Special Alert: OCC Issues Supplement to Third-Party Oversight Guidance, Emphasizes Bank Responsibilities in Managing Risks in Fintech Relationships

On June 7, 2017, the Office of the Comptroller of the Currency (OCC) issued Bulletin 2017-21 as a supplement to Bulletin 2013-29, the OCC's 2013 risk management guidance related to third-party relationships. The OCC's latest release answers 14 frequently asked questions (FAQs) and marks the second supplement issued this year to Bulletin 2013-29. Previously, on January 24, 2017, the OCC issued Bulletin 2017-7 to advise national banks, federal savings associations, and technology service providers of examination procedures the OCC would follow during supervisory examinations.

As previously summarized in Buckley Sandler's Special Alert, Bulletin 2013-29 requires banks and federal savings associations (collectively "banks") to provide comprehensive oversight of third parties, and warns that failure to have in place an effective risk management process commensurate with the risk and complexity of a bank's third-party relationships "may be an unsafe and unsound banking practice." Bulletin 2013-29 outlined a "life cycle" approach and provided detailed descriptions of steps that a bank should consider taking at five important stages of third-party relationships: (i) planning; (ii) due diligence and third-party selection; (iii) contract negotiation; (iv) ongoing monitoring; and (v) termination. Consistent with the life cycle approach established in Bulletin 2013-29, the examination procedures set forth in Bulletin 2017-7 identify steps examiners should take in requesting information relevant to assessing the banks' third-party relationship risk management at each phase of the life cycle.

The FAQs in Bulletin 2017-21 address three general themes: (i) interpretations of Bulletin 2013-29's scope and content, including applicability to bank relationships with fintech companies and marketplace lenders; (ii) opportunities for banks to collaborate with each other to manage third-party relationship risks; and (iii) outside resources that banks may use to augment their third-party risk management capabilities.

Focus on Fintech

The OCC begins the FAQs by reiterating the broad reach of Bulletin 2013-29 and its application to "any business arrangement between the bank and another entity, by contract or otherwise." Special emphasis is placed on fintech companies that perform services or deliver products on a bank's behalf, and may be

performing "critical activities[1]" as defined in Bulletin 2013-29. While Bulletin 2017-21 does not definitively categorize all fintech activities as "critical," the OCC does restate its long-standing expectation that bank management will conduct in-depth due diligence and ongoing monitoring of third-party service providers that support critical activities. In this regard, "[t]he OCC realizes that although banks may want in-depth information, they may not receive all the information they seek on each critical third-party service provider, particularly from new companies." In these situations, the OCC expects the banks to: (i) develop appropriate alternative ways to analyze these critical third-party service providers; (ii) establish risk-mitigating controls; (iii) be prepared to address interruptions in delivery (for example, use multiple payment systems, generators for power, and multiple telecommunications lines in and out of critical sites); (iv) make risk-based decisions that these critical third-party service providers are the best service providers available to the bank despite the fact that the bank cannot acquire all the information it wants; (v) retain appropriate documentation of all their efforts to obtain information and related decisions; and (vi) ensure that contracts meet the bank's needs.

As a corollary to the comprehensive and rigorous management of third-party relationships that involve critical activities, the OCC clarifies that "[n]ot all third-party relationships present the same level of risk." Picking up on a theme that the Consumer Financial Protection Bureau (CFPB) highlighted last October in its revised service provider guidance, the OCC states "[t]he goal is for the bank's risk management practices for each relationship to be commensurate with the level of risk and complexity of the third-party relationship." Relatedly, the OCC reiterates a core tenet of Bulletin 2013-29 that "[t]here is no one way for banks to structure their third-party risk management process."

In addition to other fintech-related inquiries the FAQs address, including expectations related to performing adequate financial assessments of start-up companies and leveraging fintech relationships to meet the needs of the underbanked or underserved segments of the population, the OCC provides its view on bank responsibilities related to marketplace lending arrangements with nonbank entities, which has been a special focus of the agency in recent years.[2] Although the OCC's discussion of risks and mitigants is not as detailed as the FDIC's Proposed Guidance for Third-Party Lending issued last July, the OCC strikes themes common to the FDIC proposal. The bulletin notes specific risks associated with bank partnership arrangements, such as reputation, credit, compliance, liquidity, and operations, and concludes that banks should adopt "appropriate policies, inclusive of concentration limitations" and conduct sufficient due diligence before beginning a relationship with a marketplace lender. The bulletin

[1] Bulletin 2013-29 defines as "critical" any activities involving significant bank functions (payments, clearing, settlements, and contingency planning); significant shared services (information technology); or other activities that (i) could cause a bank to face significant risk as a result of third-party failures, (ii) could have significant customer impacts, (iii) involve relationships that require significant investments in resources to implement and manage, and (iv) could have a major impact on bank operations if an alternate third party is required or if the outsourced activity must be brought in-house.

[2] For example, as previously covered in an InfoBytes Special Alert, the OCC issued a white paper outlining its authority to grant national bank charters to fintech companies and described minimum supervisory standards for successful fintech bank applicants.

also shows the OCC's intent to expand vendor management principles to reach marketplace lenders and online platforms that partner with banks to originate loans.

Opportunities for Collaboration Among Banks

Several of the FAQs relate to collaboration among banks to perform diligence and ongoing monitoring of third parties. While "user groups" and "buying clubs" are not new concepts in bank outsourcing and procurement operations, the OCC notes several ways in which banks may collaborate, including by: (i) pooling resources to perform due diligence, contract negotiation, and ongoing monitoring responsibilities; (ii) distributing costs across multiple banks; (iii) sharing third-party responses to common security, privacy, and business resiliency control assessment questionnaires; (iv) creating standardized contracts with common service providers to improve negotiating power; and (v) engaging in industrywide information sharing arrangements to better understand cyber threats to their own institutions as well as to the third parties with whom they have relationships. However, the OCC notes that "each individual bank should have its own effective third-party risk management process tailored to each bank's specific needs." Included among these individual bank responsibilities are:

- Defining the requirements for planning and termination (e.g., plans to manage the third-party service provider relationship and development of contingency plans in response to termination of service)
- Integrating the use of product and delivery channels into the bank's strategic planning process and ensuring consistency with the bank's internal controls, corporate governance, business plan, and risk appetite
- Assessing the quantity of risk posed to the bank through the third-party service provider and the ability of the bank to monitor and control the risk
- Implementing information technology controls at the bank
- Ongoing benchmarking of service provider performance against the contract or service-level agreement
- Evaluating the third party's fee structure to determine if it creates incentives that encourage inappropriate risk taking
- Monitoring the third party's actions on behalf of the bank for compliance with applicable laws and regulations
- Monitoring the third party's disaster recovery and business continuity time frames for resuming activities and recovering data for consistency with the bank's disaster recovery and business continuity plans

Acceptable Outside Resources to Enhance Bank Risk Mitigation Capabilities

The balance of the FAQs addresses the OCC's expectations with respect to certain unique approaches to risk mitigation that may allow banks to enhance services for customers and reduce overall compliance burdens. While by no means does the OCC provide an exhaustive list of such resources, the OCC notes several examples:

- Banks may outsource some or all aspects of their compliance management systems, so long as they "monitor and ensure that third parties comply with current and subsequent changes to consumer laws and regulations." Examples in the bulletin include maintenance, monitoring, and data collection and management, but the bulletin warns that such outsourcing does not replace the need for compliance resources and a strong compliance management system.
- Banks are encouraged – as part of their ongoing monitoring of third-party service providers – to request copies of regulatory examination reports of any supervised technology service providers with which a bank has an existing contract.
- Banks may enter into service provider relationships to build out mobile payment capabilities and facilitate customer payments and transfers made using web applications and in various mobile payment environments. In this regard, the OCC expects 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."
- Banks should consider requesting independent audit reports based on Statement on Standards for Attestation Engagements No. 18 (SSAE 18) to determine the effectiveness of the controls the third party has implemented to monitor the controls of its own subcontractors.

If you have questions about the ruling or other related issues, visit our Vendor Management and FinTech practice pages for more information, or contact a Buckley Sandler attorney with whom you have worked in the past.