John R. Eckert
Independent Financial Consultant
[redacted]

Kathleen E. Oldenborg
Independent Financial Consultant
[redacted]

October 18, 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
Anne 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 – Request for Comment

Thank you for the opportunity to provide a response to the agencies' invitation to comment on the proposed guidance on managing risks associated with third-party relationships.

Background information about the Authors:

At the release of OCC Bulletin 2013-29: *Third-Party Relationships: Risk Management Guidance*, dated October 30, 2019, Ms. Oldenborg and Mr. Eckert were Directors in the OCC Operational Risk Division.

Ms. Oldenborg retired from the OCC in 2019 as Director for Payment System Risk Policy, having served in various examiner roles over a 20 year period, and 15 years in the financial industry.

She currently provides independent consulting services to risk management firms on payment and operational risk.

Mr. Eckert was the Director of Operational Risk and Core Policy. Upon his retirement from the OCC in June, 2016 after 30 years of service, he continues to be involved with the banking and financial services industry. This included his employment with a large bank third-party risk management oversight team. He currently provide independent consulting services to risk management and audit based firms.

Overview

We are encouraged to observe the agencies' collaborative efforts to advance to the next stage of developing an interagency guidance that will offer a uniform framework with the intent of utilizing sound risk management principles. Managing third-party relationship risk management continues to engage subject matter experts across the financial services industry as we continue to address risk management challenges and develop best practices.

"Section 1. Introduction" provides a beneficial overview of the favorable regulatory viewpoint on the financial institution's reliance on third parties. We strongly encourage the key points provided in this section be incorporated into the final interagency guidance.

Of note, we question the timing of the interagency release of *Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks* (Guide) on August 27, 2021 instead of incorporating the guidelines into this proposed interagency guidance. We are concerned that there may be a potential for creating conflicting guidance between the Guide and the final interagency guidance pertaining to conducting due diligence for financial technology (fintech) companies.

As with the issuance of any supervisory guidance, we recommend the agencies avoid the approach of drafting content that appears to be prescriptive in nature rather than maintaining a princicples based approach. Providing a principles based approach allows financial institutions to craft its third-party relationship risk management program in accordance with its size and complexity and in alignment with its risk appetite. It also provides the benefit of effective resource utilization to reach a desired state of maturity or pursue program enhancements. Our primary concern with the proposed guidance being prescriptive may result in the guidance being utilized as a compliance checklist rather than a risk management framework which can be adopted to all levels of complexity.

General Comments

Structure of Text of Proposed Guidance on Third-Party Relationships - Enhancement and Alignment:

The Table of Contents (TOC) does not identify the "Third-Party Relationship [Risk Management] Life Cycle (TPRM Life Cycle)" section following "Risk Management." We recommend the TOC identify the TPRM Life Cycle as Section IV D and incorporate the stages of the [Third Party Relationship] Risk Management Life Cycle noted in Figure 1.

The proposed text narrative includes "4. Oversight and Accountability" as part of the TPRM Life Cycle section. We recommend the "Oversight and Accountability" section be separated from this secton and incorporated into a "Third-Party Relationship Governance and Risk Management" that is represented by the triangle in Figure 1. The TOC and narrative should be revised to identify the three components of TPRM Governance and Risk Management. To follow the flow of the proposed guidance narrative, we recommend creating a Section IV - F. "Third-Party Relationship Governance and Risk Management" with subsections being 1. Oversight and Accountability, 2. Documentation and Reporting, and 3. Independent Reviews.

By incorporating the Definitions recommendation (noted below) and revising the narrative structure to align to Figure 1: Third-Party Risk Management Life Cycle and Governance and Risk Management Coverage, the recommended structure of "Section IV. Text of the Proposed Guidance on Third-Party Relationships: Risk Management" would be:

Text of Proposed Guidance on Third-Party Relationships: Risk Management

A. Summary (Develop a narrative that incorporates first four paragraphs of Section I. Introduction and blend in the applicable Section IV. A. Summary and B. Background narrative comments.)

B. Definitions (Capture the definitions provided in the body of the proposed guidance as well as incorporate definitions provided from industry comments.)

C. Background

D. Risk Management

E. Third-Party Relationship Life Cycle

    1. Planning

    2. Due Diligence and Third-Party Selection

    3. Contract Negotiation

    4. Ongoing Monitoring

    5. Termination

F. Third-Party Relationship Governance and Risk Management (This section would address the "Triangle" around the Third-Party Relationship Life Cycle.) Develop three sub-sections:

1. Oversight and Accountability
2. Documentation and Reporting
3. Independent Reviews

G. Supervisory Review of Third-Party Relationships: Risk Management Program

Enhancing the Guidance by including Definitions:

The proposed interagency guidance contains narrative descriptions throughout the body of the document. It would be beneficial to incorporate a definitions section at the beginning of the guidance to establish clarity for banking organizations varying in size, complexity, and risk profiles. We suggest the definitions follow the Summary (Section IV. A) in the proposed content structure.

Key terms that should be included in the definitions would be Third-Party Relationship (OCC FAQ #1), Business Arrangement (OCC FAQ #2), Critical Activities, Delivery Channels, Third-Party Assessment Service Companies, Subcontractors (noting the alternative term "Fourth-Party Relationships"), Concentration Risk, Dual Employees, System and Organizational Control (SOC) Reports, and Foreign-Based Third Parties.

Definition of "Third Party Relationship"

Section A. Summary describes a third party relationship as "any business arrangement between a banking organization and another entity, by contract or otherwise". We have observed where this broad definition has been interpreted to develop TPRM programs that strive to manage all third-party relationships in a fairly similar manner. While striving to be inclusive, this broad treatment deflects from the concept of appropriately delegating resources to effectively manage critical and high-risk third-party relationships.

We recommend creating a definition utilizing the description of a third-party relationship from the Summary narrative and incorporate the activity descriptions in footnote 10 along with the information provided in FAQ No. 1 & 2.

To provide a clearer understanding of the proposed guidance application, we recommend the agencies incorporate a statement into the definition that empahsizes the need to appropriately allocate its risk management resources to oversee third parties involved with critical and high-risk activities.

Use of the term "Subcontractors"

The term “subcontractors” has a reference to being similar to “fourth parties.” We have observed the financial services industry has adopted the term “fourth parties” rather than “subcontractors.” From a practice perspective, the financial institution would place its reliance upon the third party’s controls that includes its oversight of its third parties. Considering the breadth of monitoring “fourth-party risk,” we recommend the agencies focus on fourth parties of critical or high-risk third parties that include factors such as being critical to the third party’s operation or have a direct impact on the financial institution’s staff and customers (i.e. access to confidential data). We encourage the agencies to develop sufficiently detailed narrative that will benefit the ongoing challenge of managing “fourth-party” risk.

Refinement to Figure 1: “Stages of the Risk Management Life Cycle”

We are encouraged to see the proposed guidance includes “Figure 1: Stages of the Risk Management Life Cycle.” Shortly after the release of OCC 2013-29, it was noted that the title of the graphic, “Risk Management Lifecycle” lacked any reference to the governance framework (the triangle). We suggest the title be revised to address both the TPRM life cycle and risk governance framework.

Third-Party Relationship Governance and Risk Management

There are three points that we ask the agencies to consider:

- Revising the “Documentation and Reporting” label on the Figure 1: Stages of the Risk Management Lifecycle triangle to “Third-Party Risk Program Management”.

  We encourage the guidance to promote TPRM as an integral component of a financial institution’s enterprise risk management program. TPRM is included as part of risk assessments at the functional (front line unit) and enterprise levels. This goes beyond documentaton and reporting as TPRM is included in conducting business impact analyses, measuring inherent risk levels, evaluating effectiveness of controls, and determining action plans to resolve unacceptable residual risk levels. TPRM is also considered when assessing the impact on the financial institutions customer base and operational resiliance. It also has become a component of key risk and performance indicators for management and board reporting.

  To address the challenge of managing TPRM based on a financial institutions risk and complexity, we recommend the narratives from FAQ No. 6 & 7 be incorporated into the program management narrative.

- Action and Accountability: Clearly defining Board and Management responsibilities.

One of the challenges with the release of OCC 2013-29 was distinguishing the role of the Board of Directors (Board) and management. We encourage the agencies to closely review the Board of Directors and Management narrative in the "Oversight and Accountability section to clearly deliniate responsibilities and recommend including FAQ No. 26 into the scope of the review.

- Independent Reviews: Noting the distinction between Internal Audit and Independent Risk Management.

  The narrative states that:

  > "*Banking organizations typically conduct periodic reviews of the third-party risk management process, particularly when third parties perform critical activities*. *The banking organization's internal auditor or an independent third party may perform the reviews, and senior management confirms the results are reported to the board."*

  We recommend the agencies consider revising the narrative to align with financial institution's ongoing monitoring and internal audit processes. While only specified Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches are required by the *OCC Heightened Standards* to have an Independent Risk Management function, we have observed financial institutions below the standard's threshold adopt an ongoing risk monitoring function that is independent of its business lines.

  The Proposed Guidance narrative is fairly silent on the role of Independent Audit's (IA) coverage of a financial institution's TPRM activities. We recommend the agencies incorporate narrative guidance to address the need for IA to test TPRM program effectiveness including ongoing monitoring activities. This would align the guidance to the "Three Lines of Defense" model.

Other Items for Consideration

- Include an Appendix containing related references similar to OCC 2013-29 Appendix B. This would benefit both financial institution staff and management and the regulators as a "quick reference guide."

- Include a "reminder" in the narrative content or as a footnote in the Summary Section regarding the Interagency Statement on Clarifying the Role of Supervisory Guidance dated September 11, 2018, which included the favorable practice of seeking public comment on supervisory guidance. In practice, we have observed financial institutions of various size and complexity referring to OCC 2013-29 containing "regulatory requirements."

We truly appreciate the opportunity to provide a response to the Proposed Interagency Guidance and are available to provide additional insight to the comments provided or address additional questions.

John R. Eckert
[redacted]

Kathleen E. Oldenborg
[redacted]

Responses to Proposed Guidance Questions	
1. To what extent does the guidance provide sufficient utility, relevance, comprehensiveness, and clarity for banking organizations with different risk profiles and organizational structures? In what areas should the level of detail be increased or reduced? In particular, to what extent is the level of detail in the guidance's examples helpful for banking organizations as they design and evaluate their third-party risk management practices?	Considering Section IV provides the text of the Proposed Interagency Guidance on Third-Party Relationships: Risk Management, it would be beneficial to incorporate the first four paragraphs of <u>Section I. Introduction</u> prior to the <u>Section IV. A. Summary.</u> Refer to comments contained in the response regarding recommended enhancements. One primary item is to develop a separate section on TPRM Program Governance.
2. What other aspects of third-party relationships, if any, should the guidance consider?	The guidance should consider adopting narrative around procurment activities, which have unique features.
3. In what ways, if any, could the proposed description of third-party relationships be clearer?	The Role of the Board of Directors and Management need to be clearly outlined to avoid confusion.
4. To what extent does the discussion of ''business arrangement'' in the proposed guidance provide sufficient clarity to permit banking organizations to identify those arrangements for which the guidance is appropriate? What change or additional	Refer to response comment regarding the Definition of "Third Party Relationship."

Responses to Proposed Guidance Questions	
clarification, if any, would be helpful?	
5. What changes or additional clarification, if any, would be helpful regarding the risks associated with engaging with foreign-based third parties?	Adopt the narrative from OCC 2002-16 or equivalent language from the FRB and FDIC. Suggested incorporating a definition of a foreign-based third party in the comments.
6. How could the proposed guidance better help a banking organization appropriately scale its third-party risk management practices?	The Proposed Guidance needs to be principles based and avoid prescriptive language to allow flexibility for financial institution management to design and implement a TPRM program for the financial institution's size and complexity.
7. In what ways, if any, could the proposed guidance be revised to better address challenges a banking organization may face in negotiating some third-party contracts?	Begin the section narrative with an understanding from the agencies that it realizes the bank will not likely achieve all desired contractual factors. The contract negotiation section provides significant detail to the point of being prescriptive. Would recommend the narrative be revised to provide the conceptual nature of each element and avoid the detailed factors that may be construed as requirements.
8. In what ways could the proposed description of critical activities be clarified or improved?	Incorporate a definition of critical activities in the Proposed Guidance, recognizing that "critical" may differ by institution based on complexity of activity and risk tolerances.
9. What additional information, if any, could the proposed guidance provide for banking organizations to consider when managing risks related to different types of business arrangements with third parties?	Managing risks related to different types of business arrangements requires financial institution management and/or staff to have a sufficient understanding of the business activity and clear guidance on the risk appetite of the institution.
10. What revisions to the proposed guidance, if any, would better assist banking organizations in assessing third-party risk as technologies evolve?	There has been significant advancements in the development of TPRM related applications. Depending on the FI size and complexity, utilizing TPRM based technological applications may be financially beneficial as well as produce more timely and accurate reporting for management and the Board.
11. What additional information, if any, could the proposed guidance provide to banking organizations in managing the risk associated	Any third-party involvement with a customer requires increased monitoring from several risk perspectives. From experience, financial institutions need to develop mechanisms to obtain customer experience feedback (i.e. customer service function and monitoring social media) to

Responses to Proposed Guidance Questions	
with third-party platforms that directly engage with end customers?	identify any emerging issues and be able to take prompt remediation action.
12. What risk management practices do banking organizations find most effective in managing business arrangements in which a third party engages in activities for which there are regulatory compliance requirements? How could the guidance further assist banking organizations in appropriately managing the compliance risks of these business arrangements?	Refer to the comments regarding the need to identify an independent risk monitoring function that includes ongoing compliance monitoring.
13. In what ways, if any, could the discussion of shared due diligence in the proposed guidance provide better clarity to banking organizations regarding third-party due diligence activities?	The Proposed Guidance supports the use of utilities or consortiums to conduct due diligence, which is practiced in the industry. It should be noted that management still needs to make the determination if the shared assessement is sufficient to address the financial institution's specific risks.
14. In what ways, if any, could the proposed guidance further address due diligence options, including those that may be more cost effective? In what ways, if any, could the proposed guidance provide better clarity to banking organizations conducting due diligence, including working with utilities, consortiums, or standard-setting organizations?	It is fully agreed that conducting due diligence on third parties before entering into a third party relationship is an important risk management activity. Based on discussion with industry experts, the Proposed Guidance would benefit from distinguishing between three distinct types of due diligence that are undertaken at different stages of the Lifecycle, namely procurement-based due diligence (fit for purpose, company profile, etc.), sufficient vetting (financial, litigation, sanctions, negative news), and evaluating the strength of third party controls. Of note, we question the ability for a Financial Institution to be able to assess a third party's strategic goals and objectives.
15. How could the proposed guidance be enhanced to provide more clarity on conducting due diligence for subcontractor relationships? To what extent would changing the terms used in explaining matters	Refer to the letter comments.

Responses to Proposed Guidance Questions	
involving subcontractors (for example, fourth parties) enhance the understandability and effectiveness of this proposed guidance? What other practices or principles regarding subcontractors should be addressed in the proposed guidance?	
16. What factors should a banking organization consider in determining the types of subcontracting it is comfortable accepting in a third-party relationship? What additional factors are relevant when the relationship involves a critical activity?	The primary factor is the third party's ability to properly assess its third party's processes and controls and be able to effectively maintain ongoing monitoring.
17. What additional information should the proposed guidance provide regarding a banking organization's assessment of a third party's information security and regarding information security risks involved with engaging a third party?	The inclusion of an Appendix containing references similar to OCC 2013-29 Appendix B would provide beneficial detail on factors to consider when assessing a third party's information security risks.
18. To what extent should the concepts discussed in the OCC's 2020 FAQs be incorporated into the guidance? What would be the best way to incorporate the concepts?	The comment letter specifically identify FAQ's that should be incorporated into the Proposed Guidance. Eadh FAQ should be evaluated to determine if it would provide additional clarity and support to the Proposed Guidance. In some cases, an FAQ may need to remain, but be closely evaluated to avoid inconsistent messaging.