

Chapman Client Alert

February 10, 2017

Current Issues Relevant to Our Clients

Third-Party Exam Guidance Clarifies Increased Expectations for Vendor Management

The Supplemental Examination Procedures for Risk Management of Third-Party Relationships (the “Procedures”) issued by the Office of the Comptroller of the Currency (“OCC”) on January 24, 2017, establish detailed compliance obligations for relationships with third-party service providers (“Vendors”). The Procedures are structured such that the OCC will review Vendor risk management with an approach similar to review of a credit portfolio or other similar exam procedure based on the risks associated with the Vendor and the risk mitigants the organization has in place. Examiners will obtain an inventory of all Vendor relationships, select individual files for review (including review of the underlying contract provisions), and evaluate these with respect to the organization’s adopted Vendor risk management policies and procedures.

Exit meetings from exams will include a discussion of Vendor relationships, including if an institution’s Vendor risk classification agrees with the evaluation of the OCC, a list of “exceptions” for contact terms that are not present when required or otherwise documented as waived, and overall compliance with the institution’s policy and procedures, including escalating Vendor matters when necessary to the board of directors.

While the Procedures are applicable to national banks, federal savings associations, and federal branches and agencies of foreign banks, we expect similar process and scrutiny to be followed by other regulatory agencies such as the Federal Deposit Insurance Corporation, which has issued proposed Examination Guidance for Third-Party Lending. In addition, the Procedures will impact those third-party Vendors that provide, or hope to provide, services to or partner with the financial institutions.

Objectives and Scope of the Examination

The Procedures are composed of a series of examination objectives and corresponding questions that will be used during the examination to accomplish the OCC’s examination goals. They use the supervision-by-risk structure familiar to national banks, focusing on the quantity of risk and quality of risk management for each of five categories of risk. The first examination objective is to determine the scope of the examination of the institution’s third-party risk management process and identify examination objectives and activities necessary to meet the supervisory strategy for the institution.

After scoping the exam the objectives are to determine: (1) quantity of each of the operational risk, compliance risk, reputation risk, strategic risk, and credit risk associated with the use of third parties; (2) whether the board has adopted effective policies that are consistent with safe and sound banking practices and are appropriate to the size, nature, and scope of the institution’s third-party relationship; (3) whether the institution has processes in place to manage the risk of its third-party relationships and has systems in place to provide accurate and timely assessments of the risks associated with its third-party relationships; and (4) management’s ability to supervise third-party relationships in a safe and sound manner. The information obtained by the examiner will be used to determine, document, and communicate overall findings and conclusions regarding the examination of the institution’s third-party risk management process.

Examiners determine the scope of the examination in a manner similar to their examination of an institution’s asset quality and other safety and soundness classifications. They will review past examinations; board of directors or committee minutes; outstanding enforcement actions or matters requiring attention and status of corrective action, if any; policies and procedures; a full inventory of the institution’s Vendor relationships, including risk ranking for each; an organization chart; third-party evaluation of the Vendor and complaint logs; monitoring and testing plans; and related reports, among other information. Note, however, that the Procedures instruct examiners to design their examination based on the OCC’s supervisory strategy for the institution and that “seldom will every objective or step of the expanded procedures be necessary.”

Vendor Risk Management Program

The OCC requires organizations to develop policies and procedures based on the five-phase life cycle introduced in OCC Bulletin 2013-29: planning; due diligence and third-party selection; contract negotiation; monitoring; and termination/contingency planning. Risk assessments are to be conducted for each Vendor—low, high, or critical—and reviewed periodically and changed as necessary. The methodology for determining a risk ranking should be identified and the direction of each associated risk—increasing, stable, or decreasing—should be included in the Vendor database. This information is a required component of the report of examination.

Sufficient entity personnel to effectively execute and monitor Vendor relationships is a critical component of the Vendor Risk Management Program. The Procedures question the type and number of personnel participating in Vendor management. This includes the entity's board and management as well as selection of staff with adequate experience and expertise to manage the types of Vendors contracted with by the institution. The program should include a description of how management holds employees who manage Vendor relationships responsible for adhering to policies, conducting due diligence, monitoring, escalating significant issues to senior management, responding to material weaknesses identified in independent reviews, and maintaining appropriate documentation throughout the life cycle of the Vendor.

The institution must have control systems including internal and external audits and quality assurance and information systems to measure performance of Vendors which produce information that enables managers to assess Vendor risk. Such control systems will, among other functions, identify, measure, and track Vendor performance, including exceptions to policies; provide regular reporting on risk of Vendor relationships; and identify complaints, material breaches of contract, service disruptions, and other material issues. Examiners are asked to determine whether management appropriately analyzes and acts on these reviews in a timely manner to manage associated risks.

Financial institutions should review their Vendor Risk Management Program in light of these items that the OCC may request in order to determine its examination scope. If national banks do not regularly maintain the information above, including the detailed Vendor databases, these must be prepared in anticipation of upcoming exams. Where information is not on file or otherwise available for review by the OCC, the entity's Vendor Management Office should immediately seek input from each line of business or owner of the Vendor relationship prior to an examination.

Quantity of the Risk

Examiners are asked to determine the quantity of risk in an association's Vendor relationships. The categories of risk to be evaluated are: (1) Operational Risk; (2) Compliance Risk; (3) Reputational Risk; (4) Strategic Risk; and (5) Credit Risk. The quantity of each associated risk will be identified by the examination as low, moderate, or high. An association should evaluate each type of risk when entering into a Vendor relationship. The Vendor inventory should identify all third-party relationships and call out certain of these risks by indicating those Vendors that involve critical activities (as defined in OCC Bulletin 2013-29); Vendors that use subcontractors; those Vendors that are affiliates or foreign-based entities (or domestic-based entities engaging in foreign transactions); and technology-based Vendors that are storing financial institution data. The inventory of Vendors should also include and specifically note any government-sponsored entities, marketplace lenders, financial utilities (such as Clearing House Interbank Payments System, Depository Trust Company, Fedwire Funds Service, Society for Worldwide Interbank Financial Telecommunication, and Visa and MasterCard), and consultants.

Each of these categories of risk has an associated list of questions used by examiners to identify the quantity of risk. For example, if the institution has third-party relationships that include the use of subcontractors, the institution is required to disclose its process to identify Vendors with subcontractor relationships and include the information regarding subcontractor relationships on its Vendor database.

The evaluation of the quantity of risk for Vendor programs is broken down into the categories of risk identified above and is heavily dependent on the level of management involvement to (a) administer these risks within the institution's parameters established by the board of directors and (b) mitigate those risks. This evaluation starts at the board level with adoption of the organization's risk tolerance and memorializing it within Vendor management policies and procedures. Included in the review is whether the Vendor's policies and procedures are sufficient to ensure that the Vendor can comply with new consumer compliance, OFAC, and BSA/AML requirements by their stated effective dates and whether the financial institution has a contingency or termination plan if the Vendor is unable to comply.

Marketplace Lending and Credit Risk. There has been an increasing focus on credit risk with the use of marketplace lenders, defined as companies engaged in the Internet lending business, and other providers as a source of loans. The Procedures require examiners to evaluate whether an institution has conducted adequate due diligence on these

Vendors for the type of loans originated or activities otherwise undertaken on behalf of the institution, and determine if the underwriting standards agreed upon match those of the institution and the institution's strategic goals, among other factors. While these specifically focus on marketplace lenders, the criteria used to evaluate Vendor relationships with marketplace lenders should also be used for other Vendors with which the institution has a relationship for the origination or purchase of loans.

Quality of Risk Management

Examiners are asked to determine whether the board of directors has adopted effective policies that are consistent with safe and sound banking practices for Vendor management. The quality of risk management will be identified in the examination as strong, satisfactory, insufficient, or weak. To make this determination, examiners will review the institution's policies and processes.

Policies. Examiners will consider whether the institution's policies are adequate for the institution's size, nature, and scope of its Vendor relationships. They will review the policies to determine if they establish responsibilities and accountability; include risk limits and action if limits are breached; contain criteria for defining critical Vendor relationships; require board approval of all critical Vendor contracts; and include a method to be used for Vendor risk assessment. The board must periodically review and approve Vendor policies, and the Vendor policies must be communicated to personnel with supervisory responsibilities for Vendor relationships.

Processes. In order to examine an organization's processes, the OCC will use the five life-cycle phases contained in OCC Bulletin 2013-29 described above. In each phase the examiners are asked generally to determine if the organization has processes defined as procedures, programs, and practices that "impose order on a bank's pursuit of its objectives." The processes must be adequate to manage the risk of the organization's Vendor relationships, consistent with the organization's policies and governed by appropriate checks and balances such as internal controls.

Each of the five life-cycle phases has a detailed checklist to determine compliance with the OCC's examination objective to establish whether the institution has processes in place to manage the risk of Vendor relationships for that phase of the life cycle. The requirements expand on the information contained in OCC Bulletin 2013-29. The most extensive requirements apply to life cycle phase 2—Due Diligence and Third-Party Selection. The OCC reviews the assessment

methods used by the institution to determine whether they are commensurate with the level of risk presented by the Vendor. The factors in this checklist include licenses and expertise; processes and controls to provide services in compliance with laws and regulations; adequate financial information, including litigation; unfunded liabilities, and other factors that may affect financial stability; experience and reputation, including customer complaints and litigation; fee structure and incentives; fraud prevention; background checks on management, employees, and subcontractors; information security program, including emerging threats; service levels and reporting; employee training; reliance on subcontractors; and sufficient insurance coverage.

The institution must be diligent in documenting the process and in evaluating, acknowledging, and either approving the inherent risk or selecting another Vendor. Among the considerations, the OCC asks the institution whether the financial benefits of the Vendor relationship "outweigh the estimated costs to control the risks." Management (and the board of directors as appropriate) must be involved in the decision-making process, and that process must be documented. Without documentation of the process, examiners may cite exceptions to the Procedures in their report of examination, which could also result in greater scrutiny of the institution on subsequent exams and lowering of the institution's ratings.

Conclusion and Recommendation

In response to the Procedures, institutions are advised to address Vendor management as any other line of business, including when it comes time for examination by regulators. This can be done only by having a culture of compliance toward Vendor management and implementing the necessary documentary process and procedures to give the organization the ability to respond to requests for information outlined in the Procedures as it would for any other type of regulatory exam. This information must be updated periodically as required by changes to products, by legal requirements, or by changes to the Vendor and Vendor systems.

Examiners are required to communicate the overall findings to the institution and summarize the risks and obtain commitments for corrective action from management. If necessary, the exam report will contain matters requiring attention by management and board of directors. This could impact the supervisory strategy for the institution on an ongoing basis for future exams. Therefore, an institution should conduct an evaluation of the Vendor Management Program and documentation currently used to demonstrate compliance and supplement where necessary.

Vendor contracts, especially with those Vendors designated as “critical,” must be reviewed to verify the presence of relevant contract terms or document the reason for any exceptions to policies and procedures. Although the Procedures specifically address marketplace lenders, we recommend that all Vendor relationships with loan originators be reviewed in a similar manner to verify expectations when acquiring loans from a Vendor. Finally, policies must be evaluated to ensure that the board and senior management have appropriate levels of responsibility and that employees who manage Vendor relationships are responsible for adhering to policies, conducting due diligence, monitoring, and escalating significant issues to senior management.

For More Information

If you would like further information concerning the matters discussed in this article, please contact any of the following attorneys or the Chapman attorney with whom you regularly work:

Marc P. Franson

Chicago
312.845.2988
franson@chapman.com

Scott R. Fryzel

Chicago
312.845.3784
fryzel@chapman.com

Heather L. Hansche

Chicago
312.845.3714
hansche@chapman.com

Lindsay S. Henry

Chicago
312.845.3869
lhenry@chapman.com

Chapman and Cutler LLP

Attorneys at Law • Focused on Finance®

This document has been prepared by Chapman and Cutler LLP attorneys for informational purposes only. It is general in nature and based on authorities that are subject to change. It is not intended as legal advice. Accordingly, readers should consult with, and seek the advice of, their own counsel with respect to any individual situation that involves the material contained in this document, the application of such material to their specific circumstances, or any questions relating to their own affairs that may be raised by such material.

To the extent that any part of this summary is interpreted to provide tax advice, (i) no taxpayer may rely upon this summary for the purposes of avoiding penalties, (ii) this summary may be interpreted for tax purposes as being prepared in connection with the promotion of the transactions described, and (iii) taxpayers should consult independent tax advisors.

© 2017 Chapman and Cutler LLP. All rights reserved. Attorney Advertising Material.