ONTALA PERFORMANCE SOLUTIONS™
REDEFINING THIRD PARTY MANAGEMENT

Third Party Risk Institute™

September 22, 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 (the "**Proposed Guidance**" or the **"NPR"**)

I. Background

Thank you for this opportunity to respond to and inform the Proposed Interagency Guidance on Third-Party Relationships. I am widely recognized subject matter expert.

I am currently President, Ontala Performance Solutions Ltd., a specialized management consultant and have focused solely on third party risk management in the financial services sector for the past 12.5 years and CEO, Third Party Risk Institute Ltd., which is focused on building an international network of third party risk management professionals

I authored "Third Party Risk Management: Driving Enterprise Value" published by RMA and now available in its second edition; created and am faculty for a 10 week eLearning program "Certified Third Party Risk Management Professional (C3PRMP) program, which is accredited for 66 CPE credits by NASBA

I also authored "Third Party Risk Management: A Practical Guide" which will be published by Institute for Internal Auditors later this year; and former Chief Procurement Officer and Head, Third Party Risk Management in three significantly important financial institutions.

I am RMA's subject matter expert. In this capacity, I chair the Steering Committee and facilitate confidential twice-annual Third Party Risk Management Roundtable discussions for third party risk management executives from across the sector. I frequently prepare and record expert talks on third party risk management for RMA's podcast series, and author articles on this topic for The RMA Journal.

In summary, I have been focused entirely on disseminating and strengthening third party risk management practices across the sector for the past 12.5 years.

II. General Observations

Financial institutions will benefit from the agencies' work to harmonize their respective third-party risk management guidelines and encourage adoption of a principles-based approach to third party risk management.

It is notable that effective third party risk management practices enable risk-informed decisions, which are intended to protect customers, shareholders, employees, the sector, and other key stakeholders from harm.

Based on my expertise and experience as a management consultant and former senior level executive in three SIFI's, I am in full agreement that the use of third parties can offer financial institutions significant advantages, such as quick and efficient access to new technologies, expert talent, superior capabilities, cost/benefits, new delivery channels, products, services, and markets. Regulators also have a reasonable expectation that financial institutions maintain accountability for risks associated with the use of third parties. They therefore benefit from guidance for designing and implementing sound risk management practices and providing adequate oversight and risk governance.

Of concern is the recent release (August 2021) of Guidelines for Community Banks to Conduct Due Diligence on Fintechs. There appears to be some misalignment between the content in this Guideline. and the Proposed Interagency Guidance. There is also a high potential for confusion, in part because the OCC's FAQs (nos. 16 1and 17) specifically address third party risk management practices for fintechs.

It should also be noted that many banks, particularly larger banking organizations, have made significant investments over the past decade to mature their third-party risk management program. As a result, they would need to make minimal changes to existing third-party risk management practices to comply with the Proposed Guidelines.

Many financial institutions have successfully demonstrated the effectiveness of existing programs and practices and an ability to successfully manage third party risk throughout the pandemic.

As a result, it is recommended that such institutions are given wide latitude in interpreting the final guidelines because of high costs to modify their programs to ensure full compliance with the Proposed Guidelines, with few benefits.

Accordingly, it is respectfully recommended that the final guidelines avoid taking a prescriptive approach with the use of words such as "must, should, typically". Instead, it is respectfully recommended that Proposed Guidance takes a principles-based that affords regulated entities sufficient latitude to take a risk-based approach for their third-party risk management program, in alignment with their risk appetite, complexity, size, scale, businesses that they are in, and nature of third party relationships,

Taking principles-based approach provides an additional and keeps the door open to an important benefit. It encourages regulated entities to continue to mature and evolve their practices, according to changes in their risk appetite, the threat landscape, and proven/ emerging best practices.

III. Comments on the Text of Proposed Guidance

The Proposed Guidance focuses on activities related to lifecycle management, with little mention of risk oversight. It is respectfully recommended that the Proposed Guidance be revised to recognize the importance of effective governance and risk oversight. Specifically, there are many tools, processes and procedures that must be developed and implemented to enable effective governance and oversight, the domain of enterprise risk management, senior management, and the board.

Here is some examples of methodologies and tools that should be in alignment with enterprise risk management practices and policies, and approved by the Chief Risk Officer

- Third Party Risk Management Framework
- Relationship Segmentation methodology (to determine 1) Criticality of the third party relationship, 2) exposure to Inherent Risks, and 3) impact on revenue in the event of serious outage or material failure)
- Third Party Vetting (financial, litigation, sanctions)
- Required third party Controls
- Third Party Due Diligence (to verify the existence and strength of third party controls)
- Residual Risk Ratings
- Exception Management
- Effective Challenge
- Aggregated Risk Reporting
- Quality Control/Quality Assurance
- Third Party Risk Management Policy

It is noted that risk management and risk oversight professionals rely on regulatory guidance as a reliable reference to guide their work. Because of this, the Proposed Guidance be readily actionable if it included an Introduction, Index, Glossary of Terms, and list of related Guidance. You may also wish

to consider including the lifecycle and governance graphic depicted in OCC 2013-29. It is a simple but comprehensive summary of expected practices.

It is respectfully recommended that the Proposed Guidance allows regulated entities to develop and implement policies and practices that are risk-adjusted according to the criticality of the third party relationship and activity it supports, the type and amount of risk that the third party relationship exposes the regulated entity to, and the impact on customers, revenue, their ability to comply with legal/regulatory requirements, and the sector in the event of a serious outage or material failure.

It is further respectfully recommended that language in the Proposed Guidance be revised to remove prescriptive requirements, replacing these with principles-based language. For example:

A. Summary

Definition "Third Party Relationship"

The Proposed Guidance defines the term "third party relationship," as "***any*** (emphasis added) *business arrangement between a banking organization and another entity, by contract or otherwise*."[1] Based on experience, such a definition is overly broad and may lead to the development or expansion of existing third-party risk management programs to the point that they dilute attention to those relationships that present higher levels of reliance and/or risk. In simple terms, a broad definition will create too much "noise".

Additionally, describing a third party relationship as "business arrangement between a banking organization and another entity, by contract or otherwise," does not have a materiality standard. As a consequence, this description reinforces the potential that firms will move away from risk-adjusting their practices. The inevitable result is a capacity and focus problem, with impaired risk management and oversight over third party relationships where there is high reliance and/or exposure to risk.

Based on my experience working with many regulated entities, the definition of a third party relationship is still somewhat misunderstood. I am therefore respectfully recommending that Proposed Guidance includes the following definition:

"A business arrangement with a between a regulated entity and any third party that performs a critical activity or present risks that could seriously impair the regulated entity's earnings, ability to comply with laws and regulations, and reputation by contract or otherwise. For greater clarity, business arrangements may be with vendors, outsourcers, and other entities providing goods or services, with or without financial remuneration. "

And separately states and clearly communicates the concepts of

[1] Page 18.

1) **Criticality** of the relationship to the regulated entity and/or business segment
2) **Exposure to Risk** according to the type and amount of risk, and
3) **Impact on operational resilience** in the event of serious outage or material failure.

More mature financial institutions achieve this by implementing a Relationship Segmentation methodology to enable risk-adjusted practices to manage and monitor their portfolio of third party relationships.

B. Background

Risk Acceptance

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] According to current practices, regulated entities with more mature practices have determined that they may be exposed to entity, activity, geographic, 4th party, cloud, and systemic concentration risk as a result of its relationships with third parties.

Practice has revealed that concentration risk offers both benefits and risks. In practice, regulated entities should utilize concentration risk information to make risk-informed decisions and treat risk with a wide range of risk oversight and risk mitigation strategies. Most regulated entities with mature third party risk management programs do not create "blanket" limits for their exposure to concentration risk, with the exception of geographic concentration risk. In this regard, many regulated entities have implemented KRIs for geographic concentration risk.

Given the nature and complexity of concentration risk, I am respectfully suggesting that the agencies add risk acceptance to this section in the Proposed Guidance.

C. Risk Management

Third-Party Relationship Life Cycle

I respectfully recommend that the title of Figure 1: "Stages of the Risk Management Life Cycle," be changed to read "Third-Party Risk Management Life Cycle Model and Risk Governance Framework" The Lifecycle Management Model is presented by the chevrons, and the Risk Governance Framework is evidenced by the triangle.

Due Diligence and Third-Party Selection

It is fully agreed that conducting due diligence on third parties before entering into a third party relationship is an important risk management activity. It is recommended that Proposed Guidance

[2] Page 19.

distinguishes between three distinct types of due diligence that are undertaken at different stages of the Lifecycle:
1) Procurement-based due diligence (fit for purpose, company profile, etc.)
2) Third Party Vetting (financial, litigation, sanctions, negative news) and
3) Due diligence to evaluate the strength of third party controls

Further, it is agreed that due diligence should be commensurate with the importance of the relationship to achieving key business strategies, Criticality, and the type and amount of risk that they regulated entity is exposed to as a result of its relationship with the third party.

It is of grave concern that individual due diligence "requirements" are communicated using prescriptive terms, which will be interpreted as directives (e.g., "Review the third party's overall business strategy;" Evaluate the third party's ownership structure;" etc.). It is respectfully recommended that terminology in the Proposed Guidance replaces such prescriptive terminology with to align with the recommended principles-based approach. In this case, prescriptive terminology would be replaced with terms like "consider" and "reflect on".

The Proposed Guidance describes the various factors that a regulated entity may consider when conducting due diligence such as "a. Strategies and Goals;" "b. Legal and Regulatory Compliance;" "c. Financial Condition;" I respectfully suggest that the Proposed Guidance acknowledge that a regulated entity may take a risk-based approach to due diligence. Therefore, the list of due diligence factors may not be relevant to the third party relationship and/or may greatly vary in terms of importance according to the businesses the regulated entity is in, geographies where it operates, the criticality of the relationship, and the types and amount of risk the third party relationship exposes it to.

Additionally, the Proposed Guidance states that regulated entities should "Consider whether third party periodically conducts thorough background checks and confirm that third parties have policies and procedures in place for identifying and removing employees who do not meet minimum background check requirements or are otherwise barred from working in the financial services sectors". Many states prohibit barring and/or removal of employees who fail background checks. I respectfully suggest that this section be amended to include the term "unless prohibited by law".

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." It is recommended that the Proposed Guidance be expanded to note that regulated entities may choose to rely on third party due diligence and reports and accept related risks and relationships.

With respect to Insurance coverages, in practice insurance certificates are usually obtainable, but insurance policies are not. Insurance types and limitations are therefore accessible but the specifics about policy coverages are usually not available. I disagree with this section and respectfully recommend that the Proposed Guidance be amended to reflect what is feasible.

Proposed Guidance states that regulated entities will "obtain information regarding legally binding arrangements with subcontractors or other parties": Legally binding agreements between third parties and material fourth parties are subject to non-disclosure agreements and cannot be obtained. It is respectfully recommended that Proposed Guidance is updated to allow regulated entities to mitigate and accept fourth party risks by way of an agreement with the third party that they accept liability for their fourth parties within the contract agreement with the third party.

It is appreciated that Proposed Guidance supports the use of utilities or consortiums to conduct due diligence, I disagree 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. It is the role of management to decide on matters relating to third party relationships involving critical activities.

a. Strategies and Goals

The Proposed Guidance states that a regulated entity 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." Based on many years of experience and Chief Procurement Officer and Head, Third Party Risk Management, unless there is a long-term, trusted strategic relationship in place that directly engages senior management from the regulated entity and the third party, the third party will not provide confidential, competitive information about their business strategy, strategic business arrangements, particularly those protected by an NDA, and non-public M&A activities.

Subcontractors: Describe as "Material Fourth Parties"

The Proposed Guidance uses the term "subcontractor," and notes that subcontractors are also referred to as "fourth parties." The term subcontractor is confusing, because it is also used to describe temporary employees, contractors to third parties, and so on. For this reason, it is respectfully recommended that the term "subcontractors" be replaced with "fourth parties", with a definition in the Glossary of Terms. As a consequence, critical third parties to material fourth parties would be referred to as "material fifth parties," and so on.

Moreover, it is highly recommended that the concept of "materiality" be introduced in relationship to fourth parties. In practice, regulated entities often rely on legal counsel to define "material" in the context of fourth party relationships. This limits the scope of due diligence to identification of fourth parties that are critical to the third party's ability to identify, assess, manage, and controls their critical third parties – the regulated entity's material fourth parties' and reliably fulfill contractual obligations

It is further noted that regulated entities do not have a contractual relationship with fourth parties. As a result, they are unable to conduct due diligence on fourth parties and beyond. Instead, it is

respectfully recommended that regulated entities evaluate the existence and strength of their critical third parties' risk management capabilities as they apply to their ability to identify, assess, manage, and control third party risk. This approach is feasible and provides a reasonable degree of risk insight into material fourth parties.

It is further respectfully recommended that regulated entities do not attempt to acquire performance data on material fourth parties. In practice it is sufficient to rely on the third party to manage its contractual obligations and service level commitments. It is noted that requesting such information impinges on management of material fourth parties, which may impair regulated entities contractual rights in the event of significant disruptions and/or material failure.

The Proposed Guidance states that a material or significant contract with a third party typically should prohibit assignment, transfer, or subcontracting by the third party of its obligations to another entity without the regulated entity's consent. I disagree with this section because this is not something a third party will agree to, particularly large fintechs widely used across the sector. Even with smaller third parties, they are often not able to reliably execute an obligation to obtain consent to use a new fourth party from all of its clients and are unlikely to agree to this term.

Proposed Guidance states that "The banking organization's materiality thresholds and the third party's procedures for immediately notifying the banking organization whenever service disruptions, security breaches, compliance lapses, enforcement actions, regulatory proceedings, or other events pose a significant risk to the banking organization (for example, financial difficulty, catastrophic events, and significant incidents)." Materiality thresholds are uncommon across the sector. I respectfully recommend amending this section to suggest that regulated entities consider including notification and escalation clauses in agreements with third parties, related to outages, breaches and other disruptive risk incidents. "Immediate" notification is not feasible, so it is suggested that contractual obligations to notify are time bound.

Termination

It is respectfully recommended that the Proposed Guidance be amended to include key elements related to termination assistance that may be considered when entering into a third party relationship, what may be considered in a contractual agreement with respect to orderly exit and managing transition risk when implementing and exiting a third party relationship. I respectfully disagree with the requirement to include the right to terminate a contract without penalty. In practice, introducing a "termination for convenience" clause introduces uncertainty to the third party relationship, which erodes trust and drives higher pricing.

Oversight and Accountability

The regulated entity's board of directors (or a designated board committee) and senior management are responsible for overseeing overall risk management processes. It is respectfully recommended that Proposed Guidance be updated to different between the accountabilities and responsibilities of

the board and senior management and acknowledge the rights of the board of directors to delegate certain responsibilities. Specifically, the board should not be accountable for selecting critical third parties or approving contractual agreements.

From OCC FAQs:

1. Include ability to rely on third party audits and pooled audit reports providing "reports contain sufficient information to assess the third party's controls" (pg. 75 – 76)

2. "Being prepared to address interruptions in delivery (e.g., use multiple payment systems, generators for power, and multiple telecom lines in and out of critical sites)." These actions do not consider cases where a single third party serves entire sector; such an alternative is not feasible. Consider additional verbiage to include "where possible". (pg. 66)

Thank you for inviting comments to the Proposed Interagency Guidance. I really appreciate this opportunity and would be delighted to lend any assistance that you may find helpful or respond to any questions you may have.

Linda Tuck Chapman
CEO Third Party Risk Institute Ltd.
linda@3PRInstitute.com

President Ontala Performance Solutions Ltd.
lindatuckchapman@ontala.com