Reprinted with permission from ACC Docket

30-SECOND SUMMARY The Federal Reserve and the Office of the Comptroller of the Currency (OCC) have issued extensive new guidance to financial institutions about the use of third parties to perform functions for the institution. Service providers seeking to do business with financial institutions should understand that compliance with agency standards will be an important element in any successful effort to enter into a relationship with their potential customers. Service providers should assess their operations through the lens that would be applied if the services were performed by an internal bank department, structured to satisfy the governance and risk management standards, which regulators would expect if the bank had not outsourced the activities.

NEW REGULATORY EXPECTATIONS

FOR SERVICE PROVIDERS TO FINANCIAL INSTITUTIONS

By Andrew Ting and Paul Rothstein

With the push for greater risk management by US federal regulators since the 2008 financial crisis, relevant agencies have significantly increased their scrutiny of financial institution service providers. The Federal Reserve and the Office of the Comptroller of the Currency (OCC) have issued extensive new guidance to financial institutions[1] about the use of third parties to perform functions for the institution or company, or to provide products or services to their customers (collectively, "service providers"). Service providers seeking to do business with financial institutions should understand that compliance with agency standards will be an important element in any successful effort to enter into a relationship with their potential customers.

A key principle embodied in the guidance is the expectation that a service provider will comply with and conform to the standards that would be applicable if the financial institution were conducting the activity directly. Thus, as financial institutions implement these new standards, they will require additional guarantees regarding the qualifications and quality of service provider operations. The guidance also emphasizes quality of the initial and on-going diligence of the financial institution deciding to use a third party to perform a function for the institution. This requirement translates into both more rigor from institutions when entering into relationships with third-party service providers, and enhanced on-going diligence through the course of the relationship. This article provides an overview of the key expectations contained in the Federal Reserve and OCC guidance, and will help service provider in-house counsel to establish, maintain and/or enhance their companies' relationships with financial institutions.

In the last quarter of 2013, the Federal Reserve and the OCC issued guidance concerning their expectations for commercial relationships between financial institutions and their service providers. On Oct. 30, 2013, the OCC issued "Third-Party Relationships: Risk Management Guidance" (OCC Bulletin).[2] On Dec. 5, 2013, the Federal Reserve issued "Guidance on Managing Outsourcing Risk" (the Federal Reserve Guidance).[3] The OCC Bulletin and the Federal Reserve Guidance affect not only financial institutions supervised by those regulators, but also service providers to those financial institutions. The OCC Bulletin broadly defines service providers to include providers of "tax, legal, audit, or information technology operations ... third parties that subcontract activities to other foreign and domestic providers," as well as other third parties that assist financial institutions to comply with applicable laws or regulations. Similarly, the Federal Reserve Guidance notes that financial institutions may subcontract activities such as accounting, appraisal management, internal audit, human resources, sales and marketing, loan review, asset and wealth management, procurement and loan servicing.

Service providers as outsourced bank departments

Service providers and financial institutions should not think of service providers simply as external entities; instead, in order to meet federal regulatory expectations, both should consider the full system of output of information and deliverables. In other words, they should assess their operations through the lens that would be applied if the services were performed by an internal bank department. They should structure the relationship to satisfy the governance and risk management standards, which regulators would expect if the bank had not subcontracted the activities.

This perspective may surprise service providers that mostly serve industries less regulated than the financial sector. However, the OCC Bulletin notes that the OCC "generally has the authority to examine and to regulate the 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."[4] Therefore, a service provider to a financial institution must think in terms of the compliance, quality assurance, risk management, governance and audit functions that would be expected for its financial institution client. The extent of these undertakings will depend on the nature and dimensions of the outsourced service, and how critical that function is to the operations of the outsourcing institution. A multinational financial institution may have more complex operations that require more risk management by a service provider, but even services performed for a smaller community bank may require more scrutiny if they are critical to that bank's operations.

Consequently, service provider counsel should prepare their clients for the possibility of both heightened requirements by their clients and examinations by regulators who will probe whether the outsourced activity meets regulatory standards. Similarly, by proactively addressing the new guidance, financial institution counsel can improve vendor relationships, operations and regulatory review. Financial institutions may accomplish the foregoing by alerting service providers, particularly those without a significant financial industry background, to increased OCC and Federal Reserve scrutiny.

The OCC Bulletin emphasizes the shared responsibility of financial institutions and service providers to proactively address regulatory expectations during each phase of their business relationship. These eight phases are:

1. planning;
2. due diligence and objective third-party selection;
3. contract negotiation;
4. on-going auditing and monitoring;
5. termination;
6. oversight and accountability;
7. documentation and reporting; and
8. independent reviews to align the bank's strategy and manage risks.

Throughout the life cycle of the contract, the OCC emphasizes a number of themes, including the following: analysis and risk assessment, objectivity, responsibility, continuing oversight, security and compliance. The Federal Reserve Guidance also calls out the importance of risk assessments, due diligence, contract negotiation and oversight, as well as incentive compensation and business continuity plans. In order to address the issues raised by the OCC Bulletin and Federal Reserve Guidance, the discussion below follows the eight phases from the OCC Bulletin, weaving in additional nuances from the Federal Reserve Guidance when appropriate.

Andrew Ting is a deputy general counsel with Promontory Financial Group, LLC, where he provides legal advice for Promontory's worldwide operations, including compliance, technology and contract matters. *ating@promontory.com*

Paul Rothstein is a technology lawyer and consultant with Promontory Financial Group, LLC. *prothstein@promontory.com*

The extent of due diligence conducted on a service provider should be commensurate with the criticality and risks posed by the service provider's activities.

Planning

The OCC expects financial institutions to engage in extensive planning to determine how to enter into a service-provider relationship. Such planning requires the use of objective criteria to evaluate how the institution's initiatives, customers and policies will be affected by the service provider's performance. In order to help a financial institution evaluate the service provider's performance, a service provider should be prepared to proactively address the quality of its compliance and operations in performing the services for its other clients. This is both good compliance and good business, because offering qualitative customer references and quantitative metrics, such as service levels in pitch materials, may determine which provider is selected to perform the services.

Service providers that have relied in the past on good relationships to win business should, as a result of regulatory expectations in the planning phase, expect heightened questions from financial institutions. In many institutions, procurement officers may have had significant autonomy to select service providers. As an added layer of complexity, the new regulatory guidance will likely result in additional levels of legal and compliance review. Financial institution senior management in risk management and compliance may become more closely involved in service-provider selection. Indeed, the OCC Bulletin expresses an expectation that a financial institution's board of directors will have to approve critical activities, which include functions that significantly impact customers or that are high risk, costly or operationally significant. Service providers should expect that these additional levels of review will increase the time and effort needed to establish a new relationship with a financial institution; both service providers and their prospective clients should build these expectations into their anticipated timelines. As noted above, proactively demonstrating compliance and the best value-add approach will help in the selection of service providers and ease of engagement.

Due diligence and objective third-party selection

The OCC sets out 16 due diligence considerations for service providers to financial institutions:

- strategies and goals;
- information systems management;
- conflicting arrangements with other parties;
- incident reporting and management programs;
- financial condition;
- resilience/business continuity;
- business experience and reputation;
- physical security;
- fee structure and incentives;
- human resource management;
- qualifications of company principals;
- reliance on subcontractors;
- risk management;
- insurance coverage;
- information security; and
- legal and regulatory compliance.

These factors highlight the importance of stability from different perspectives — the financial condition and incentives of the service provider, the quality of its management and personnel, and the organizational and technical safeguards that the service provider implements for the protection of its business and its clients. The extent of due diligence conducted on a service provider should be commensurate with the criticality and risks posed by the service provider's activities. The OCC states that a "bank should not rely solely on experience with or prior knowledge of the third party as a proxy for an objective, in-depth assessment of the third party's ability to perform the activity in compliance with all applicable laws and regulations and in a safe and sound manner."

Service provider counsel should expect questions relating to all of these factors. The level of detail will vary depending on the significance of the activity, and the types of information requested may well evolve over time. For example, as federal agencies issue new regulations for different sectors, such as mortgages and consumer debt, service providers should expect questionnaires relating to their adherence to applicable regulations. Resistance to such inquiries and delays in satisfying the concerns raised by such inquiries could well result in a lengthened sales cycle and, potentially, loss of a customer.

The Federal Reserve Guidance specifically suggests that service providers should be prepared to respond to the following diligence requests: the background and reputation of the service provider and its principals; specific background checks of its employees; customer references; verification of licenses and certification; review of the service provider's financial condition. In order to facilitate the financial institution's review of the service provider's operations and internal controls, it is prudent for service providers to also maintain third-party audit reports, such as SSAE 16 and SOC 3 internal control reports.[5]

Service providers can drive efficiency by using the equivalent of a central portal accessible to its financial institution clients, with frequently asked

questions and transparent reports that proactively address expected diligence requests. Feedback on the value of this information can help service providers to continually improve their operations.

Contract negotiation

The OCC Bulletin and Federal Reserve Guidance devote substantial attention to optimal contract terms. Service provider counsel outside the government contracts area may not be familiar with external government requirements that closely affect commercial contract terms. However, service providers to financial institutions should understand the following regulatory expectations for their service provider contracts:

Form. Service providers and financial institutions should make agreements explicit, clear in scope and purpose, and in a written, mutually agreed contract. Oral agreements or any kind of "handshake" deal increases the risk for non-compliance and are considered insufficient.

Performance measures. The two regulators recommend measurable performance standards based on industry standards to motivate performance. Depending on the nature of the service being provided, service providers may want to consider modifying their form contracts to provide for service level agreements (SLAs), which are already quite common in telecommunications and technology agreements. SLAs in technology agreements for financial institutions often require a certain percentage of service availability; such percentages are quite often above 99 percent. SLAs for technical support may include required response times for different levels of emergencies. Of course, not all services are amenable to quantifiable performance measures, and the OCC notes that standard measures may not be appropriate for more customized services. Such customized services may include consulting services involving qualitative aspects of a financial institution. In addition to SLAs, technology service providers may want to consider implementing customer "dashboards." Such dashboards can give financial institution customers real-time metrics about system operation, if such metrics are provided for the benefit of information sharing and do not imply any additional obligations or information contrary to the contract.

Record-keeping requirements. Financial institutions will ask their service providers to provide accurate and comprehensive information and reports related to the services. Anti-money laundering and similar transactional compliance services may result in more in-depth record-keeping requirements. The OCC specifically notes that contracts with third parties should contain provisions acknowledging that the OCC may examine applicable information in the hands of service providers in the same manner that it can examine the records and operations of financial institutions.

Termination provisions. The regulators expect that contracts contain clear and detailed termination provisions. The OCC Bulletin states that contracts with financial institutions must include a provision that the OCC can direct the termination of a contract between a service provider and the financial institution without penalty. Financial institutions will likely request that service providers provide transition services to any replacement providers or to the institution itself upon contract termination. Such terms may include data delivery and relevant support services to the replacement provider. Service providers will want to consider the following issues: length of transition period, reimbursement for transition costs, and cooperation among the parties during transition. Even if a servicer generally resists extensive transition services, it should be prepared for its financial institution clients to pay more attention to those provisions.

Notification. Service providers can expect to receive requests for notification on the occurrence of service disruptions, security breaches, changes in employment or management, or corporate organizational changes. The OCC and Federal Reserve clearly believe that a financial institution's board of directors cannot relieve itself of responsibility by simply outsourcing a service to a third party. Notification of service provider-status changes is a key part of a financial institution's oversight of the service provider. Service providers would be well served to implement internal controls to identify applicable disruptions or changes and to promptly inform their financial institution customers of any issues.

Audits. If you have had any experience in this sector, then you will not be surprised to learn that the OCC stresses the financial institution's right to receive the results of the service provider's financial, security and other audits. Service providers should be prepared to receive requests for the results of such audits.

Compliance with law. Service providers can expect requests to comply with all applicable laws and with specific representations for compliance with anti-money laundering and privacy laws. Financial institutions may request the right to monitor compliance with such laws on an on-going basis. Given the breadth of US federal, state, and international banking laws and regulations, counsel will have to consider the specific services to be provided to determine applicable laws and regulations. For example, compliance with international bank secrecy and data privacy laws may affect how service providers structure their performance of services, obtain needed certifications, and establish appropriate policies and procedures..

Price allocation. Regulators expect contracts to identify provisions that

Due to the highly confidential nature of banking information, confidentiality agreements are consistently used on a global scale and will focus, in particular, on strong protections for personally identifiable information of customers.

could provide inefficient or unethical financial incentives by the service provider. The Federal Reserve notes that "[a]n example of an inappropriate incentive would be one where variable fees or commissions encourage the service provider to direct customers to products with higher profit margins without due consideration of whether such products are suitable for the customer."

Intellectual property and related matters. Ownership of intellectual property is important in any relationship in which IP is being created, licensed or transferred. The Federal Reserve and OCC indicate that the contract between a service provider and a financial institution should address ownership of technology and bank records, and, for software licensors, escrow of source code. Source code escrow arrangements concern licensors because third parties may use software source code to replicate the software or create unauthorized modifications or enhancements; licensors commonly refer to source code as their "crown jewels." Service providers should be prepared for requests for source code escrows.

Confidentiality. Due to the highly confidential nature of banking information, confidentiality agreements are consistently used on a global scale and will focus, in particular, on strong protections for personally identifiable information of customers. Such protections will include provisions relating to the destruction or return of such information. The Federal Reserve specifically notes the requirement to comply with the FFIEC IT Examination Handbook,[6] as well as the customer security regulatory standards established pursuant to Gramm-Leach-Bliley Act § 501(b). The Federal Reserve Guidance notes the following: "These measures should be mapped directly to the security processes at financial institutions, as well as be included or referenced in agreements between financial institutions and service providers." The service provider should seek to work with the financial institution's IT security personnel to ensure that security processes are appropriately mapped to the requirements of the applicable service.

Business continuity. A business continuity plan summarizes an organization's preparations to maintain services during any potential disruption, including natural disasters, terrorist attacks, technical outages and similar occurrences. The Federal Reserve Guidance states that financial institutions should ensure that the service provider has an adequate and effective business continuity plan aligned to the financial institution's operations. Both the financial institution and the service provider should also document roles and responsibilities for maintaining and periodically testing the service provider's business continuity plans. As a result of these regulatory expectations, financial institutions may request a service provider's business continuity plans during the due diligence phase.

Indemnification and limitation of liability. Counsel should be prepared to deal with the separate issues of indemnification and limits on contractual damages. Indemnification relates to claims by entities not subject to the agreement. A contract could provide for indemnification if a third party sues a financial institution for intellectual property infringement based on the technology provided by the service provider. A cap on damages relates to breach of the agreement by the parties to the agreement. A limitation of liability provision may address limits on indemnification or contractual damages, or both. Additionally a limitation of liability provision may address the forms of contractual damages, such as consequential damages, incidental damages and punitive damages, that may be available under the contract.

Both regulators identify indemnification by the service provider of the financial institutions as an important issue. Service providers can expect to receive requests for indemnification resulting from failure to obtain all necessary intellectual property licenses.

The OCC states that any limitation of liability should be proportional to the bank's potential loss. The Federal Reserve Guidance notes that service providers may want to contractually limit their liability, and that such a limitation of liability should be reviewed to determine whether it is reasonable. While service providers can be expected to limit their own liability, they should expect resistance from both their customers and regulators if they limit liability to a low amount or attempt to disclaim all damages.

Insurance. Service providers can expect to receive requests for certificates of insurance and notifications of changes to insurance coverage. The types of insurance required by financial institutions vary considerably but may include commercial general liability, umbrella liability, errors and omissions (E&O), workers compensation, employee dishonesty and automobile insurance. Also, various institutions may have different coverage requirements. Financial institutions may also request to be listed as an additional insured on the service provider's certificates of insurance. Service providers should maintain current lists of insurance policies, including material terms of such policies.

Dispute resolution. The OCC and the Federal Reserve both encourage deliberation between the financial institution and the service provider regarding an appropriate dispute resolution clause. Service provider counsel should consider implementing internal executive escalation procedures as a precursor to litigation. Counsel may also wish to consider the merits of expedited alternative dispute resolution.

Customer complaints. Both the OCC and the Federal Reserve expect financial institutions to be aware of customer complaints received by their service providers, and to assure that appropriate service mechanisms are in place to assist individual customers and identify systemic customer service problems. If the service provider handles customer complaints, then the contract may include service levels for timely customer response and providing summary reports to the financial institution that track the status and resolution of complaints.

Subcontracting. Both regulators discuss the issue of a financial institution's oversight of subcontracting by service providers. The primary service provider should still have overall accountability for all services that its subcontractors provide to the financial institution.

Foreign law. Both regulators note the variability of local law when using foreign service providers. The Federal Reserve states, "financial institutions should consider the authority or ability of home country supervisors to gain access to the financial institution's customer information while examining the foreign service provider." Service provider counsel should analyze the laws of applicable jurisdictions. In particular, service providers dealing with personally identifiable information should consider the laws of the jurisdiction where the information is generated, as well as the jurisdiction where the service occurs. For example, a service provider may be sanctioned if it exports personal data outside a jurisdiction without following that jurisdiction's privacy requirements.

On-going monitoring

Outsourcing a financial institution's function does not remove the institution's responsibility for overseeing the service provider performance. The institution will also need to devote additional attention to critical activities, and the obligation to monitor a service provider includes the obligation to consider periodically if an outsourced service becomes critical in nature. A change in criticality, even after the contract is signed, will necessitate heightened service provider responsiveness to additional bank scrutiny. Service providers should view the monitoring phase as a continuation of the due diligence phase. Institutions, for example, may insist on periodic on-site visits to service provider facilities by the bank and its regulators to validate that regulatory expectations for the services performed are being fulfilled.

Termination

The Federal Reserve notes that financial institutions should maintain an exit strategy, including a pool of comparable service providers, in the event that a contracted service provider is unable to satisfactorily perform its obligations. The OCC notes the following issues to consider with respect to contract termination:

- expiration or satisfaction of the contract;
- breach of contract;
- desire to seek an alternative third party;
- desire to bring the activity in house; and
- desire to discontinue the activity.

The first two terms are standard for any commercial contract. If a contract term is completed, or if the terms specified in the contract are satisfied, the contract naturally terminates. If a party breaches a contract and does not cure the breach, commercial contracts and contract law provide for damages for that breach.

The last three termination types specified are different variants of termination for convenience. Such provisions, which do not necessarily correlate with a service provider's performance, may result in extensive negotiation regarding termination payments to a service provider and the service provider's responsibility to perform transition services to assist the replacement service provider. In any negotiation between

ACC EXTRAS ON… Third-party relationships

ACC Docket
Storm Clouds Ahead? What Every Cloud Service Provider Should Know (Nov. 2012).
www.acc.com/docket/storm_nov12

Quick Reference
Third-Party Essentials: A Reputation/Liability Checkup When Using Third Parties Globally (Jun. 2012).
www.acc.com/quickref/third-party_jun12

Form & Policy
Third-Party Confidential Information Handling Procedures (Jun. 2009).
www.acc.com/form/third-party_jun09

Presentation
Managing Risks in Third-Party Relationships (Jun. 2013).
www.acc.com/third-party_jun13

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT *WWW.ACC.COM*, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

a financial institution and a service provider that involves termination for convenience, counsel may wish to consult with in-house accounting departments to determine the effect of such terms on revenue recognition; termination for convenience may result in changes to revenue recognition that can change the underlying economics of the transaction and the associated pricing. The "contract negotiation" section above addresses other business considerations for termination provisions.

Oversight and accountability

The OCC identifies separate roles and responsibilities for a bank's board of directors, senior bank management and bank employees who directly manage third-party relationships. For example, the board of directors should monitor the overall third-party risk management process. Not surprisingly, the OCC expects bank employees who directly manage third-party relationships to focus on day-to-day activities and to escalate problems as appropriate. Senior bank management has intermediate responsibilities, including supervising employees with direct authority over service providers and escalating critical issues to the board of directors (or a board-level committee). Therefore, service providers can expect interactions with different levels of management based on the criticality of the service. Providers of large-scale services to financial institutions should consider designating specific employees to manage the customer relationship and provide data. Such employees can enhance the transparency, responsiveness and accountability expected by financial institutions and the federal financial institution regulators, and have enough seniority to effectively and efficiently address performance issues when they arise.

Documentation and reporting, and independent review

The final two phases are closely related to each other and the "oversight and accountability" phase. Service providers must cooperate with a bank's on-going collection and review of information about the service provider and the performance of the services. Such review and evaluation of the service provider's performance should include the involvement of the bank's independent auditors, when appropriate, to ensure objective analysis of factors such as performance, conflicts of interest and adequate staffing. Accordingly, a service provider that performs services for multiple financial institutions should be prepared to cooperate with a review of its performance by each financial institution, each financial institution's independent auditor and each financial institution's regulators.

Heightened risk management for specific service providers

In addition to the eight phases of the relationship between a financial institution and a service provider from the OCC Bulletin, the Federal Reserve specifically identifies four types of service providers that merit additional risk analysis:

- organizations that generate suspicious activity reports (SARs), who must comply with the Bank Secrecy Act;
- foreign-based service providers, who must comply with applicable US laws, regulations and regulatory guidance;
- outside professionals who perform work that has been traditionally carried out by internal auditors; and
- providers of risk management services, who should provide information that explains the product components, design and intended use, to determine whether the products and/or services are appropriate for the institution's exposures and risks.

Counsel for service providers face new challenges as their financial institution clients work to comply with OCC and Federal Reserve risk management guidance for service provider relationships, and the new expectations for their clients translate into new expectations for the service providers. Accordingly, counsel for service providers should be prepared to help their companies implement contractual arrangements, transparent reporting and enhanced governance, to ensure that services performed for financial institution clients fulfil both the clients' needs and its regulator's expectations. **ACC**

NOTES

1 The OCC guidance applies to national banks and federal savings associations. The Federal Reserve guidance applies to state banks that are members of the Federal Reserve System, bank, and savings and loan holding companies (including their non-bank subsidiaries), and US operations of foreign banking organizations. For purposes of this article, "financial institution" refers to all of the entities covered by either the OCC or Federal Reserve guidance.

2 Office of the Comptroller of the Currency Bulletin 2013-29, Risk Management Guidance, available at *www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html* (Oct. 30, 2013).

3 Board of Governors of the Federal Reserve System, Guidance on Managing Outsourcing Risk, available at *www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf* (Dec. 5, 2013).

4 Sources of this authority include 12 USC § 1867(c) and 12 USC § 1464(d)(7).

5 Further information about the SSAE 16 standards and SOC 3 reports is available at the American Institute of Certified Public Accountants (AIPCPA) website, *www.aicpa.org*.

6 Federal Financial Institutions Examination Council, IT Examination Handbook, available at *http://ithandbook.ffiec.gov/it-booklets/information-security.aspx (2006).*