Skadden

Skadden, Arps, Slate, Meagher & Flom LLP & Affiliates

Outsourcing by Financial Services Companies: Impact of the OCC and FRB Guidelines

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Stuart D. Levi
New York
212.735.2750
stuart.levi@skadden.com

William J. Sweet, Jr.
Washington, D.C.
202.371.7030
william.sweet@skadden.com

James S. Talbot
New York
212.735.4133
james.talbot@skadden.com

* * *

Four Times Square, New York, NY 10036
Telephone: 212.735.3000

WWW.SKADDEN.COM

Outsourcing has become a critical component of financial institutions' management of their business operations and control of their costs. In addition, institutions are outsourcing increasingly complex and sensitive banking and financial operations to third parties. In light of these developments, the Office of the Controller of the Currency (OCC) and the Federal Reserve Board (FRB) recently issued guidance on how financial institutions should manage third-party risks. The guidance issued by each agency has particular relevance to outsourcing transactions and provides companies with a roadmap of the key areas of concern to regulators. Institutions also should expect that regulators will ask them to compare their policies and procedures against the new OCC and FRB guidance.

As discussed below, many of the suggestions in the OCC and FRB guidance concern provisions of outsourcing agreements (such as subcontracting) where vendors often push back. Financial institutions can therefore use the guidance to support and bolster their position when negotiating these provisions with vendors.

We summarize the OCC and FRB guidance below and include (in bold italics) our comments and key take-aways.

OCC Guidance on Managing Third-Party Risk

The Office of the Comptroller of the Currency has issued guidance to national banks and federal savings associations on assessing the risk in third-party relationships, with a particular focus on outsourcing relationships (the OCC Guidance).[1] The OCC Guidance rescinds and replaces OCC Bulleting 2001-47, "Third Party Relationships: Risk Management Principles" and OCC Advisory Letter 2000-9. The OCC accurately observes that banks are outsourcing increasingly complex functions and processes, which is exposing them to greater risk. These "critical activities" include: (1) significant bank functions such as payments, clearing, settlement and custody; (2) those involving significant shared services, such as information technology; and (3) activities that could have significant customer impacts, require significant investment in resources, or significantly impact bank operations if the relationship failed.

In assessing the industry, the OCC found that certain banks had failed to properly assess the risks and costs of managing third party relationships; had failed to perform appropriate due diligence and entered into agreements that incentivized the service provider to take risks that are detrimental to the bank. These risks include operational, compliance, reputational and strategic (*i.e.*, the bank cannot remain competitive because of poor outsourcing performance). Therefore, it is not surprising that the new OCC Guidance places increased emphasis on legal and regulatory compliance and post-termination transition.

The OCC notes that banks should adopt risk management practices that are commensurate with the risk they are undertaking. The OCC Guidance touches on a number

1 OCC Bulletin 2013-29; Risk Management Guidance (October 30, 2013).

of issues that come up in negotiating outsourcing transactions. Significantly, the OCC cautions that "[a] bank's failure to have an effective third-party risk management process that is commensurate with the level of risk, complexity of third-party relationships, and organizational structure of the bank may be an unsafe and unsound banking practice." Banks should, therefore, pay careful attention to the OCC Guidance. However, the OCC Guidance also provides banks with important leverage when negotiating outsourcing agreements, since they can point to the OCC Guidance as the basis for why certain provisions are required.

We summarize the OCC Guidance below, inserting (in bold/italics) our thoughts based on our experience with outsourcing by financial services institutions.

Risk Management Lifecycle

The OCC sets forth what it deems the five key phases for effective risk management: planning, due diligence, contract negotiation, ongoing monitoring and termination.

Planning

This phase focuses on developing a plan to manage the relationship and assess the risks. This includes a cost-benefit analysis weighing the financial benefits with the estimate costs to control and oversee the vendor. This planning phase should include, among other items:

- Assessing the nature of customer interactions with the vendor.
- Assessing the information security implications.
- Assessing the regulatory implications.

The OCC correctly observes that many outsourcing customers, including banks, fail to appreciate the amount of resources required to manage an outsourcing relationship. In contrast to the planning proposed by* Bulletin 2001-47*, the new OCC Guidance recommends that regulatory compliance, information security and contingency planning (*i.e.*, post-termination transition) be part of the planning phase. This change reflects the importance of these areas in the outsourcing arena.

Due Diligence and Third-Party Selection

The OCC observes that all too often banks rely on their prior experience with the vendor as a proxy for due diligence. ***The OCC correctly observes that every outsourcing project should include a thorough due diligence phase. Although the RFP process can be time-consuming, it provides a critical opportunity for banks to assess and compare various service providers.***

Such due diligence should include the following steps. Those marked with an (*) indicate an addition to the requirements set forth in *Bulletin 2001-47*:

- Reviewing whether the third party's business strategy — such as its plans for mergers and divestitures and its quality initiatives — aligns with the bank. ***This is an important, and often overlooked-part of the diligence process. Banks may learn that the vendor is rumored to be divesting a key part of its business or looking to merge with other vendors.***
- Evaluating the vendor's legal and regulatory compliance programs. (*)
- Reviewing the vendor's audited financial statements and otherwise conducting due diligence of its financial condition.

- Evaluating the bank's reputation and depth of resources.
- Assessing the proposed fee structure to determine if it creates inappropriate risks (such as high upfront fees). (*)
- Reviewing the vendor's background check policies. ***Vendors often push back on this requirement, so the OCC's Guidance in this area provides banks with an important argument as to why such a provision in the Master Services Agreement (MSA) would be required.***
- Assessing the vendor's information and physical security programs and policies. (*)
- Reviewing the company's programs to train employees on policies and procedures. ***Banks learn that the vendor has robust policies on paper, but fails to train its employees adequately.***
- Assessing a vendor's use of, and reliance on, subcontractors, and its ability to assess and monitor them. ***Vendors increasingly are relying on subcontractors to perform tasks that the customer likely thought the vendor would perform itself. This is the result of vendors looking to cut their own costs. Therefore, understanding the manner in which a vendor uses subcontractors, and any limits on such usage it is willing to agree to, is critical.***
- Assessing the vendor's insurance coverage. ***The issue of insurance coverage is often tabled until the end of contract negotiations, and banks sometimes find that a vendor's insurance does not meet the bank's minimum requirements for third parties. Learning about the vendor's insurance coverage during the diligence phase can prevent issues in the future when this topic is negotiated. Indeed, many outsourcing customers require the vendor to disclose its insurance coverage during the RFP phase.***
- Reviewing the vendor's incident reporting procedures. (*)
- Assessing a vendor's third-party relationships (*e.g.,* with subcontractors) to see if they create conflicts. (*) ***While this proposal makes sense, banks may find that vendors will not disclose the specifics of their third-party contractual relationships.***

Contract Negotiations

The OCC describes a number of key provisions that should be included in each outsourcing agreement. The OCC Guidance therefore provides a bank with important leverage when arguing that certain provisions need to be included in an MSA:

- **Nature and Scope of Arrangement**. A description of the services to be provided is at the core of any MSA. However, the OCC recommends that the description also include the ancillary services such as software or other technology support and maintenance, employee training and customer service.
- **Performance Measures or Benchmarks**. Service levels are a second area that is essential to an MSA. The OCC cautions, however, that performance measures should not "incentivize undesirable performance, such as encouraging processing volume or speed without regard for accuracy, compliance requirements, or adverse effects on customers." ***In addition, banks should review the SLAs carefully to make sure that they properly reflect the bank's requirements. Customers often agree to SLAs that, if achieved, do not necessarily provide the customer with any meaningful benefit.***

- **Responsibilities for Providing, Receiving and Retaining Information**. A central theme of the OCC guidance is reporting and monitoring. The OCC recommends that the contract requires the vendor to provide and retain timely, accurate, and comprehensive information that allow the bank to monitor performance, service levels, and risks. ***In general, such a provision would not be controversial. However, the OCC also recommends specific types of reporting that vendors may push back on. The OCC Guidance provides banks with the leverage to demand these reports. These suggested reports include:***
  - The prompt notification of financial difficulty, catastrophic events and significant incidents such as information breaches, data loss, service or system interruptions, compliance lapses, enforcement actions or other regulatory actions. ***While prompt information about a data breach has become a standard requirement in MSAs, notification of financial difficulty or regulatory actions (that do not directly arise from the services being provided to the bank itself) may be more controversial.***
  - Personnel changes, or implementing new or revised policies, processes and information technology. ***Vendors often are reluctant to allow customers to micro-manage their operations. In the vendor's view, if services meet the SLAs, then the customer should not be entitled to further information. As a result, vendors may be reluctant to notify the bank about personnel changes.***
  - Notification to the bank of significant strategic business changes, such as mergers, acquisitions, joint ventures, divestitures or other business activities that could affect the activities involved. ***Vendors may be reluctant to provide such notifications, and in any event, may indicate that they can only do so when the transaction can be publicly disclosed. Again, the OCC Guidance provides the requisite leverage for a bank to demand this clause.***
- **Responsibility for Compliance With Applicable Laws and Regulations**. The MSA should address compliance with laws, regulations, guidance and self-regulatory standards. ***Compliance with law, and more specifically, which party is responsible for monitoring changes in the law — and which party bears the cost of any required changes — often are key areas of disputes in financial service outsourcing agreements. Banks should pay close attention to how this provision is phrased in the MSA.***
- **Cost and Compensation**. Banks should ensure the contracts do not include burdensome upfront fees or incentives that could result in inappropriate risk taking by the bank or third party. Specify the conditions under which the cost structure may be changed, including limits on any cost increases. ***A key area of dispute in MSA negotiations is which party bears the costs of technology upgrades required to keep current with industry standards or in changes to the bank's requirements. Banks should be as specific as possible in defining which party bears these costs.***
- **Ownership and License**. The MSA should include appropriate warranties by the vendor related to its use of third-party intellectual property licenses.
- **Confidentiality and Integrity**. The MSA should specify when and how the vendor will disclose information security breaches that have resulted in unauthorized intrusions or access that may materially affect the bank or its customers. In addition, the MSA should address the power of each party to change security and risk management procedures and requirements, and to resolve any confidentiality and integrity issues arising out of shared use of facilities owned by the third party. ***Over the last three years, vendors have pushed***

back considerably on their obligations in the event of a data breach. Their primary concern is a cybersecurity attack that results in harm to the bank's customers, even though the vendor had industry standard security procedures in place (that may have even been vetted and approved by the bank). The key areas of disagreement in these negotiations include (1) vendors looking to cap their liability (and possibly even eliminate it if their security protocols were approved by the bank and followed, (2) obligations to notify the bank if the vendor had a breach that impacted another customer (in such cases the bank may still want to know of the intrusion) and (3) the timeliness within which a breach event must be disclosed.

- **Business Resumption and Contingency Plans**. The MSA should require the vendor to provide the bank with disaster recovery plans. ***Vendors likely will not push back on the need to have disaster recovery plan, but may try and limit the bank's right to review or audit the full plan. The OCC requirement should help banks in any disagreement on whether the plan needs to be disclosed.***

- **Indemnification**. Banks should carefully assess any indemnifications they are providing the vendor.

- **Insurance**. The MSA should stipulate that the third party is required to maintain adequate insurance, notify the bank of material changes to coverage and provide evidence of coverage where appropriate. ***See the discussion of insurance in the due diligence section.***

- **Dispute Resolution**. Banks also should determine whether any liability caps are in proportion to the amount of loss the bank might experience, and consider whether the MSA should include a dispute resolution process. ***Liability caps are one of the most controversial aspects of any MSA. The bank should carefully consider whether caps are appropriate and, as the OCC notes, whether they leave the bank with adequate protection. If the vendor insists on a cap, the bank should consider whether there should be different caps depending on the harm that was caused. Banks should also reject the all-too-common "one times' service fees" formulation unless that amount is an accurate reflection of the bank's risk.***

- **Default and Termination**. The OCC makes three key points:

  – The bank should determine whether it includes a provision that enables the bank to terminate the contract, upon reasonable notice and without penalty, in the event that the OCC formally directs the bank to terminate the relationship. ***Vendors often push back on such regulatory termination rights on the grounds that, if they did not breach the agreement, they should not bear all the risk of a regulatory mandate. The bank should try to limit its exposure in these situations to covering the vendor's sunk costs (as opposed to also covering future profits).***

  – The MSA should permit the bank to terminate the relationship in a timely matter without prohibitive expense. ***In some cases, vendors demand exceedingly high termination penalties if the bank looks to terminate in an early year of the term. The OCC Guidance will help banks argue for "cost-effective" termination rights.***

  – The MSA should include termination and notification requirements with timeframes to allow for the orderly conversion to another vendor.

- **Customer Complaints**. The MSA should specify whether the bank or vendor is responsible for responding to customer complaints.

- **Subcontracting**. The MSA should specify (1) the activities that cannot be subcontracted; (2) whether the bank prohibits the vendor from subcontracting activities to certain locations or to specific subcontractors. The bank should also have the right to terminate the MSA without penalty if the vendor's subcontracting arrangements do not comply with the MSA. ***Banks typically see the subcontracting issue as an "all or nothing" issue. As the OCC Guidance highlights, subcontracting can be parsed in a manner that limits its scope, the subcontractors that can be used or the location of the subcontractor.***

- **Foreign-Based Third Parties**. MSAs with foreign-based third parties should include choice-of-law and jurisdictional provisions that provide for adjudication of all disputes under the laws of a specified jurisdiction.

- **OCC Supervision**. The MSA should stipulate that the performance of activities by the vendor is subject to OCC examination oversight, including access to all work papers, drafts and other materials. ***As the OCC Guidance notes, the OCC has the authority to examine and regulate functions or operations performed or provided by third parties to the same extent as if they were performed by the bank itself on its own premises. In addition to general audit provisions, banks should include a specific reference to the OCC authority in the MSA.***

Ongoing Monitoring

Once an MSA is signed, banks need to establish procedures to monitor the activities of the service provider on an ongoing basis. This is particularly important when the third-party relationship involves critical activities, and may include on-site visits. Banks also should ensure that their ongoing monitoring adapt accordingly because both the level and types of risks may change over the lifetime of third-party relationships. ***Outsourcing customers frequently monitor the service provider during cutover, but then become lax during steady state. The result is that service quality often slips during the middle and later years of an agreement. Formal procedures to monitor vendor activity can help address this issue.***

As part of the ongoing monitoring, the OCC suggests that the following areas be taken into account:

- business strategy (including acquisitions, divestitures, joint ventures) and reputation (including litigation) that may pose conflicting interests and impact the service provider's ability to meet contractual obligations and service-level agreements.

- compliance with legal and regulatory requirements.

- financial condition.

- insurance coverage.

- key personnel and ability to retain essential knowledge in support of the activities.

- ability to effectively manage risk by identifying and addressing issues before they are cited in audit reports.

- process for adjusting policies, procedures and controls in response to changing threats, new vulnerabilities, material breaches or other serious incidents.

- information technology used or the management of information systems.

- ability to respond to and recover from service disruptions or degradations and meet business resilience expectations.

- reliance on, exposure to or performance of subcontractors; location of subcontractors; and the ongoing monitoring and control testing of subcontractors.
- agreements with other entities that may pose a conflict of interest or introduce reputation, operational or other risks to the bank.
- ability to maintain the confidentiality and integrity of the bank's information and systems.
- volume, nature and trends of consumer complaints, in particular those that indicate compliance or risk management problems.
- ability to appropriately remediate customer complaints.

The foregoing list provides a thorough overview of the areas companies should consider. It also provides banks with leverage to argue that they need ongoing access to financial information; changes to policies and IT; etc. While the list in many ways mirrors **Bulletin 2001-47*, it adds legal and regulatory compliance, information security and subcontracting as areas to be monitored on a going-forward basis.***

Termination

Banks should establish a transition plan with the service provider to ensure a smooth transition to bring the services in-house or to migrate to a new service provider in the event of contract expiration or termination. This includes data retention the handling of intellectual property that was jointly developed by the parties and ongoing compliance with law. ***In many cases, the MSA requires such a plan be created post-signing but, once the relationship commences, creation of the plan is relegated to the back burner and often never completed. If the customer waits to draft a transition plan when an MSA is about to be terminated, it will be doing this important activity when cooperation between the parties may be at a low point.***

Steady-State Requirements

The OCC recommends a number of steps banks should take during the outsourcing engagement:

- **Oversight and Accountability**: This includes assigning clear roles and responsibilities for managing the relationship, and integrating the risk management process with the bank's broader risk management processes. Specifically, the OCC recommends that not only employees and senior management have defined roles, but also that, for critical activity outsourcing, the board assesses the risk, reviews due diligence reports and approves the MSA.
- **Proper Document and Reporting**: The OCC sees proper reporting as a way to facilitate risk management. This includes not only reporting from the vendor, but also internal reports that list all third-party relationships and their risk profile, ongoing audit reports and cost analyses.
- **Independent Reviews**: Independent reviews allows a bank to assess the ongoing risk. ***It is important that the MSA allow the bank to conduct third-party audits. Some vendors will require such third parties to sign confidentiality agreements, and may want to exclude anyone they deem a competitor.***

FRB Guidance on Managing Outsourcing Risk

Shortly after the OCC released its guidance on third-party risk, the Federal Reserve Board issued specific guidance on outsourcing for "financial institutions," which it defines as: state member

banks, bank and savings and loan holding companies (including their nonbank subsidiaries), and U.S. operations of foreign banking organizations (the FRB Guidance).[2] Like the OCC, the FRB highlighted the increased risk that exists as increasingly critical functions are outsourced.

The FRB Guidance begins by listing the key risks from outsourcing: compliance; concentration (*i.e.,* relying on a limited number of service providers or providers concentrated in a limited geographic region); reputational; country (*i.e.*, outsourcing to a country where the economic, political or social conditions are not stable); operational and legal.

Board of Director and Senior Management Responsibilities

The FRB recommends that the board or its executive committee of the board establish policies for the use of service providers. These polices should include risk assessments and due diligence, standards for contract provisions and considerations, ongoing monitoring of service providers, and business continuity and contingency planning. Senior management should be tasked with ensuring these polices are properly executed.

Service Provider Risk Management Programs

A financial institution's risk management program should focus on outsourced activities that "have a substantial impact on a financial institution's financial condition; are critical to the institution's ongoing operations; involve sensitive customer information or new bank products or services; or pose material compliance risk." The risk assessment will depend on the criticality of the function being outsourced and the reputation of the service provider. The FRC defines a series of core elements for risk management that, in many ways, overlap those set forth by the OCC. These are risk assessments, due diligence and selection of service providers, contract provisions and considerations, incentive compensation review and oversight and monitoring of service providers.

Risk Assessment

According to the FRB, a financial institution should first determine whether outsourcing is consistent with its strategic direction, and then conduct cost/benefit and benefit/risk assessments. As part of this assessment, financial institutions should confirm there are qualified and experienced service providers to perform the service on an ongoing basis. ***This is a critical point for financial institutions to consider. Given the somewhat unique nature of many outsourcing projects in this industry, financial institutions may find that there are few (or no) qualified and experienced vendors.***

Financial institutions also should consider if they will be able to provide the appropriate oversight and monitoring of the vendor going forward.

Due Diligence

The FRB correctly points out that outsourcing diligence should include technical experts and the key stakeholders. Due diligence should cover the vendor's business background, reputation and strategy, financial performance and condition and operations and internal controls.

The financial due diligence should take into account "the potential impact of the financial institution's business relationship on the service provider's financial condition." ***The FRB correctly observes that outsourcing customers often fail to consider how their own project will put pressure on the vendor's resources.***

---

2 Federal Reserve Board, *Guidance on Managing Outsourcing Risk*, December 5, 2013. The FRB Guidance supplements the *FFIEC Outsourcing Technology Services* (June 2004) at http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx.

Other factors to consider during financial due diligence include:

- The service provider's most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity and operating results.
- The service provider's sustainability, including factors such as the length of time that the service provider has been in business and the service provider's growth of market share for a given service.
- The service provider's commitment (both in terms of financial and staff resources) to provide the contracted services to the financial institution for the duration of the contract.
- The adequacy of the service provider's insurance coverage.
- The adequacy of the service provider's review of the financial condition of any subcontractors.

Contract Provisions and Considerations

The FRB notes that all outsourcing agreements should be in writing and sets forth some of the key provisions. These include defining the scope of the services, subcontracting rights, service fees, audit rights, the establishment of performance metrics, information security requirements (including requirements for data breach notifications), IP ownership (including whether any source code should be escrowed), liability limitations, termination triggers and contingency planning.

While most of the FRB suggestions in this area are routine, it makes two notable recommendations with respect to subcontracting: (1) financial institutions should pay special attention to foreign subcontractors, since their information security and data privacy standards may be different and (2) the MSA should include the service provider's process for assessing the subcontractor's financial condition to fulfill contractual obligations.

Incentive Compensation Review

The financial institution should make sure that it has processes in place to monitor whether any incentive compensation it offers is providing the "wrong" incentives to the vendor and placing the financial institution at risk. ***As noted above in the discussion of the OCC Guidance, customers typically agree to incentive compensation that, if achieved, does not necessarily provide the customer with any meaningful benefit.***

Oversight and Monitoring

The oversight process, including the level and frequency of management reporting, should be risk-focused. For example, higher risk service providers may require more frequent assessment and monitoring. ***This is an important point for financial institutions to consider. Outsourcing customers sometimes view monitoring as a "check the box" exercise. Looking at it from a risk perspective should help financial institutions better focus on this important step in the outsourcing life cycle.***

Ongoing monitoring should include:

- The vendor's financial condition, including their most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity and operating results. In addition, if the vendor relies significantly on subcontractors to provide the service, it should include the vendor's controls and due diligence regarding the subcontractors.

Financial institutions should expect resistance in this area and can rely on the FRB Guidance to justify why this information is required.

- The vendor's internal controls, such as the American Institute of Certified Public (including the Accountants' Service Organization Control 2 report).
- Triggers to escalate oversight and monitoring when the vendor fails to meet performance, compliance, control, or viability expectations. This should include a termination right if not properly addressed.

Business Continuity and Contingency Planning

Financial institution contingency plans should focus on critical services provided by the vendor and alternative arrangements in the event the vendor is unable to perform. The FRB advises that financial institutions have a contingency plan in place and periodically test it; which is a step most institutions take. ***However, the FRB also advises that financial institutions maintain an exit strategy, including a pool of comparable service providers, in the event that a contracted service provider is unable to perform. Most outsourcing customers do not take this extra step, and financial institutions should be mindful of the FRB Guidance on this point.***

Additional Risk Considerations

The FRB Guidance concludes by listing additional risks that financial institution outsourcing clients should consider:

- **Suspicious Activity Report (SAR) Outsourcing**. The FRB notes that, given the confidentiality of suspicious activity reporting, the outsourcing of any SAR-related function is more complex. Financial institution management should ensure they understand the risks associated with such an arrangement and any Bank Secrecy Act specific guidance in this area.
- **Foreign-based service providers**. Financial institutions should ensure that foreign-based vendors are in compliance with applicable U.S. laws, regulations and regulatory guidance. In addition, the FRB makes the important point that local laws in the vendor's home country may limit on-site reviews, and therefore should be reviewed. Finally, financial institutions should consider the authority of foreign regulators to access the financial institution's customer information while auditing the foreign-based vendor.
- **Internal audit**. Financial institutions should refer to existing guidance on the engagement of independent public accounting firms and other outside professionals to perform work that traditionally has been carried out by internal auditors.
- **Risk management activities**. In the event a financial institution outsources risk management activities (*e.g.*, model risk management), it should require the vendor to provide evidence of the product's component and design so the financial institution can measure it against its own risk exposures.