Client Alert

June 12, 2017

OCC Guidance Suggests Flexibility for Third-Party Risk Management

By Oliver I. Ireland, Barbara R. Mendelson, Nathan D. Taylor, Jeremy R. Mandell, and Calvin D. Funk

On June 7, 2017, the Office of the Comptroller of the Currency ("OCC") issued frequently asked questions ("FAQs") that supplement the OCC's 2013 guidance entitled "Third-Party Relationships: Risk Management Guidance" ("2013 Bulletin"). The 2013 Bulletin sets forth the OCC's expectation for banks' due diligence and ongoing monitoring of third-party service providers, including enhanced diligence and monitoring for third parties that support critical activities.[1] While the FAQs affirm this guidance, they provide substantial flexibility for banks to right-size their approach to third-party risk management, including with respect to banks' financial technology ("fintech") partnerships.[2] This alert highlights key aspects of the FAQs.

THE THIRD-PARTY RISK MANAGEMENT GUIDANCE IS BROAD…

The FAQs confirm the broad scope of the 2013 Bulletin, stating that any business arrangement between the bank and another entity—including outsourced products and services, use of outside consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements—are third-party relationships subject to the guidance.

These business arrangements include banks relationships with fintech partners. Specifically, the FAQs state that "[i]f 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 and the OCC would expect bank management to include the fintech company in the bank's third-party risk management process."

The FAQs also confirm the 2013 Bulletin definition of "critical activities" and the OCC's expectation that banks have more comprehensive and rigorous management of third-party relationships that involve critical activities. Generally, critical activities include significant bank functions (e.g., payments, clearing, settlements, and custody); significant shared services (e.g., information technology); or other activities that could result in significant risk exposure if a third party fails to meet expectations, could have significant bank customer impact, require significant investment, or could have a major impact on bank operations if the third party fails to perform as expected.

[1] For additional information on the 2013 Bulletin, see our earlier client alert.

[2] The FAQs respond in part to the OCC's commitment, from its responsible innovation initiative, to provide guidance to banks on how to manage risks related to fintech partnerships.

…BUT FLEXIBLE

Notwithstanding the broad scope of the 2013 Bulletin, the FAQs provide flexibility for banks in managing third-party risk. The FAQs state that "[n]ot all third-party relationships present the same level of risk," and "[b]ank management should determine the risks associated with each third-party relationship and then determine how to adjust risk management practices for each relationship" so that the "bank's risk management practices for each relationship [are] commensurate with the level of risk and complexity of the third-party relationship."

The FAQs further provide that "[t]he level of due diligence and ongoing monitoring … may differ for, and should be specific to, each third-party relationship. The level of due diligence and ongoing monitoring should be consistent with the level of risk and complexity posed by each third-party relationship." There is, of course, an expectation that with respect to critical activities "due diligence and ongoing monitoring will be robust, comprehensive, and appropriately documented."

The FAQs signal flexibility in other meaningful ways. For example, the FAQs

- provide for flexibility with respect to banks' structuring of their third-party risk management process;
- indicate that a bank, while maintaining its own effective third-party risk management process tailored to its specific needs, can collaborate with other banks to address the OCC's expectations for managing third-party relationships;
- state that banks may engage in information sharing—including through the Financial Services Information Sharing and Analysis Center ("FS-ISAC"), the U.S. Computer Emergency Readiness Team ("US-CERT"), InfraGard, and other information-sharing organizations that monitor cyber threats and vulnerabilities—to better understand cyber threats to the bank itself or to service providers; and
- state that a bank may "outsource some or all aspects of their compliance management systems to third parties, so long as banks monitor and ensure that third parties comply with current and subsequent changes to consumer laws and regulations." (Note that this is among the strongest language we have seen from the OCC on this point and signals significant flexibility for banks' compliance management systems.)

Notwithstanding this flexibility, the OCC repeatedly reminds banks that "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." Consistent with the 2013 Bulletin, an effective risk management process will include

- policies and procedures for selecting, assessing, and overseeing third parties;
- written contracts outlining the rights and responsibilities of all parties;
- ongoing monitoring of the third party's activities and performance;
- contingency plans for third-party relationships;
- clear roles and responsibilities for overseeing and managing third-party relationships;
- documentation and reporting that facilitates oversight, accountability, monitoring, and risk management; and
- audits of the effectiveness of the risk management process.

The FAQs also signal flexibility in performing third-party due diligence. For example, the FAQs note that when a bank does not receive all of the information it seeks about a third-party service provider that supports the bank's critical activities, there is an expectation that the board of directors and management will

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

With respect to fintechs, the FAQs acknowledge that some third parties may be start-ups with limited financial information. The FAQs state that when assessing the financial condition of a fintech, a bank "may consider a [fintech's] access to funds, its funding sources, earnings, net cash flow, expected growth, projected borrowing capacity, and other factors that may affect the third party's overall financial stability." However, the OCC emphasizes that credit underwriting is not required.

The FAQs specifically address risk management for marketplace lending and mobile payment arrangements. With respect to marketplace lending, the FAQs state that a bank's board and management should understand the range of risks posed by marketplace lending arrangements—reputation, credit, concentrations, compliance, market, liquidity, and operational—and banks should have effective personnel, processes, and systems for monitoring and controlling such risks. As an example, the FAQs state that banks should monitor marketplace lenders to ensure that they appropriately implement applicable consumer protection laws and should not originate or support marketplace lenders that have inadequate compliance management processes. The OCC also focuses on the provision of payment cards to mobile wallets, stating that banks should "work with mobile payment providers to establish processes for authenticating enrollment of customers' account information that the customers provide to the mobile payment providers."

CONCLUSION

All told, the FAQs provide welcome relief to banks and bank service providers from the prevailing (and strict) reading of the 2013 Bulletin. While the guidance does not break new ground and might otherwise be lost in a crowded news cycle, the FAQs seem to signal a change in emphasis from the OCC, or, at minimum, they remind banks of their flexibility to take their own risk-based approach to managing third-party relationships.

Contact:

Oliver I. Ireland	**Barbara R. Mendelson**	**Nathan D. Taylor**	**Jeremy R. Mandell**	**Calvin D. Funk**
(202) 778-1614	(212) 468-8118	(202) 778-1644	(202) 887-1505	(202) 887-6930
oireland@mofo.com	bmendelson@mofo.com	ndtaylor@mofo.com	jmandell@mofo.com	cfunk@mofo.com

Client Alert

Financial Services Team

California		New York	
Alexis A. Amezcua	(415) 268-6557	James M. Bergin	(212) 468-8033
Elizabeth Balassone	(415) 268-7585	Meghan E. Dwyer	(212) 336-4067
Roland E. Brandel	(415) 268-7093	David J. Fioccola	(212) 336-4069
Sarah Nicole Davis	(415) 268-7478	Marc-Alain Galeazzi	(212) 336-4153
Henry M. Fields	(213) 892-5275	Adam J. Hunt	(212) 336-4341
Joseph Gabai	(213) 892-5284	Jessica Kaufman	(212) 336-4257
Angela E. Kleine	(415) 268-6214	Mark P. Ladner	(212) 468-8035
Jim McCabe	(415) 268-7011	Jiang Liu	(212) 468-8008
James R. McGuire	(415) 268-7013	David H. Medlar	(212) 336-4302
Mark David McPherson	(212) 468-8263	Barbara R. Mendelson	(212) 468-8118
Ben Patterson	(415) 268-6818	Michael B. Miller	(212) 468-8009
Sylvia Rivera	(213) 892-5734	Judy Man Ni Mok	(212) 336-4073
Nicholas Alan Roethlisberger	(415) 268-7534	Jeffrey K. Rosenberg	(212) 336-4130
William L. Stern	(415) 268-7637	Mark R. Sobin	(212) 336-4222
Nancy R. Thomas	(213) 892-5561	Joan P. Warrington	(212) 506-7307
Lauren Lynn Wroblewski	(415) 268-6458		

Washington, D.C.		Washington, D.C. (continued)	
Rick Fischer	(202) 887-1566	Donald C. Lampe	(202) 887-1524
Adam J. Fleisher	(202) 887-8781	Jeremy R. Mandell	(202) 887-1505
Natalie A. Fleming Nolen	(202) 887-1551	Amanda J. Mollo	(202) 778-1609
Calvin D. Funk	(202) 887-6930	Obrea O. Poindexter	(202) 887-8741
Julian E. Hammar	(202) 887-1679	Ryan J. Richardson	(202) 887-8761
Oliver I. Ireland	(202) 778-1614	Sean Ruff	(202) 887-1530
Crystal N. Kaldjob	(202) 887-1687	Trevor R. Salter	(202) 887-1527
Steven M. Kaufmann	(202) 887-8794	Nathan D. Taylor	(202) 778-1644

Client Alert

Privacy + Data Security Team

New York		California	
John P. Carlin	(212) 336-8600	Jay Donde	(415) 268-6276
Melissa M. Crespo	(212) 336-4354	Christine E. Lyon	(650) 813-5770
Suhna N. Pierce	(212) 336-4150	Mary Race	(650) 813-5609
Marian A. Waldmann Agarwal	(212) 336-4230	Joseph R. Rosner	(213) 892-5314
Miriam H. Wugmeister	(212) 506-7213	Andrew B. Serwin	(858) 720-5134

Washington, D.C.	
Adam J. Fleisher	(202) 887-8781
Julie O'Neill	(202) 887-8764
Nathan D. Taylor	(202) 778-1644

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. 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 13 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.