November 21, 2013

OCC Issues New Third-Party Risk Management Guidance

By Rick Fischer, Andrew M. Smith and Ryan H. Rogers

On October 30, 2013, the Office of the Comptroller of the Currency (OCC) issued new guidance on risks presented by third-party relationships, entitled "Third-Party Relationships: Risk Management Guidance" ("2013 Bulletin"). In the 2013 Bulletin, the OCC expresses its concern that the quality of bank risk management practices has not kept pace with the complexity of third-party relationships. According to the OCC, banks are expected to engage in "more comprehensive and rigorous oversight and management" of third-party relationships, particularly where the third party is involved with "critical activities."

The 2013 Bulletin rescinds earlier OCC guidance issued in 2001, entitled "Third-Party Relationships: Risk Management Principles" ("2001 Bulletin").[1] Notably, the 2013 Bulletin provides considerably more detail than the 2001 Bulletin on the OCC's expectations for bank contractual relationships with, and oversight responsibilities for, third parties. The OCC's new third-party guidance is a strong signal of the increased regulatory scrutiny that banks will encounter in their use of third parties as service providers.

This alert highlights differences between the 2013 Bulletin and the 2001 Bulletin.

"Critical Activities" versus "Material Relationships"

The 2013 Bulletin makes clear the OCC's regulatory expectation that banks will focus additional resources on third-party relationships that involve "critical activities." According to the 2013 Bulletin, critical activities include significant bank functions such as payment, clearing, settlement and custody functions, as well as "significant shared services" such as information technology. Critical activities also include any activities that could have "significant customer impacts."

For third-party relationships that are likely to involve critical activities, the OCC expects banks to conduct "extensive due diligence" before entering into the relationship. The 2013 Bulletin also states that the bank's board of directors should approve any contract that will involve critical activities prior to execution. And, for existing or future third-party relationships that may not presently involve critical activities, the OCC makes clear that the bank's senior management is responsible for "periodically" assessing the relationships to determine whether the third party's activities have become a critical activity. Under the guidance, senior management also is responsible for ensuring that periodic

[1] The 2013 Bulletin also rescinded an OCC advisory letter issued in 2000, entitled "Third-Party Risk," that primarily addressed credit-related activities arranged through third parties, including factoring arrangements, vendor-sponsored "credit repair" products and syndicated loan participation.

"independent reviews" are conducted on the third-party risk management process when a bank involves third parties in critical activities.

The 2001 Bulletin did not provide definitive guidance on the types of third-party relationships that could be subject to heightened scrutiny during the examination process or that otherwise warranted the allocation of particular bank resources. Instead, the 2001 Bulletin stated only that examiners will "review the risks associated with all material third-party relationships and activities together with other bank risks using the supervision-by-risk framework." Although the 2001 Bulletin referred to "critical services" and "significant vendors" that are critical to the bank's operation, it did so in the context of monitoring and documenting third-party relationships. Even in these instances, the standard for determining whether a contractual relationship was "material" focused on the expenditure of bank funds under the contract and whether that amount was "substantial."

As a result, the 2013 Bulletin provides clearer guidance on how to approach third-party relationships that involve activities that may be viewed by the OCC as critical to bank operations.

Notable Changes

In General. The 2001 Bulletin was structured around a five-part "risk management process" focusing on: (1) risk assessment and strategic planning; (2) selecting a third party and due diligence; (3) contract issues; (4) oversight of third-party relationships; and (5) documentation. Although the 2013 Bulletin retains the substance of these five risk areas, it is based on an eight-part "risk management life cycle." Under the "life cycle" approach, the OCC has significantly expanded the guidance provided in the 2001 Bulletin, while also addressing additional topics not discussed in the earlier guidance.

Due Diligence in Third-Party Selection. The 2013 Bulletin provides significantly more detailed guidance on the due diligence required before entering into a third-party contractual relationship. In addition to covering the 11 due diligence touch points in the 2001 Bulletin, the 2013 Bulletin addresses the following additional due diligence requirements:

- **Fee and Incentive Structures.** Banks should evaluate the third party's fee structure and incentives to determine whether they create burdensome upfront fees, or result in inappropriate risk taking, by either the third party or the bank.
- **Compliance with Law.** Banks should evaluate the third party's legal and regulatory compliance program to confirm that the third party has the necessary licenses to operate and to verify its compliance with applicable regulations.
- **Incident Reporting and Employee Management.** Banks should review and assess the third party's incident reporting and management procedures for lines of accountability, and ensure that processes are clearly documented. The third party should have a program in place to train and hold employees accountable for compliance with policies and procedures.

Contract Negotiation. The guidance provided in the 2013 Bulletin regarding the topics that should be addressed as part of third-party contract negotiations is substantially similar to the guidance in the 2001 Bulletin. However, the OCC has added two new areas of focus for contract negotiation—responsibility for compliance with applicable law and the use of subcontractors. On the latter topic, the 2013 Bulletin states that contracts should include provisions that: (1) provide for notification of intent to use a subcontractor; (2) specify the activities that cannot be subcontracted; (3) address reporting requirements (e.g., conformance with performance measures and audit results); and (4) assign liability to the third party for activities or actions by its subcontractors.

Oversight and Accountability Functions. The 2013 Bulletin provides detailed guidance on the roles and responsibilities of the bank's board of directors, senior management and employees who directly manage third-party relationships.

- **Board of Directors.** A bank's board of directors is responsible for: (1) ensuring that effective processes are in place to manage risks; (2) approving risk-based policies governing third-party risk management; (3) reviewing and approving plans for using third parties for critical activities; (4) reviewing due diligence summaries; and (5) ensuring that any management issues revealed by ongoing monitoring are remedied.

- **Senior Bank Management.** The responsibilities of senior bank management include: (1) implementing and managing the risk management process; (2) establishing policies and procedures for governing the process and for identifying third-party engagements that involve critical activities; and (3) reviewing and overseeing third-party relationships generally.

- **Bank Employees Who Directly Manage Third-Party Relationships.** These bank employees must perform specific tasks to ensure third-party compliance, including: (1) conducting due diligence; (2) ensuring compliance with recordkeeping and reporting requirements; (3) escalating issues as necessary; and (4) maintaining appropriate documentation throughout the risk management life cycle.

The OCC has made it clear that it intends to exert its oversight authority more aggressively over banks and third parties with which they have relationships. As a result, it is important for banks to have appropriate policies and procedures sufficient to satisfy the OCC's 2013 guidance, especially in connection with critical activities.

Resources:

The 2013 Bulletin is accessible at http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

The 2001 Bulletin, which has been rescinded by the OCC, is accessible at http://www.occ.gov/static/news-issuances/bulletins/rescinded/bulletin-2001-47.pdf.

Contact:

Rick Fischer
(202) 887-1566
lfischer@mofo.com

Andrew M. Smith
(202) 887-1558
andrewsmith@mofo.com

Ryan H. Rogers
(202) 778-1507
rrogers@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 10 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.