Skadden

Outsourcing in the Financial Services Industry: Finding Opportunities and Managing Risk

March 24 , 2014

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or 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

4 Times Square
New York, NY 10036

On February 27, 2014, Skadden presented a webinar titled "Outsourcing in the Financial Services Industry: Finding Opportunities and Managing Risk." Firm partners Stuart Levi and Bill Sweet and counsel Jamie Talbot presented an in-depth review of the outsourcing opportunities and risks financial institutions face today. Topics covered were the impact of the recent Office of the Comptroller of the Currency (OCC) and Federal Reserve Board (FRB) guidance on managing third-party risk, best practices when negotiating outsourcing agreements in the financial institutions industry, positions vendors take on critical issues, and ways in which cybersecurity attacks are shaping the outsourcing landscape.

OCC and FRB Guidance on Managing Third-Party Risk

Bill Sweet began the presentation with an overview of the guidelines promulgated by the OCC in October 2013 and the FRB in December 2013. Both sets of guidelines showcase an expanded scope beyond the traditional focus on IT matters and stem from concern that financial institutions are outsourcing riskier and more complex functions, yet the management of outsourcing risk has not kept pace with such expansion. The guidelines set out in the OCC's Risk Management Guidance are more proscriptive in establishing the greatest requirements for outsourcing of "critical activities." Critical activities include specific named activities as well as any outsourcing activity that meets a four-part test. The test requires that the activity (i) pose a risk to the financial institution if the third party fails to meet its requirements or expectations, (ii) could have significant customer impact, (iii) requires significant investment and resources to manage, and (iv) has a major impact to the operations of the financial institution. Practically speaking, this is a functional test to measure the materiality of the outsourcing arrangement. The OCC guidelines also include discrete, specific tasks for the bank board, senior management and bank employees who manage third-party relationships. For example, the board must approve all contracts with third parties that provide critical activities.

The guidelines set out in the FRB's Guidance on Managing Outsourcing Risk are shorter and more principle-based. The guidelines focus on business functions and activities, but unlike the OCC guidelines do not specifically define covered activities. Instead, the level of compliance is based upon the risk assessment associated with the activity. The FRB guidelines do not contain distinct tasks for bank management or bank employees. Instead, the board generally is responsible for establishing broad policies and overseeing their implementation. Bill noted that the OCC and the FRB did not take a joint interagency approach. Instead, the FRB acted after the OCC issued its guidelines, which means there is no reason to expect convergence between the two agencies.

Bill observed that these were both published as guidelines not regulations; therefore, they are not binding. Under a guideline, the relevant agency examiner is to exercise discretion in determining the applicability of the guidelines and act on a case-by-case basis. Bill noted that guidelines are, in fact, often applied as written and without discretion. Institutions that do not follow the guidelines will be considered by the agency to be engaged in unsafe and unsound practices — a determination that could be used in an examination report or enforcement proceeding if the agency believed the noncompliance is grave enough to bring to that level.

Bill noted that it is still too early to determine how rigorously these guidelines will be applied, but it seems likely they will be extremely important because of the continuing growth of outsourcing in business models today.

The Outsourcing Landscape

Stuart Levi continued the webinar with an overview of the critical developments in recent years that have changed the financial services outsourcing landscape. Outsourcing has moved beyond traditional forms, such as IT and human resources, to operational functions and increasingly complex and industry-specific services. As a result, the risk profile associated with outsourcing in this sector has never been greater, which has brought greater scrutiny from regulators. In addition, vendors are looking to cut costs as their margins shrink. This translates into tougher negotiations and vendors looking to exploit contract loopholes.

Stuart spoke about how financial services companies face a unique set of risks. As compared to other industries, financial service companies are more likely to provide vendors with access to sensitive confidential information (such as financial and trading information, customer information, etc.). They also are more likely to outsource sensitive customer-facing transactions. Finally, in recent years, financial institutions have experienced large volume fluctuations and constantly evolving business models, which can impact fee structures, change control provisions and effect termination rights.

Stuart then addressed how the new OCC and FRB guidelines should impact a company's approach to outsourcing transactions. Both sets of guidelines (although the OCC more explicitly) look at an outsourcing transaction as having a risk management life cycle. During each phase of the transaction, the financial services company must effectively manage its risk. These phases include: planning, due diligence and vendor selection, contract negotiation, ongoing monitoring and termination. In the preplanning stage, companies should organize and coordinate internal stakeholders, review third-party and customer agreements for any restrictions that might impact the ability to outsource, track internal Service Level Agreements (SLAs) to create a baseline for any potential vendor, and consider the global regulatory approvals and notifications that may be required to outsource (which could delay start dates in certain countries).

The planning stage requires companies to consider the oversight and governance necessary for an outsourcing relationship. Companies typically do not appreciate the amount of time and effort required to oversee a vendor and often fall short in this area. The risk — besides operational issues — is that regulators easily can focus on this as a shortcoming of the company's risk management program. Stuart emphasized that it is important for a company to consider, before entering into a transaction, whether the benefit of outsourcing outweighs the cost to manage the risk.

The regulatory guidance particularly has been focused on the due diligence and vendor selection phase of the transaction. Companies should have a formalized, but flexible, process to evaluate, among other areas: the financial condition of the vendor, the vendor's

strategic goals, the vendor's policies and procedures, and the vendor's potential vulnerabilities. The OCC noted, in particular, that inquiry into the vendor's financial condition should be "as comprehensive as if extending credit to the third party." Reviewing a vendor's policies and procedures is particularly important given that vendors are resisting the requirement to comply with customer policies and procedures, and advocating that they should be able to comply with their own policies. Companies also should conduct diligence into the vendor's prior performance, including whether it has experienced any service degradation issues or has experience working with a regulated entity.

Stuart outlined two types of outsourcing structures increasingly prevalent in the financial services industry — captive and hybrid outsourcing. Captive-entity outsourcing involves outsourcing to a company's own affiliate or subsidiary, typically located in a foreign jurisdiction. Some companies will acquire small service providers and convert them to captives. The benefits of captive-entity outsourcing include cost-savings, potential revenue generation by providing services out to third parties, better control over the service provider, exposure to local markets using a low-risk approach, easier management of policies and procedures (since the entity will be following those of the parent), and less governance friction. However, a company should consider that, as compared to traditional third-party outsourcing, the cost savings are typically not as attractive because it is harder to convert variable to fixed costs, SLAs will not be as strictly enforced, there is no ability to shift risk, and there is less access to the "best of the breed" technologies.

Stuart explained that hybrid outsourcing is where a third-party vendor provides a customer with standard outsourcing services as well as a "hosted" environment in which the customer's own employees work, typically in the same building. Hybrid outsourcing, therefore, allows an organization to easily shift a service between providing it in-house and outsourcing it since all that is required is rebadging the employee. For example, if a customer decides to bring a service back in-house, it merely has to have the relevant employees move from being employed by the outsourcers to being employed by the company. A company using hybrid outsourcing must carefully craft a written agreement to deal with the allocation of rights and responsibilities. The company also must establish procedures to maintain confidential documents and keep information separate.

Positions Vendors Take on Critical Issues

Stuart noted that companies also should consider the dramatic growth in subcontracting by service providers. Since vendors themselves are looking for the lowest cost providers they are more inclined to subcontract. This can raise a new set of issues for financial services companies. In entering into an outsourcing transaction, companies should consider:

- **Defining "subcontractor":** Focus on what services the potential subcontractor would provide. A subcontractor usually would not include the provider of commodities such as telecommunications services.
- **Allocating legal liability versus operational risk:** Vendors often argue that they should have free reign to subcontract since they remain responsible for the subcontractor. However, while this is true, it merely provides the customer with a legal claim. Customers likely are more interested in making sure there are no operational issues before a breach even arises and, therefore, will want more control over subcontractors.
- **Excluded services:** Consider whether there are any key services the company would not want to allow being outsourced.

- **Approval rights:** Consider whether the company has the resources to conduct a meaningful approval process. All too often companies demand approval rights over subcontractors but don't have the resources to conduct a meaningful evaluation. Approving a subcontractor without conducting meaningful diligence could put the customer on the hook for the subcontractor's failures.
- **Subcontractor agreements:** Customers may want the right to review the subcontracting agreement or provide "canned" terms the vendor must include in all of its subcontractor agreements.

Stuart also noted that vendors are pushing back against liability for data breach. Vendors are concerned they are exposed to significant risk in an area they cannot fully control. Financial services companies should, therefore, carefully examine the vendor's policies and procedures on cybersecurity to ensure the vendor has sufficient protections in place. In most cases, the company will want to apply its own requirements as well. Companies also should require, in the outsourcing agreement, that the vendor inform the company when there has been a third-party breach, even if such breach does not impact the customer directly. Companies also should review their customer agreements to understand their exposure vis-à-vis their clients and how that translates to the allocation of risk with the vendor. For example, if a client agreement insulates a company from liability, it might not need to shift liability risk to the vendor.

Contract Guidelines for Risk Management

The OCC and FRB typically did not require specific provisions or outcomes, but instead suggested companies consider the following issues in their discussions and negotiations with vendors.

Scope of Services

Jamie Talbot noted that defining the scope of services can be a tool for controlling costs and clarifying responsibilities. Vendors often seek revenue on out-of-scope services, so it is important to identify what services the vendor is expected to perform for the prices described in the agreement. A company should consider whether to include a general or specific definition of the scope of services. For specialized services, specificity in the definition of scope of services is best, but specificity also bears the risk of omission. A general approach, by contrast, provides a broader umbrella for arguing that a specific service is included. For highly specialized services, specificity is usually best. For standardized services, a more general approach can sometimes work as there is more of an industry standard for what the service is meant to include. Vendors often seek revenue on out-of-scope services; therefore, whether using a general approach or a specific approach, it is important to include a sweep's clause, which ultimately pulls into the scope of services the customary, incidental or inherent parts of providing the services described in the agreement.

A company may want to address any ancillary services, such as technology maintenance, procurement and training as part of the contract, as to avoid the vendor seeking additional fees for those services. It also is important to address access and control (including facilities, personnel, systems and customer information communication).

Performance Measures

Jamie continued the webinar by addressing performance measures in outsourcing contracts, which can provide specific criteria for evaluating vendor performance and provide tools for incentivizing vendor behavior. SLAs define specific metrics for the services. In setting SLAs, it is important to build in objective criteria that can be measured easily. The consequences for a vendor failure to meet the SLAs typically are financial credits.

Jamie noted that when structuring SLAs, there are a number of variables that a company and a vendor can use to incentivize the vendor in the appropriate areas. These include establishing Key Performance Indicators (which identify certain SLAs as the most important and are sometimes the only ones with actual associated credits), setting the size of the credits themselves and establishing at-risk amounts (which protect vendors from experiencing a significant impact on revenue).

Vendors sometimes request a regime in which they are able to earn back SLA credits or receive additional fees for exceeding SLAs. In our view, these usually do not benefit the customer, who receives no additional revenue from the improved performance. In those cases, the earnback or additional fees benefit only the vendor.

Finally, Jamie noted that companies should be careful to balance SLAs so as not to encourage the vendor to sacrifice quality for metrics. For example, a volume-based SLA can encourage the vendor to provide poor quality service in order to meet the volume commitments.

Compliance with Laws

Companies should consider that legal compliance can be among the most difficult parts of the negotiations when entering into outsourcing agreements. Vendors always will agree to comply with the law, but allocating costs and responsibility among the parties can be complicated. The parties also must address who is responsible for monitoring changes in the law, determining requirements and determining the compliance date. If costs are shifted to the vendor, it may disincentivize the vendor from devoting enough resources to ensure "best of breed" compliance. If the costs are shifted to the customer, the customer may find itself bearing unnecessary costs. The level of regulatory oversight often will drive this issue. Heavily regulated entities, like financial institutions, will be more conservative in compliance matters and should be more willing to take on additional costs and burdens to ensure compliance.

Termination Rights

Jamie explained that outsourcing negotiations also should address termination rights. Regulators advise companies to develop an exit strategy that is not overly burdensome. Termination events can include material breach, failure to comply with law, convenience, bankruptcy (or some prebankruptcy trigger), reputational harm and regulator directive. Vendors may push back on both termination for bankruptcy and reputational harm. A material breach may arise due to repeated failures to meet SLAs. Jamie noted that it is beneficial for companies to negotiate credits for both individual failures and the ability to terminate for repeated failures.

Partial termination rights can be a helpful tool for companies to address service issues. Termination of an entire contract may not be a credible threat to vendors, in light of the cost and time that would be needed to transition all of the services elsewhere. Partial termination — where only specific services are terminated while the remainder of the contract remains in place — is more realistic for the customer.

Companies may want to negotiate for partial termination rights whereby a company may terminate on a service-by-service basis. Companies also should limit the instances where vendors may terminate (usually limited to material breach by the customer). In some circumstances, customers may be required to pay a termination fee (*e.g.*, stranded costs), however, the OCC notes that these costs should not be "prohibitive."

Post Termination

After the contract expires or is terminated, the customer and vendor will still have obligations to one another. These may include providing termination assistance, returning or destroying of customer information, returning customer equipment, ongoing monitoring of the vendor to ensure compliance with these termination obligations, and implementing any provisions that may survive expiration of the agreement.

Indemnification and Liability Limitations

Jamie noted that robust indemnification obligations may help address risk, however, customers should assess carefully any customer indemnity to vendor. In outsourcing agreements, indemnity typically is limited to third-party claims, leaving the parties to negotiate specific limits on liability for claims solely between the two of them. Vendor indemnity for third-party claims for breach of agreement should be carefully negotiated as not to undermine any liability caps. Vendor indemnity for violations of law should be drafted in light of which party has retained responsibility for determining compliance with law issues.

Ultimately, any limits on vendor liability should be commensurate with the risk faced by the customer. Companies should keep in mind that capping liability at the cost of the contract might not adequately cover the risk to the customer. Some consequential damages exclusions also may be appropriate for critical issues like data recovery, confidentiality and reputational harm.

Audit

Jamie also addressed audit issues and noted that maximum flexibility is more critical than ever in light of heightened regulatory scrutiny. Typically, vendors will not push back, with certain key exceptions for caps on audit hours, access to materials and access to subcontractors.

Transition Planning

Stuart concluded the webinar with an overview of post-term transition planning. He emphasized that it is best for companies to create a transition plan for their outsourced services before it becomes necessary. All too often, the issue is put on the back burner and never addressed. Some key considerations for transition planning include: whether the company can terminate certain services and how that would impact service levels and fees; requiring the vendor to cooperate with the company and its new vendor; and which party bears the cost of transition services. Stuart noted that given the importance of transition services, companies increasingly are willing to pay for these services — even if they terminated for breach by the vendor — to ensure that the transition services are provided correctly and at the highest level.