Published on *The National Law Review* https://natlawreview.com

Interagency Guidance for Bank Risk Management of Third-Party Relationships

Article By:

Blockchain Law at Hunton Andrews Kurth

On June 6, 2023, the Federal Deposit Insurance Corporation ("FDIC"), the Board of Governors of the Federal Reserve System ("FRB") and the Office of the Comptroller of the Currency ("OCC") (collectively, the "Agencies") issued final guidance on managing risks associated with third-party relationships, including relationships with fintechs (the "Final Guidance").[1] Effective as of the June 6, 2023 issuance date, the Final Guidance replaces each of the Agencies' existing guidance on third-party risk management and provides consistency in the Agencies' supervisory approaches.[2] The Final Guidance is directed to all banking organizations supervised by the Agencies and advises such organizations to consider and account for the level of risk, complexity and size of the institution, as well as the nature of the third-party relationship, when conducting sound risk management.

Background and Highlights

On July 19, 2021, the Agencies published proposed guidance for banking organizations on managing risks associated with third-party relationships (the "Proposed Guidance"). The Proposed Guidance was based on the OCC's existing third-party risk

management guidance from 2013[3] and involved changes to reflect the extension of the scope of applicability to banking organizations supervised by all three Agencies. The Proposed Guidance also included as an exhibit the OCC's 2020 FAQs,[4] which were released in March 2020 to clarify the OCC's 2013 guidance and expand to new industry topics and technology developments. The Proposed Guidance provided a risk management framework, which covered various stages in the life cycle of third-party relationships, described in more detail below.

The Final Guidance mirrors the Proposed Guidance in that it is based on the OCC's existing guidance and is also consistent with each Agencies' previously released guidance on third-party relationships. However, the Final Guidance contains additional information and clarifications regarding the increasing growth of relationships between banks and third parties who are either "traditional" service and technology providers or fintechs who are either partnering with or in "banking-as-a-service" relationships with banks. The Final Guidance has implications for banks and fintechs, as discussed further below.

The Final Guidance also emphasizes the required involvement, approval and oversight of the bank's board of directors regarding third-party risk management. The board of directors should oversee third-party risk management, provide clear guidance regarding acceptable risk tolerance, approve relevant board policies and ensure the establishment of appropriate bank procedures and practices. The Final Guidance states that a bank's board of directors should be aware of and, as appropriate, approve contracts involving higher-risk activities. For example, where a third-party relationship involves "critical activities," a bank may present plans to and seek the approval of the board.

The Final Guidance also contains a statement that as "guidance," the Final Guidance does not have the force and effect of law and does not impose new requirements on banks; however, the Final Guidance will inform how the Agencies will engage in supervision of banks' third-party risk management programs.

Overview of Final Guidance

The Final Guidance applies to all third-party relationships, specifically "any business arrangement between a banking organization and another entity, by contract or otherwise."[5] Further, such relationships "may exist despite a lack of a contract or remuneration" and may include "outsourced services, use of independent consultants, referral arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, and joint ventures."[6]

The Final Guidance provides an overview of risk management and explains that not all relationships present the same level of risk, and, therefore, not all relationships require the same level or type of oversight or risk management. Accordingly, a banking organization must tailor risk management practices, commensurate with the banking organization's size, complexity and risk profile and with the nature of the third-party relationship. Similarly, critical activities may require banking organizations to engage in more comprehensive and demanding oversight and management of third-party relationships. **Such critical activities may include activities that may:**

1. cause a banking organization to face substantial risk if the party fails to meet expectations;

2. have significant customer impacts; or

3. have a significant impact on a banking organization's financial condition or operations.

The Agencies incorporated concepts related to critical activities from OCC FAQs 7, 8 and 9, acknowledging that a critical activity may not be considered critical for all banking organizations. Therefore, banking organizations must apply a sound methodology to designate which activities and third-party relationships require more comprehensive oversight compared to others in order to implement effective risk management.

Like the Proposed Guidance, the Agencies reference third-party relationship life cycle in the Final Guidance, acknowledging that effective third-party risk management generally follows a "continuous life cycle for third-party relationships."[7] The Final Guidance emphasizes the importance of utilizing staff with the requisite knowledge and skill in each stage of the risk management life, such staff may include experts, legal counsel and/or external support. The Final Guidance discusses the following stages of the risk management life cycle: Planning; Due Diligence and Third-Party Selection; Contract Negotiation; Ongoing Monitoring; and Termination.

The Final Guidance makes clear that while collaboration with other banks and banking organizations may be beneficial and reduce the burden of due diligence, especially for community banking organizations, such collaboration does not shift the responsibility of banks to manage third-party relationships in a safe and sound manner and in compliance with applicable laws and regulations. Further, consistent with OCC FAQ 5, the Final Guidance acknowledges that a bank may have limited negotiating power in contract negotiations. The Final Guidance clarifies that

relationships with a third party, including the use of a third party's subcontractors (i.e., "4th Party" or "flow-down" due diligence and monitoring), should be evaluated based on the risk the relationship poses and may ultimately require applying mitigating factors in the event the use of subcontractors heightens or adds risks.

Next, the Final Guidance discusses governance issues, including oversight and accountability, independent reviews and documentation and reporting. The Final Guidance incorporates concepts from OCC FAQs 6 and 26, altering the guidance to emphasize that the board's functions of oversight and accountability apply throughout the risk management life cycle rather than at a specific stage.

Finally, the Final Guidance provides a brief overview of each Agencies' supervisory reviews, emphasizing that each Agency will review its supervised banking organizations' risk management of third-party relationships as part of its standard supervisory processes. The Final Guidance provides typical activities conducted by examiners while reviewing third-party risk management. The Final Guidance closes by stating legal authority or corrective measures, including enforcement actions, may be used depending on a party's ability to fulfill its obligations in a safe and sound manner and in compliance with applicable laws and regulations.

Key Developments and Changes

While the Final Guidance is similar to the Proposed Guidance, it also involves key developments and changes. The Final Guidance incorporates various concepts from several OCC FAQs as noted above. The Final Guidance expressly mentions third-party relationships formed with "new or novel structures and features"

such as “fintech companies.”[8] Further, the Final Guidance suggests that “[m]aintaining a complete inventory of all third-party relationships,”[9] and completing periodic risk assessments for each third-party relationship may be supportive of a bank’s determination of whether risks have changed over time and if any updates to such risk management practices are needed.

Unlike the Proposed Guidance, the Final Guidance does not specifically exclude customer relationships from the definition of “business arrangement.” The preamble states that the Agencies implemented such change to reduce ambiguity as “some business relationships may incorporate elements or features of a customer relationship.”[10] The Final Guidance revises the definition of “critical activities,” and eliminates “significant investment” and “significant bank function” from the term to avoid imprecise concepts. The Final Guidance clarifies that the term “foreign-based third-party” does not include a U.S.-based subsidiary of a foreign firm, rather the term refers to a third-party whose servicing operations are located in a foreign country and are subject to the laws and jurisdiction of such foreign country.

The Agencies emphasize that the considerations provided in the Final Guidance are intended to be merely illustrative rather than impose actual requirements and may not be applicable or material to each banking organization or third-party relationship. Further, the Final Guidance refines and distinguishes the board’s responsibilities from management’s responsibilities, while emphasizing that the board has ultimate oversight responsibility to ensure a banking organization operates in a safe and sound manner and complies with applicable laws and regulations.

While the Final Guidance explicitly states that it is intended as guidance and does not have the force and effect of law and nor

does it impose new requirements on banking organizations, it nonetheless will guide the Agencies' supervision of banking organizations' third-party risk management systems going forward. The Agencies further announced that they plan to engage with community banks and develop additional resources to assist "smaller, non-complex community banking organizations" in the future to help these organizations manage relevant third-party risks.[11]

Dissent by Governor Michelle Bowman

FRB Governor Michelle Bowman was the sole dissenting vote on the Final Guidance. In her statement, Governor Bowman stated that unlike the Proposed Guidance, which was supplemented by several implementation aids and tools that provided clear, practical and tailored expectations for small banks, the Final Guidance fails to take comparable measures to mitigate regulatory burden on smaller institutions. Further, Governor Bowman expressed that while the Final Guidance recommends that a sound third-party risk management framework should be tailored according to a bank's level of risk, complexity and size, the Final Guidance, nonetheless, fails to provide the "necessary clarity or supplemental tools to facilitate small bank implementation."[12] Governor Bowman also emphasized the Agencies' failure to articulate a timeline for the promised development of additional resources to assist small, non-complex community banks. Governor Bowman expressed disappointment in the Agencies' failure to make the "upfront investment to reduce confusion and burden on community banks" and further noted that she expects community banks will find the Final Guidance challenging to implement.[13]

Implications for Banks, Fintechs and Bank Technology Vendors

Implications for Banks

- Banks may want to consider whether enhancements to documentation related to third-party risk management would be helpful to formalize or evidence existing processes or procedures. Banks should consider implementing or enhancing their existing inventory of all third-party relationships.
- While most banks already tailor policies and procedures to ensure they reflect a risk-based approach to third-party risk management (even if not formally documented), banks may want to review/update their process for identifying “critical activities” as defined in the Final Guidance.
- The preamble to the Final Guidance clarifies that the intended scope of third-party relationships covered by the Final Guidance is broad, and banks may want to review their current third-party risk management framework and consider whether any changes are needed. For example, the Federal Reserve’s previous guidance on third-party risk management was limited to outsourcing relationships with service providers.
- Smaller banks and community banks should be on the lookout for additional resources from the Agencies intended to assist smaller, non-complex community banks in managing relevant third-party risks.
- Smaller banks and community banks should also consider that entering into more involved fintech partnerships (especially those where the bank will be the issuing bank for products and services marketed and supported by the fintech) will result in complex and costly onboarding and monitoring and oversight for the fintech partners. For example, in many bank-fintech partnerships, the bank is continuously reviewing and approving the fintech’s marketing materials, and has ongoing obligations for any BSA/AML and OFAC components that are

outsourced to the fintech partner.
- With respect to bank-fintech partnerships, it remains to be seen whether the Agencies' Final Guidance and specific "in-scope" coverage of fintech partnerships will result in an increased number of exams of service providers under the Bank Service Company Act, which authorizes the Agencies to regulate and examine the performance of services authorized under the Act provided to banking organizations by third-party service providers.

Implications for Bank Third-Party Vendors and Suppliers

- Third-party vendors and suppliers providing products and services to banks may expect to see modified or expanded due diligence and onboarding requirements, additional or modified contract or agreement terms and additional or modified ongoing monitoring, oversight, auditing and testing required by their bank customers.
- Third-party vendors and suppliers can expect additional requirements regarding their own third-party vendors or suppliers (i.e., "4th party" or "flow-down" due diligence and oversight) as a result of the Final Guidance.

Implications for Bank-Fintech Partnerships

- The Final Guidance explicitly references that partnerships with innovative or new structures and features are "in scope," including those where a bank's fintech partner interacts directly with end customers. While many banks already included existing fintech partners within the framework of the bank's third-party risk management framework, for FDIC and Federal Reserve regulated banks, the Final Guidance provides additional clarification and granularity of requirements that may result in amendments to existing

contracts, changes in the level and nature of bank oversight and required bank approvals, and other components of existing bank-fintech partnerships.

- The Final Guidance did not provide guidance on specific third-party relationships with fintechs, but the preamble to the Final Guidance noted that some relationships are new or novel structures and arrangements that may introduce new or increase existing risks to a bank, including those with interactions directly between the fintech and the bank's customers. Those bank "customers" include customers referred into the bank through marketing and outreach efforts of the fintech.
- Fintechs in particular should read the Final Guidance together with recent enforcement actions and consent orders from the OCC and the FDIC specific to bank-fintech partnerships (for example, the August 2022 OCC consent order with Blue Ridge Bank), as those consent orders highlight areas of emphasis for the regulators examining bank-fintech partnerships, such as BSA/AML and OFAC compliance.
- With respect to BSA/AML and OFAC compliance in particular, this is an ongoing challenge given that the bank is on the regulatory hook for compliance (as the bank is for other applicable regulations like UDAAP/UDAP, Regulation E, etc.), but where the bank has no true "customer-facing" role, and the bank is depending on its fintech partner for customer identification (CIP/KYC) and due diligence procedures, and even monitoring transactions for OFAC screening or other suspicious activities.
- As illustrated by the recent enforcement actions and consent orders referenced above, a bank risks a "matter requiring attention" or potentially even an enforcement action and consent order if the third-party fintech partner does not have a BSA/AML and OFAC compliance program commensurate with

the risks posed by the end customers or bank products. Fintechs should expect additional requirements and monitoring from banks, including a bank requiring third-party independent testing and auditing of the fintech's BSA/AML and OFAC screening processes and performance.
- As a result of a combination of the Final Guidance, recent enforcement actions and consent orders, and some class action claims brought against high-profile fintechs (and their partner banks), fintechs should also expect additional requirements, monitoring, testing and oversight from bank partners on the fintech's Regulation E dispute resolution and investigation procedures regarding alleged fraudulent or unauthorized transactions, as well as more general fintech processes and procedures for handling end customer complaints.

Additional Takeaways and Practical Advice

The Final Guidance illustrates the Agencies' increased focus on relationships between banking organization and third parties, including both traditional service providers and fintechs. Because the Final Guidance generally aligned to the Proposed Guidance, it does not impose significant changes to a banking organization's third-party risk management framework; however, it does provide new considerations and factors for banking organizations to take into account when monitoring and maintaining such third-party relationships. Banking organizations should review the key developments and changes from the Proposed Guidance, as discussed above, and identify any policies or procedures that may need to be updated to meet the expectations outlined in the Final Guidance.

While the Final Guidance specifically applies to banking

organizations, fintechs partnering with banking organizations should review the Final Guidance and should expect banking organizations to follow the guidance in contract negotiations, diligence requests and monitoring procedures. Although community banks should expect additional resources to be released at a later date, they should review the Final Guidance and make any adjustments to their risk management policies as needed and practicable in the meantime.

---

[1] "Interagency Guidance on Third-Party Relationships: Risk Management," 88 FR 37920 (June 6, 2023).

[2] *See* SR Letter 13–19/CA Letter 13-21, "Guidance on Managing Outsourcing Risk" (December 5, 2013, updated February 26, 2021); FIL-44-2008, "Guidance for Managing Third- Party Risk" (June 6, 2008); OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance" and OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29." The OCC also issued foreign based third-party guidance, OCC Bulletin 2002-16, "Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance."

[3] OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance."

[4] OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29."

[5] "Interagency Guidance on Third-Party Relationships: Risk Management," 88 FR 37920 (June 6, 2023) at 37927.

[6] *Id.*

[7] *Id.* at 37928.

[8] *Id.* at 37927.

[9] *Id.*

[10] *Id.* at 37922. *See also* Statement by Jonathan McKernan, Director, FDIC Board of Directors, on Third-Party Risk Management Guidance ("As originally proposed in July 2021, the third-party risk management guidance generally excluded a bank's customer relationships from its scope. This exclusion of customer relationships was consistent with existing guidance at the time. Today's final joint guidance has removed the proposal's exclusion of customer relationships. According to the agencies, this change 'is intended to reduce ambiguity.' In my view, the exclusion's removal itself creates ambiguity. The final guidance is now unclear as to whether or when it applies to arrangements involving depositors, borrowers, or other customers of traditional banking services.").

[11] *Id.* at 37926.

[12] Board of Governors of the Federal Reserve System, Statement on Third Party Risk Management Guidance by Governor Michelle W. Bowman, (June 6, 2023) https://www.federalreserve.gov/newsevents/pressreleases/bowman-statement-20230606.htm.

[13] *Id.*