. As noted in the Proposed Guidance, "third-party business arrangements generally exclude a banking organization's customers"[15] and customer relationships do not pose the type of risk to banks that is mitigated through third-party risk management efforts. Additionally, the final guidance should explicitly recognize that relationships between regulated banks pose minimal risk, as all banks are required to follow the final guidance and are already subject to prudential regulation.

IV. The Agencies Must Clarify the Applicability of Currently-Existing FAQs and Issue Future FAQs on an Interagency Basis

CBA requests that the Agencies clarify how future FAQs will be handled. This harmonization effort could be undermined if the Board, the FDIC, and the OCC each are able to issue separate FAQs related to the final guidance; in such instance, three different risk management guidance documents would have been exchanged for three different sets of FAQs interpreting the same guidance. To promote the aim of harmonizing divergent guidance, CBA recommends that the Agencies clarify the applicability of the current FAQs during the interim period between the issuance of final guidance and the issuance of subsequent FAQs, as well as specify that any future FAQs will be issued on an interagency basis with an opportunity for public comment.

V. FAQ 4 on Data Aggregators from the OCC's 2020 FAQs Should Not Be Incorporated into the Final Guidance

Rather than adopting FAQ 4 and defining which data aggregator relationships constitute third-party relationships subject to the final guidance, the final guidance should give banks the discretion to evaluate their relationships with data aggregators and adopt risk management procedures commensurate with the risk associated with a data aggregator, similar to the flexibility a bank should have under the final guidance for its other third-party risk management efforts. FAQ 4 is unclear regarding which entities are data aggregators with whom a bank has a third-party relationship. FAQ 4 states "[a] bank that has a business arrangement with a data aggregator has a third-party relationship," but also provides that "[w]hether a bank has a business arrangement with the data aggregator depends on the level of formality of any arrangements the bank has with the data aggregator for sharing customer-permissioned data."[16] Rather than defining which data aggregator relationships rise to the level of a third-party relationship subject to the guidance, the final guidance should instead acknowledge that banks have flexibility in evaluating data

[15] *Id*. at 38,187.
[16] *Id*. at 38,197.

aggregator relationships and tailoring risk management approaches based on the banks' assessments of each data aggregator relationship's risk.

FAQ 4 in its current form should not be incorporated into the final guidance. If FAQ 4 were incorporated in its current form, banks would be exposed to risk of non-compliance regardless of the level of formality of its relationship with the data aggregator. If a bank were to not have a contractual relationship with a data aggregator, the bank would run the risk of non-compliance because of an alleged lack of sufficient oversight due to failure to have a contractual relationship. Yet if a bank does have a contractual relationship with the data aggregator, the bank is subject to even more obligations related to the third-party risk management. This added friction will disincentivize relationships with data aggregators that benefit consumers. Accordingly, banks should not have a blanket obligation to subject data aggregator relationships to onerous contracting, ongoing monitoring, and due diligence requirements. There may be circumstances in which a bank's ability to impose oversight on data aggregators is limited, such as when a bank is required to share customer data with a data aggregator and lacks the ability to choose whether to engage with that data aggregator. The final guidance should allow banks to manage their relationships with data aggregators based on the banks' own evaluation of and appetite for the risks posed by the data aggregator and should acknowledge that banks can place restrictions on the time, place, or manner of access as part of its third-party risk management efforts for data aggregators in connection with the use of APIs and/or screen scraping.[17] Banks should be empowered to protect consumer data and preserve the safety and soundness of the financial system in circumstances in which a bank has good reason to believe that access or data use may be fraudulent, presents security risks to the consumer or the bank itself, or is beyond what is required for the product or service offered the consumer. Additionally, banks should be empowered to impose periodic reauthorization requirements in order to protect against abuse by data aggregators in situations where a consumer was not able to revoke the original authorization granted to a data aggregator.

Finally, the Agencies should acknowledge in the final guidance that the use of APIs and tokenization by data aggregators is more secure and offers consumers greater protection than screen scraping. The Agencies should encourage institutions to start shifting away from credential-based access or screen scraping data access, and to instead pursue safer and more sound practices, such as APIs and tokenized access.

* * *

Once again, CBA appreciates the efforts by the Agencies to develop a framework based on sound risk management principles. A framework that harmonizes standards and promotes flexibility in the management of distinct third-party relationships and their associated risks will benefit consumers and industry. We thank you for the opportunity to share our comments.

[17] The Bureau is currently in the process of undertaking a Section 1033 rulemaking, which could impact banks' obligations with respect to data aggregators. CBA expresses its hope that such Section 1033 rulemaking by the Bureau is consistent with obligations for banks in the Agencies' final guidance.

Sincerely,

Brian Fritzsche
Assistant Vice President, Regulatory Counsel
Consumer Bankers Association