October 14, 2021

Via E-Mail: regs.comments@occ.treas.gov
Office of the Comptroller of the Currency
Chief Counsel's Office
Attention: Comment Processing
Suite 3E-218
400 7th Street, SW
Washington, DC 20219

Via E-Mail: regs.comments@federalreserve.gov
Ann E. Misback, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, Northwest
Washington, DC 20551

Via E-Mail: comments@FDIC.gov
James P. Sheesley, Assistant Executive Secretary
Attention: Comments/Legal ESS
Federal Deposit Insurance Corporation
550 17th Street, Northwest
Washington, DC 20429

Re: Proposed Interagency Guidance on Third-Party Relationships: Risk Management (the "**Proposed Guidance**" or the **"NPR"**)

I. Background

The Risk Management Association ("**RMA**") appreciates this opportunity to respond to and inform the Proposed Interagency Guidance on Third-Party Relationships. RMA is a member-driven professional association whose sole purpose is to advance the use of sound risk management principles in the financial services industry. RMA helps its members use sound risk principles to improve institutional performance and financial stability, and enhance the risk competency of individuals through information, education, peer-sharing and networking. RMA has approximately 1,700 institutional members, which include banks of all sizes as well as non-bank financial institutions.

One of the most important components of RMA's mission is to provide independent analysis on matters pertaining to risk and capital regulation. In this regard, the comments contained herein are informed by subject matter experts from member institutions of RMA's Operational Risk Council, ERM Council and Third-Party Risk Management Roundtable steering committee.

II. General Observations

RMA agrees with the general premise that the use of third parties can offer banking organizations significant advantages, such as quicker and more efficient access to new technologies, human capital, delivery channels, products, services and markets. In addition, RMA agrees with the principle that the use of third parties by banking organizations does not remove the need for sound risk management practices.

RMA appreciates the agencies' work to harmonize their respective third-party risk management guidelines and is encouraged by the principles-based approach – in part – that the agencies have taken in developing the Proposed Guidance. RMA recommends that the agencies' August 2021 Guidelines for Community Banks to Conduct Due Diligence on Fintechs ("Fintech Guidelines") be incorporated into the Proposed Guidance to the extent not already captured therein as part of the OCC's FAQs (i.e., nos. 16 and 17). If the Fintech Guidelines are not incorporated into the Proposed Guidance, community banks will have multiple guidelines to consider, which defeats the purpose of having a unified approach to third-party risk management.

RMA notes that many banks, particularly larger banking organizations, have very mature third-party risk management programs and may need only minimal revisions to their third-party risk management frameworks to align their respective programs with the Proposed Guidelines. These institutions should be given wide latitude in interpreting the final guidelines as there are very real cost-benefit concerns were they to be required to modify their programs to create alignment with the Proposed Guidelines. The rationale which supports this view is simple: These are the institutions that have demonstrated a proactive, risk-based approach to the development, implementation and administration of their third-party risk management programs, and, accordingly, help to drive leading and best practices at both the practitioner and regulatory levels.

Accordingly, RMA believes that the final guidelines should be principles-based to afford banking organizations the opportunity to take a risk-based approach with respect to their third-party risk management programs in concert with their risk appetite and size, scale and complexity of their businesses. Stated differently, while there may be many common attributes to banks' third-party risk management programs, the Proposed Guidance should not be construed as requiring a common approach leading to convergence.

III. Comments on the Text of Proposed Guidance

RMA has several high-level comments with respect to the Proposed Guidance, supplemented by more specific comments detailed further below. At the outset, RMA believes that the readability and comprehension of the Proposed Guidance would be improved by the addition of a definitions section at the beginning of the Proposed Guidance which could be placed after the Summary. RMA also notes that Appendix B of the OCC's 2013-29 Guidance contained a table of regulatory publications – more than 50 handbooks, bulletins and advisory letters – that provided additional detail on third-party risk management practices relating to specific banking activities which is not being carried forward into the Proposed Guidance. A similar resource would prove to be a great benefit for banking organizations that have less mature third-party risk management programs.

The Proposed Guidance states in several sections that the level of risk, complexity and size of the banking organization and nature of the third-party relationship may be considered by the banking organization. In other areas, the Proposed Guidance appears to be very prescriptive such as "2. Due Diligence and Third-Party Selection." RMA respectfully suggests that the Proposed Guidance be revised such that the entirety of the Proposed Guidance be written and, importantly, interpreted to take a principles-based approach that takes into account the nature of the third-party relationship, the level of risk to which the bank is exposed and the size, scope and complexity of the banking organization. Thus, words used in the Proposed Guidance such as "evaluate," "confirm," and "should" would be interpreted by banking organizations as suggestions (as in the case of the Planning portion of the Proposed Guidance) rather than as mandates or directives as in the case of the Due Diligence section of the Proposed Guidance. Therefore, the Proposed Guidance would be written and interpreted as considerations, rather than mandates, for a third-party risk management program rather than requirements for such a program.

Definition of the Term "Third-Party Relationship"

The Proposed Guidance defines the term "third-party relationship" in the Summary as "***any*** (emphasis added) *business arrangement between a banking organization and another entity, by contract or otherwise.*"[1] RMA respectfully suggests that this definition is overly broad and could lead to the development of third-party risk management programs that are not cost-effective. The use of the word "any" in the definition expressly precludes a bank taking a risk-based approach to its third-party risk management program since the word "any" as used in this context means "all" business arrangements. For example, Merriam-Webster defines the word "any" to mean "every –

[1] Page 18. N.B. Page references are to the OCC's publication of the Proposed Guidance.

used to indicate one selected without restriction." *See* *https://www.merriam-webster.com/dictionary/any*.

Moreover, the phrase "business arrangement between a banking organization and another entity, by contract or otherwise," is not qualified by any materiality standard. As a consequence, all business arrangements are created equal and would be subsumed by the Proposed Guidelines.

Based on the foregoing, RMA respectfully suggests that the definition of the term "third-party relationship" be revised to consider two distinct inquiries: (a) the criticality and scope of the relationship ("Criticality"); and (b) the nature of the risk presented by the use of the third party ("Risk Exposure").

Criticality is best described as a banking organization's inward-facing determination of reliance on a third party, while Risk Exposure refers to a banking organization's assessment of the inherent and residual risks associated with a third-party business arrangement. RMA would note that banking organizations with more mature third-party risk management programs separate the concepts of Criticality and Risk Exposure in their relationship segmentation methodology. RMA concurs with the Proposed Guidance that customer relationships are outside of the scope of a "third-party relationship."

RMA respectfully suggests that the agencies consider defining the term "third-party relationship" as follows:

> A business arrangement between a banking organization and any third party which either (a) performs a critical activity, or (b) poses risks that could significantly affect the banking organization's earnings, capital or reputation; but excludes relationships where the business arrangement between the parties is solely predicated on the bank providing banking services.

Concentration Risk

The Background section of the Proposed Guidance states that "a banking organization may be exposed to concentration risk if it is overly reliant on a particular third-party service provider."[2] RMA respectfully suggests that concentration risk may arise not only through third parties, but also through geographies and fourth parties. Geographic concentrations can arise when a banking organization's internal operations and/or its third and fourth parties are located in the same region or are dependent upon and/or leverage the same power or telecommunications infrastructure.

[2] Page 19.

Fourth-party concentration risk can arise when multiple third parties use the same fourth party.[3] Given the nature and complexity of concentration risk, RMA respectfully suggests that the Proposed Guidance would be enhanced by the recognition that banks address concentration risk in alignment with their existing risk governance frameworks.

Third-Party Relationship Life Cycle

RMA respectfully suggests that Figure 1: "Stages of the Risk Management Life Cycle" be amended to read "Stages of Third-Party Risk Management Life Cycle and Governance Framework" as the life cycle is represented by the direction circle, while the governance framework is evidenced by the triangle.

Due Diligence and Third-Party Selection

RMA agrees that conducting due diligence on third parties before selecting and entering into contracts or relationships is an important risk management activity. RMA believes that the Proposed Guidance would be strengthened by distinguishing between due diligence undertaken incident to third-party selection, i.e., procurement-based due diligence, and the evaluation of the third party's control environment.

The Proposed Guidance provides that a banking organization typically considers certain enumerated factors when conducting due diligence on a third party with whom it may enter into a relationship. RMA appreciates the caveat that the degree of due diligence should be commensurate with the level of risk and complexity of each third-party relationship. However, the individual due diligence items are drafted in a directive or prescriptive manner (e.g., "Review the third-party's overall business strategy;" "Evaluate the third-party's ownership structure;" etc.). RMA believes that the Proposed Guidance can be further clarified by noting that the information considered in the course of due diligence and the weight given to each such type of information will vary depending upon the circumstances.

The Proposed Guidance recognizes that "in some instances, a banking organization may not be able to obtain the desired due diligence information from the third party." RMA believes that the Proposed Guidance would be enhanced by noting that the banking organization may, in such circumstances, evaluate the risks posed by the third party in alignment with the bank's existing risk governance frameworks.

---

[3] *See* https://www.rmahq.org/journal-articles/2021/june/third-party-concentration-risk/?gmssopc=1 for a fuller discussion of concentration risk in the context of third-party risk management.

While RMA supports the use of utilities or consortiums to conduct due diligence, RMA disagrees with the express statement that "(u)se of such external services does not abrogate ***the responsibility of the board of directors to decide*** on matters relating to third-party relationships involving critical activities…" The role of the board of directors is to provide oversight of management and approve policies that outline management's approach to manage a bank's critical activities; it is the role of management to decide on matters relating to third-party relationships involving critical activities.

The Proposed Guidance describes the various factors that a banking organization considers when conducting due diligence such as "a. Strategies and Goals;" "b. Legal and Regulatory Compliance;" "c. Financial Condition;" *et seq.* RMA respectfully suggests that the Proposed Guidance acknowledge that a banking organization may take a risk-based approach to due diligence and recognize that the factors described in the Proposed Guidance may be weighted differently by banking organizations generally and by any individual banking organization when contemplating a specific third-party relationship.

Due Diligence: Strategies and Goals

The first sentence of the Proposed Guidance provides that a banking organization should "***review*** (emphasis added) the third party's overall business strategy and goals to consider how the third party's current and proposed strategic business arrangements (such as mergers, acquisitions, divestitures, partnerships, joint ventures, or joint marketing initiatives) may affect the activity." RMA respectfully suggests that third parties are unlikely to provide information regarding proposed strategic business arrangements due to the non-public nature of such arrangements for public companies; moreover, disclosure regarding such arrangements may be prohibited by confidentiality agreements.

Due Diligence: Reliance on Subcontractors

The Proposed Guidance expressly uses the term "subcontractors," and notes that subcontractors are also referred to as "fourth parties." The term subcontractors is very cumbersome when considered in the context of a given subcontractor's own subcontractors, who may, in turn, have their own subcontractors. For this reason, RMA suggests that the term subcontractors be dispensed with and "fourth parties" be substituted in its stead. As a consequence, fourth parties' subcontractors would be referred to as "fifth parties," and so on. Making this subtle distinction reinforces the concept that a bank may be precluded by contract or circumstances from effectively performing due diligence with respect to any fourth party's subcontractors.

The Proposed Guidance contemplated that a bank should conduct due diligence on a third party's critical subcontractors (i.e., critical fourth parties) similar to the due diligence performed on the

third party in certain instances "such as when additional risk may arise due to concentration-related risk, when the third party outsources significant activities, or when subcontracting poses other material risks." We suggest that the Proposed Guidance be modified to recognize that such due diligence may not be practicable given that the bank would not be in privity of contract with such fourth parties. Accordingly, we recommend that the Proposed Guidance be written to suggest that the focus of a bank's assessment should, instead, be on the third party's own third-party risk management program and the third party's ability to manage its own third parties (i.e., fourth parties).

The Proposed Guidance states that banks should "obtain information regarding legally binding arrangements with subcontractors or other parties to determine whether the third party has indemnified itself, as such arrangements may transfer risks to the banking organization." We note that a bank may be contractually prohibited from obtaining copies of contracts between its third parties and their respective fourth parties, where the contracts between the third party and its respective fourth parties have confidentiality provisions which extend to the terms of such contracts.

Moreover, RMA recommends that the definition of the term "fourth party" be amended to reflect not simply any subcontractor of a third party but reflect risk-based considerations such that fourth parties (for purposes of the final guidelines) be limited to "material fourth parties," which would be determined by whether the fourth party does one or more of the following:

(a) provides material products or services to the third party;
(b) is critical to the third party's ability to deliver products and services to the bank; and/or
(c) exposes the bank to a material threshold of risk as determined by the bank.

In order to determine whether a fourth party is "material," in addition to the factors noted above, consideration should be given as to whether the third party places significant reliance on the fourth party to deliver the applicable product or service and the impact of any disruption on the fourth party's supply of such product or service. This construct will lead to a bank having a more focused and cost-effective assessment program so that banks would only assess a third party's "material" fourth parties rather than all fourth parties.

* * * * *

In conclusion, RMA supports the agencies' goal of harmonizing their respective third-party risk management guidance and believes that the final guidelines should be principles-based to afford banking organizations the opportunity to take a risk-based approach with respect to their third-party risk management programs in concert with their risk appetite and size, scale and complexity

of their businesses. Should there be any questions concerning the comments reflected above, kindly contact Edward J. DeMarco, Jr., Chief Administrative Officer and General Counsel at (215) 446-4052 or edemarco@rmahq.org.

Very truly yours,

Edward J. DeMarco, Jr.

Edward J. DeMarco, Jr.
Chief Administrative Officer
General Counsel