Office of the Comptroller of the Currency Issues Third-Party Relationship Frequently Asked Questions

On June 7, the Office of the Comptroller of the Currency (OCC) issued a set of frequently asked questions (FAQs)\(^1\) to supplement its 2013 guidance on third-party relationship risk management (Bulletin).\(^2\) The FAQs affirm the Bulletin’s broad applicability while (i) re-emphasizing the need for oversight of third-party relationships to be risk-based and tailored to individual institution needs and (ii) delving into several more detailed compliance questions. Of particular note, the FAQs focus on bank relationships with financial technology (fintech) partners and the ability of banks to collaborate among themselves to manage third-party relationships in line with OCC requirements.

**Overview: Broad Scope and Board Oversight**

The Bulletin broadly defined third-party relationships as “any business arrangement between a bank and another entity, by contract or otherwise” and subjected those third-party relationships that involve “critical activities” to more robust due diligence, monitoring and risk management requirements. Critical activities were defined to include “significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology)” or other activities that generally could (i) cause a bank to face significant risk in third-party failure; (ii) result in significant customer impact; (iii) require significant investment to implement the relationship and manage its risk; and (iv) have a major effect on bank operations if the bank must find an alternate provider of the services.

The FAQs retain this breadth, maintain the differentiation of relationships involving critical activities versus others with lower risk and continue to emphasize the role of a bank’s board in oversight of institution-specific risk management processes. In general, bank management “should conduct in-depth due diligence and ongoing monitoring” in regard to critical activities with the expectation that both diligence and monitoring will be “robust, comprehensive, and appropriately documented.” Where bank management determines activities to be low risk, management is to follow board-established policies and procedures. Banks must periodically update their third-party risk assessments throughout the relationship.

---


Ultimately, “the board is responsible for overseeing the development of an effective third-party risk management process commensurate with the level of risk and complexity of the third-party relationships.” The OCC notes explicitly that “[p]eriodic board reporting is essential to ensure that board responsibilities are fulfilled.”

**Fintech, Marketplace Lending, and Mobile Payments Relationships**

Focusing on bank-fintech relationships, which likely were a key driver for the FAQs, the OCC notes that when “a fintech company performs services or delivers products on behalf of a bank or banks, the relationship meets the definition of a third-party relationship” that should be subject to the bank’s third-party risk management process. Akin to any other third-party service provider, a fintech company arrangement may or may not be considered a critical activity in this regard.

In an important acknowledgement of the diligence challenges banks face from time to time in conducting diligence of third parties, the FAQs also specifically address situations where a bank does not receive sufficient information from a third-party service provider that supports a critical activity. In that situation, the OCC expects a bank board and management to:

- develop appropriate alternative ways to analyze these critical third-party service providers;
- establish risk-mitigating controls;
- prepare to address delivery interruptions;
- make risk-based decisions that despite the lacking information, these critical third-party service providers remain the best service providers available;
- retain appropriate documentation of all efforts to obtain information and related decisions; and
- ensure that contracts meet bank needs.

Addressing another aspect of due diligence, particularly in the fintech space, the FAQs expand on the Bulletin, which directed banks to evaluate the financial condition of third-party service providers. The FAQs note that for “a start-up or less established fintech company, the bank may consider a company’s access to funds, its funding sources, earnings, net cash flow, expected growth, projected borrowing capacity, and other factors that may affect … overall financial stability.” Importantly, the FAQs clarify that the OCC does not require banks to ensure that prospective third parties, including but not limited to fintech entities, meet the bank’s lending criteria. Nonetheless, banks should be careful to differentiate between those relationships that create direct versus indirect credit exposure.

The FAQs also specifically address marketplace lending arrangements with nonbank entities and relationships to facilitate mobile payments. In the marketplace lending context, the FAQs assert that a bank board and its management should understand the relationships among the entities involved and the risks specific to marketplace lending relationships, including reputational, credit, concentration, compliance, market, liquidity and operational risks. Management must also ensure it has proper personnel, processes and systems to monitor and control these risks, including, for example, adequate loan underwriting guidelines and appropriate board-adopted policies that include concentration limits. The FAQs direct banks to work with mobile payment providers “to establish processes for authenticating enrollment of customers’ account information that the customers provide to the mobile payment providers” as mobile payment
environments become more ubiquitous and as customer expectations dictate that transaction accounts as well as credit, debit or prepaid cards issued by banks are able to be used in mobile wallets.

**Collaboration, Outsourcing and Acquiring Information**

In response to industry requests for guidance on cooperative third-party diligence and oversight mechanisms, the FAQs indicate that banks may, subject to antitrust laws, collaborate with other banks “to meet certain expectations, such as performing the due diligence, contract negotiation, and ongoing monitoring responsibilities” required by the OCC. Accordingly, where appropriate, banks may take advantage of tools that offer standardized approaches to perform due diligence on third-party service providers. The FAQs also indicate that collaboration among banks “can result in increased negotiating power and lower costs to banks during the contract negotiation phase of the risk management life cycle.” Furthermore, information-sharing organizations, including the Financial Services Information Sharing and Analysis Center, the U.S. Computer Emergency Readiness Team and InfraGard, provide a means to improve systematic understanding of cyberthreats to both banks and their third-party providers. Notwithstanding this acknowledgement of the benefits of collaboration, the OCC also cautions that (i) customized services do not lend themselves to collaboration, (ii) even generic services may pose different risks for different banks and (iii) banks will always retain responsibility to assess the particular way they use a third-party provider and to tailor their risk management processes accordingly.

Banks may also obtain access to interagency technology service providers’ (TSP) reports of examination from the OCC, subject to certain limitations. Specifically, TSP reports will be made available only to banks with existing contractual relationships with the TSP at the time of examination. While the OCC has long indicated that examination reports are available only to the TSP’s actual bank clients, the restriction that contracted parties cannot get access to the most recent pre-contract examination will put banks at a disadvantage early in their relationships with TSPs.

Finally, the FAQs provide express authority for banks to outsource “some or all” of their compliance management systems to third parties, provided they “monitor and ensure that third parties comply with current and subsequent changes to consumer laws and regulations.” Banks may further rely on a third party’s Service Organization Control report prepared in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No. 18 (SSAE 18). The SSAE 18 report may be particularly useful to banks because it addresses whether the third party effectively oversees its own subcontractors or “fourth parties,” an area of increasing focus among the banking agencies.

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work or

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joel D. Feinberg</td>
<td><a href="mailto:jfeinberg@sidley.com">jfeinberg@sidley.com</a></td>
<td>+1 202 736 8473</td>
</tr>
<tr>
<td>David E. Teitelbaum</td>
<td><a href="mailto:dteitelbaum@sidley.com">dteitelbaum@sidley.com</a></td>
<td>+1 202 736 8683</td>
</tr>
<tr>
<td>John K. Van De Weert</td>
<td><a href="mailto:jvandeweert@sidley.com">jvandeweert@sidley.com</a></td>
<td>+1 202 736 8094</td>
</tr>
<tr>
<td>David A. Miller</td>
<td><a href="mailto:david.miller@sidley.com">david.miller@sidley.com</a></td>
<td>+1 202 736 8336</td>
</tr>
</tbody>
</table>
Sidley Banking and Financial Services Practice

The Banking and Financial Services Practice group offers counseling, transaction and litigation services to domestic and non-U.S. financial institutions and their holding companies, as well as securities, insurance, finance, mortgage and diversified companies that provide financial services. We also represent all sectors of the payments industry, including payment networks and processors, money transmitters, and payers and payees in various systems. We represent financial services clients before the U.S. Department of the Treasury, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau and state regulatory agencies, as well as financial services regulators in other jurisdictions where we have offices. In addition, we represent clients before the United States Supreme Court, other federal courts and state courts.

To receive Sidley Updates, please subscribe at www.sidley.com/subscribe.