Federal Banking Agencies Issue Proposed Guidance on Third-Party Risk Management: **Five Things To Know**

On Tuesday, July 13, 2021, the Board of Governors of the Federal Reserve System ("Federal Reserve"), the Office of the Comptroller of the Currency ("OCC"), and the Federal Deposit Insurance Corporation ("FDIC" and, collectively, the "Agencies") invited public comment on proposed interagency guidance on managing risks associated with third-party relationships (the "Proposed Guidance"). By harmonizing for the first time the Agencies' supervisory expectations and guidance on third-party risk management, which has become a significant supervisory priority in recent years, the Proposed Guidance would promote consistency in how the Agencies will assess banking organizations' third-party risk management.

The Proposed Guidance would apply to all banking organizations supervised by the Agencies ("banking organizations"), and would be based upon the OCC's 2013 guidance in this area ("OCC Guidance") subject to a number of changes; a chart highlighting key differences between the Proposed Guidance and the 2013 OCC Guidance is included as an Appendix to this alert. Comments on the Proposed Guidance are due 60 days after publication in the Federal Register.

1 The Proposed Guidance would help harmonize supervisory expectations for how banking organizations manage the risks posed by vendors, fintech partners, and other third parties, largely adopting the approach taken by the OCC since 2013.

Over the past decade, the three Agencies have established similar but not identical supervisory expectations for third-party risk management, creating the potential for inconsistency across the different agencies. By establishing a single interagency framework based largely on the OCC Guidance, with which many banking organizations are already familiar, the Proposed Guidance should help support alignment across the Agencies and alleviate the potential for tension between the OCC and FDIC's supervisory expectations at the bank subsidiary level and the Federal Reserve's enterprise-wide expectations at the bank holding company level.

---

2 The Proposed Guidance would apply broadly to products and services provided by a wide range of third parties, including fintech partners, to banking organizations.

The preamble to the Proposed Guidance notes that competition, innovation in the banking industry, and advances in technology have contributed to banking organizations' increasing reliance on third parties to perform business functions, deliver support services, and facilitate the provision of new and existing products and services. In particular, the Agencies have highlighted both in the Proposed Guidance and accompanying press release the importance of third-party risk management in the context of fintech partnerships; supervisory interest in these partnerships in particular may be a key motivation for the issuance of the Proposed Guidance.

3 The Proposed Guidance would continue the Agencies' existing focus on a risk-based approach to managing third-party risks.

The preamble to the Proposed Guidance notes that the use of third parties may present elevated risks to banking organizations and their customers, and thus banking organizations should employ a risk-based approach to manage these risks and to ensure that third parties operate in a safe and sound manner. For example, the Proposed Guidance would expect banking organizations to provide more rigorous oversight over third-party relationships involving "critical activities" (i.e., significant bank functions that could generate significant risks, costs, or customer or operational impacts for the banking organization). The concept and definition of "critical activities" derive from the OCC Guidance.

4 Like the OCC Guidance, the Proposed Guidance would center on a continuous third-party risk management life cycle.

Under the Proposed Guidance, the key components of the third-party risk management life cycle would be:

- **Planning.** Before entering into a third-party relationship, a banking organization evaluates the risks that would be generated by that relationship and develops a risk management plan for the relationship and associated risks. The Proposed Guidance would outline a number of factors typically considered in this plan, including how the arrangement would align with the banking organization's strategy and whether the financial benefits outweigh the costs.
- **Due Diligence and Third-Party Selection.** After the planning stage but before entering into the third-party relationship, a banking organization conducts due diligence on the relationship to assess the third party's ability to perform the activity as expected, to operate in a safe and sound manner, and to comply with applicable requirements, including laws, regulations, and bank policies. The diligence should be commensurate with the level of risk and complexity involved in the relationship. The Proposed Guidance would list key diligence areas, including the third party's strategies and goals, legal and regulatory compliance, financial condition, risk management, and information security.
- **Contract Negotiation.** Once the banking organization has selected the third party, a banking organization negotiates a contract with the party that meets the needs of the banking organization. The Proposed Guidance would list a wide range of factors that a banking organization typically considers when negotiating with a third party service provider, including the nature and scope of the arrangement, performance measures or benchmarks, the service provider's obligation to provide information and maintain records, the right of the banking organization to audit the service provider, confidentiality, limits on liability, and subcontracting. As applicable, contracts stipulate that the service provider will comply with examinations by the applicable Agency, as the Agencies generally have authority to examine and regulate such activities to the same extent as if the activities were performed by the banking organization itself.

- **Oversight and Accountability.** The banking organization's board of directors and management fulfill their respective roles in overseeing overall risk management processes. For example, the board of directors (or a committee thereof) is responsible for approving related policies and reviewing management reports, while management is responsible for confirming that appropriate due diligence has been conducted on third-party service providers and that the banking organization has appropriate systems of internal controls and compliance management. Additionally, a banking organization typically conducts periodic independent reviews of its third-party risk management program and properly documents and reports on its third-party risk management processes at each stage of the third-party risk management life cycle.
- **Ongoing Monitoring.** After the third-party relationship has been established, a banking organization continually monitors the relationship to ensure that the third party is meeting its obligations and the banking organization's controls are operating effectively. The Proposed Guidance would list key factors that a banking organization typically considers as part of its monitoring activities, including changes to the third party's strategy or financial condition, compliance with applicable law and regulation, and remediation of customer complaints.
- **Termination.** Once a banking organization determines that it intends to terminate a third-party relationship, it is important to transition these services in an efficient manner to another provider, bring the activities in-house, or discontinue offering these services. The Proposed Guidance would outline key factors in planning for the termination of a third-party service provider, which include, as applicable, alternative service providers, risks associated with data management and joint intellectual property, and risks to the banking organization resulting from the third party's failure to meet its obligations.

---

5 Although based on the OCC Guidance, the Proposed Guidance would make certain key changes, including the adoption of less prescriptive language, consistent with the 2021 Final Rule Clarifying the Role of Supervisory Guidance adopted by the Agencies and other federal banking regulators.[1]

Relative to the OCC Guidance, the Proposed Guidance includes a variety of modifications, including important revisions that move away from language that state firms "should" take certain actions or "ensure" certain results. Instead, the Proposed Guidance would list considerations "typically" considered by banking organizations and otherwise would use less prescriptive language throughout. As a result, the Proposed Guidance would increase flexibility for banking organizations in applying the Proposed Guidance in a risk-based manner in practice. Additionally, the Proposed Guidance would incorporate additional topics that have become increasingly important to banking organizations and the Agencies since the OCC Guidance was issued in 2013, such as cybersecurity and data protection. A chart highlighting key differences between the OCC Guidance and the Proposed Guidance is included as an Appendix to this alert.

[1] *See* 12 C.F.R. part 4, Appendix A to Subpart F (OCC); 12 C.F.R. part 262, Appendix A (Federal Reserve); 12 C.F.R. part 302, Appendix A (FDIC).

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Financial Services practice:

Randy Benjenk	+1 202 662 5041	rbenjenk@cov.com
Jeremy Newell	+1 212 841 1296	jnewell@cov.com
Michael Nonaka	+1 202 662 5727	mnonaka@cov.com
Karen Solomon	+1 202 662 5489	ksolomon@cov.com
Andrew Ruben	+1 212 841 1032	aruben@cov.com

Appendix: Comparison of OCC Guidance and Proposed Guidance

Topic	Key Differences Between OCC Guidance and the Proposed Guidance
Scope of Application	• The Proposed Guidance would apply to all insured depository institutions and bank holding companies, not just OCC-supervised institutions. • The Proposed Guidance would maintain a broad definition of "third-party relationship," but also explicitly address a wider range of circumstances, such as relationships with fintech companies and holding companies.
Overall Approach	• The Proposed Guidance would maintain the expectation that banking organizations adopt a risk-based third-party risk management program, but would list factors at each stage of the third-party risk management life cycle that banking organizations "typically" consider, rather than mandate consideration of each factor or certain actions or results through terms like "should" or "ensure." • The Proposed Guidance would be organized according to the same third-party risk management life cycle, but certain headings and requirements would be modified, as discussed below. • The Proposed Guidance would separately include the OCC's 2020 FAQs on Third-Party Relationships as an exhibit, but the finalized guidance may incorporate concepts from these FAQs based on public comment.
Overall Risk Management Expectations	• Like the OCC Guidance, the Proposed Guidance would emphasize that banking organizations should adopt a tailored approach to third-party risk management that is commensurate with the level of risk and complexity of both the third-party relationships and the banking organization's operations. Unlike the OCC Guidance, however, the preamble to the Proposed Guidance explicitly reassures smaller and less complex banking organizations that they are not expected to adopt an approach that would be more appropriate for larger and more complex organizations. To that end, the preamble notes that the Proposed Guidance would be intended to provide risk management "principles" that can be employed as appropriate to the circumstances of each banking organization.

Life Cycle Stage 1: Planning	• The Proposed Guidance would note that greater planning and consideration is typically *warranted*, rather than *necessary*, when planning for a third-party relationship engaging in critical activities. The Proposed Guidance similarly would note that a banking organization's board of directors *may* – but, unlike in the OCC Guidance, is not required to – review and approve plans involving critical activities.
	• The Proposed Guidance would outline a similar set of factors to be considered at this stage, but would state that these factors are "typically considered" rather than "should" be considered.
	• The Proposed Guidance would add one factor to be considered, which is the banking organization's ability to provide adequate oversight and management of the proposed third-party relationship on an ongoing basis. It would also shift two factors that were placed within the first stage of the OCC Guidance's life cycle into the second stage:
	  ○ Assessing the extent to which the activities are subject to specific laws and regulations; and
	  ○ Considering whether the selection of the third party is consistent with the banking organization's broader corporate policies and practices, including its diversity policies and practices.

Life Cycle Stage 2: Due Diligence and Third-Party Selection	• Unlike the OCC Guidance, the Proposed Guidance would state that, where the banking organization cannot obtain the desired diligence information from a third party, it should identify these limitations and evaluate the associated risks to determine if they are acceptable, which may be the case if the third party does not have a long operational history or demonstrated financial performance. This addition may be particularly relevant to partnerships with recently-established fintech companies and other service providers. • Unlike the OCC Guidance, the Proposed Guidance would not require that management present results of due diligence to the board of directors when making recommendations for third-party relationships that involve critical activities. • The Proposed Guidance would permit banking organizations to rely on external services, organizations, or other entities to facilitate due diligence, an approach not discussed in the OCC Guidance. • The Proposed Guidance would list due diligence considerations that are similar to those in the OCC Guidance, but would make several key changes to certain of these considerations, including: ○ ***Legal and Regulatory Compliance.*** The Proposed Guidance would add that the banking organization typically considers the beneficial ownership of the service provider and, as applicable, whether the provider has developed a process for mitigating customer harm. ○ ***Information Security.*** The Proposed Guidance would add that the banking organization typically considers the extent to which the third party uses controls to limit access to the banking organization's data and transactions. ○ ***Reputation.*** The Proposed Guidance would omit diligence relating to the reputation of the third-party service provider and its principals. ○ ***Operational Resilience.*** The Proposed Guidance would specify that diligence relating to the resiliency of the third-party service provider is specific to the service provider's operational resilience, including its technology-related operational resilience. ○ ***Insurance.*** The Proposed Guidance would note that a banking organization typically considers whether the third party has insurance coverage for cybersecurity.
Life Cycle Stage 3: Contract Negotiation	• Like the OCC Guidance, the Proposed Guidance would maintain an expectation that the banking organization's board of directors approve contracts involving critical activities. However, unlike the OCC Guidance, the Proposed Guidance would specify that the board of directors may delegate this responsibility to an appropriate committee of the board. • The Proposed Guidance would add an explicit acknowledgement that banking organizations may gain advantage by negotiating contracts as a group with other users. • The Proposed Guidance would add an expectation that significant third-party contracts not permit assignment, transfer, or subcontracting without the banking organization's consent. • The Proposed Guidance would list contract negotiation considerations that are similar to those in the OCC Guidance, but would make several key changes to certain of these considerations, including: ○ ***Responsibilities for Providing, Receiving, and Retaining Information.*** The Proposed Guidance would add contract requirements that the banking organization can (i) access and protect its data and (ii) specify the type and frequency of management information reports to be received from the third party.

	○ ***Operational Resilience and Business Continuity.*** In addition to retitling this heading from "Business Resumption and Contingency Plans," the Proposed Guidance would also address consideration of whether the contract permits the banking organization to terminate the service without penalty if the third-party service provider cannot provide the services as agreed. ○ ***Insurance.*** The Proposed Guidance would add new language noting that the contract may require third-party service providers to maintain cybersecurity insurance. ○ ***Supervision.*** The Proposed Guidance would expect contracts to stipulate that the performance of activities by external parties for the banking organization is subject to regulatory examination oversight, and that the banking organization may terminate the relationship upon reasonable notice and without penalty as directed by the applicable Agency. The OCC Guidance includes these requirements, but only for OCC-supervised institutions; thus, the change of scope here could have much broader consequences for relationships at the holding company level.
Life Cycle Stage 4: Ongoing Monitoring	• The Proposed Guidance generally would align with the OCC Guidance on this topic, including that neither document requires monitoring to cover particular topics. The Proposed Guidance lists areas that banking organizations "typically consider," in gentle contrast to the OCC Guidance's reference to areas that banking organizations "may" consider. • That said, where the OCC Guidance states that more comprehensive monitoring is *necessary* when the third-party relationship involves critical activities, the Proposed Guidance would state that more comprehensive monitoring is *typically necessary* when the third-party relationship is higher risk, giving banking organizations greater flexibility to determine when more comprehensive monitoring is appropriate. • The Proposed Guidance would list ongoing monitoring considerations that are similar to those in the OCC Guidance, but would add two new key considerations: ○ ***Overall.*** The Proposed Guidance would add that banking organizations evaluate the overall effectiveness of the third-party relationship and the consistency of the relationship with the banking organization's strategic goals. ○ ***Training.*** The Proposed Guidance would add that banking organizations typically monitor the adequacy of relevant training provided to employees of the banking organization and the third party.
Life Cycle Stage 5: Termination	• Unlike the OCC Guidance, the Proposed Guidance would list termination-related considerations that banking organizations *typically* consider, rather than *must* consider. • The Proposed Guidance would list termination considerations that are similar to those in the OCC Guidance, but would add two new key considerations: ○ ***Alternative service providers.*** The Proposed Guidance would add consideration of potential third-party service providers to which the services could be transitioned. ○ ***Broader set of risks.*** The Proposed Guidance would note that banking organizations typically consider the "risks" generated by a third party's inability to meet expectations, rather than only the associated reputation risks under such circumstances.
Oversight and Accountability	The Proposed Guidance would make certain key changes with respect to the oversight and accountability responsibilities of the banking organization. • ***Board of directors.*** Consistent with changes noted above and unlike the OCC Guidance, the Proposed Guidance would not require the board of directors to (i) review and approve management plans for using third parties that involve critical

	activities or (ii) review a summary of due diligence results and management's recommendations to use third parties that involve critical activities. • ***Management.*** The Proposed Guidance would remove the distinction in the OCC Guidance between "senior bank management" and "bank employees who directly manage third-party relationships," and generally would adopt a more high-level, less prescriptive set of expectations for management. For example, rather than requiring senior managers to hold accountable the banking organization employees who manage direct relationships with third parties, the Proposed Guidance would require that management provide "appropriate organizational structures, management, and staffing." • ***Independent reviews.*** The Proposed Guidance and the OCC Guidance provide similar examples of typical third-party risk management independent reviews, except that the Proposed Guidance would remove specific mention of assessing the banking organization's process for identifying and managing risks associated with complex third-party relationships. • ***Documentation and reporting.*** The Proposed Guidance and the OCC Guidance provide similar examples of typical third-party risk management documentation and reporting, except that the Proposed Guidance would include reports from third parties of service disruptions, security breaches, or other events that pose a significant risk to the banking organization. In addition, the Proposed Guidance would replace certain types of reports outlined in the OCC Guidance with the more generalized term "risk assessments."