THE REVIEW OF
BANKING & FINANCIAL SERVICES
A PERIODIC REVIEW OF SPECIAL LEGAL DEVELOPMENTS AFFECTING LENDING AND OTHER FINANCIAL INSTITUTIONS

Vol. 20 No. 9 September 2004

OUTSOURCING BY FINANCIAL INSTITUTIONS: A SURVEY OF REGULATORY GUIDANCE

The Emerging Regulatory Consensus is that Management of Outsourcing Risks Requires Financial Institutions to Assess Those Risks, Perform Due Diligence of Service Providers, Require Protective Contract Terms, and Perform Ongoing Oversight and Monitoring. The Authors Discuss These Requirements.

By Andrew L. Sandler, Anand S. Raman and Valerie L. Hletko*

Outsourcing by U.S. financial institutions is rapidly increasing, as flexibility and cost savings drive information technology, accounting, audit, electronic funds transfer, investment management and human resources into lower wage, generally overseas, labor markets. Within the next five years, for example, Deloitte Consulting, LLP, estimates that $356 billion B or 15% B of the financial service industry's current cost base will move offshore.

This trend towards outsourcing, and the associated reduction in domestic employment, has moved the topic into a central place in the national debate, with presidential candidates, congressmen and B increasingly B bank regulatory agencies staking out positions on the issue. For instance, it was reported earlier this year that California Senator Diane Feinstein had written to the Office of the Comptroller of the Currency, expressing concern about compliance with financial privacy laws in outsourced operations. Senator Feinstein also reportedly requested that the OCC provide information about the number of contractors it had audited and how many examiners it has assigned to monitor overseas operations. For its part, the OCC has stated that it has the right to examine banks' outsourcing arrangements, even where they are conducted by entities regulated by foreign governments.[1]

*ANDREW L. SANDLER *is senior partner,* ANAND S. RAMAN *is counsel, and* VALERIE L. HLETKO *is a member of the Consumer Financial Services and Enforcement Practice in the Washington, D.C. Office of Skadden, Arps, Slate, Meagher & Flom LLP. The authors are actively involved in the creation of compliance and risk management programs and the defense of financial institutions in government enforcement and class action litigation. Their email addresses are, respectively,* asandler@skadden.com, araman@skadden.com, and vhletko@skadden.com.

1. OCC Bulletin 2002-16: Bank Use of Foreign-Based Third-Party Service Providers (May 15, 2002), at 5-6.

IN THIS ISSUE

● ***Outsourcing By Financial Institutions: A Survey of Regulatory Guidance***

With this atmosphere of political pressure as well as the increasing visibility of outsourcing, it is highly likely that bank regulatory agencies will intensify their reviews of outsourced financial services operations in the near future. Financial institutions, for their part, would be well served by conducting self-assessments of their outsourced operations in view of regulatory guidance on key issues.

This article surveys the principal bank regulatory guidance on outsourcing. We focus on the principal recent pronouncements by the OCC, Federal Reserve Board ("FRB"), Office of Thrift Supervision ("OTS"), Federal Deposit Insurance Corporation ("FDIC"), National Credit Union Administration ("NCUA") and Federal Financial Institutions Examination Council ("FFIEC"). We also reference several informational "white papers" authored by members of these agencies' staffs, which while not necessarily expressing the agencies' official views, are nonetheless instructive.

Although this area is rapidly developing, there appears to be an emerging regulatory consensus that the critical areas in managing outsourcing risk are:

(i) proper risk assessment;

(ii) service provider due diligence and selection;

(iii) appropriate contract terms; and

(iv) proper ongoing oversight and monitoring of service providers.[2]

A further point stressed by the regulatory agencies is that controls over outsourced operations be "equivalent to those that would be implemented if the activity were conducted internally."[3] These topics are discussed in turn below.

RISK ASSESSMENT

The regulatory agencies are in agreement that outsourcing presents myriad risks B and that the responsible management of outsourcing relationships begins with an understanding and measurement of those risks.[4] As the FDIC has stated, "Institutions and their customers can achieve benefits through outsourcing of products and services. However, responsibility for managing the risks associated with those products cannot be outsourced."[5]

2. FFIEC, Risk Management of Outsourced Technology Services (November 28, 2000), at 3 ("FFIEC, Risk Management"); OCC Bulletin 2001-8: Guidelines Establishing Standards for Safeguarding Customer Information (February 15, 2001), at 1 ("OCC Bulletin 2001-8").
3. FRB, SR 00-4 (SUP), Outsourcing of Information and Transaction Processing (February 29, 2000), at 2.
4. FDIC, FIL-81-2000: Risk Management of Technology Outsourcing (November 29, 2000), at 1 ("FIL 81-2000); OCC Bulletin 2001-8, at 6.
5. FIL 81-2000, at 1.

Standard & Poor's

The Review of Banking & Financial Services is a periodic supplement of the *The Review of Securities & Commodities Regulation,* which is published 22 times a year by Standard & Poor's, a division of The McGraw-Hill Companies. Executive Office 55 Water Street, New York, New York 10041. Editorial Office, 299 Park Avenue 16th floor, New York, New York 10171. Subscription rates: $1075 per year in U.S., Canada and Mexico; $1140 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and universities. For subscription information and customer service, please call (800) 852-1641. General Editor: Michael O. Finkelstein. Associate Editor: Sarah Strauss Himmelfarb. ISSN: 1051-1741. Information has been obtained by *The Review of Banking & Financial Services* from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, *The Review of Banking & Financial Services* does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or for the results obtained from the use of such information.

The McGraw-Hill Companies

Indeed, "[w]ithout an effective risk assessment phase, outsourcing technology services may be inconsistent with the institution's strategic plans, too costly, or introduce unforeseen risks."[6] On the other hand, "[n]o single system is ideal for every bank," and the degree and formality of the risk assessment may turn on the extent of the outsourcing relationship and the size of the financial institution.[7] Finally, as discussed below, foreign-based service providers present special risks, and therefore require a particularly intense risk assessment.[8]

Strategic Risk

Financial institutions are exposed to strategic risk B "the risk from adverse business decisions or improper implementation of those decisions" B to the extent that they rely on third parties "without fully performing due diligence reviews or implementing the appropriate risk management infrastructure."[9] Therefore, prior to entering into any outsourcing arrangement, and particularly one involving foreign outsourcing, a financial institution must evaluate a service provider's ability to meet its needs.

In the case of overseas outsourcing, financial institutions are well-advised to evaluate the foreign jurisdiction's laws, regulatory requirements, local business practices, accounting standards and legal environment. Such an evaluation should take into account the parties' respective responsibilities to respond to regulatory changes that could impair fulfillment of any contractual term.[10]

Country Risk

The risk to financial institutions is magnified to the extent that their third-party service providers are located overseas. Because of this risk, some agencies B such as the OTS B require regulated entities to notify them in advance prior to establishing a relationship with a foreign service provider.[11]

One element of risk in connection with foreign outsourcing is "country risk," which is "the risk that economic, social, and political conditions and events in a foreign country might adversely affect a bank's financial interests."12 Such risk, it has been noted, can have an "overarching effect on a bank's international activities."[13] Consequently, a financial institution must evaluate and continuously monitor country risk B and have "appropriate contingency plans and exit strategies" in the event of adverse material changes in the risk level.[14]

As part of the initial evaluation of a service provider, a financial institution should have an accurate system for reporting country exposures, a country risk rating system, established country exposure limits, regular monitoring of country conditions, periodic stress testing of foreign exposures, and adequate internal controls and audit functions.[15] Following selection of a service provider, a financial institution "must closely monitor foreign government policies and political, social, economic and legal conditions in countries where it has a contractual relationship with a service provider."[16]

Compliance Risk

The regulatory agencies have stressed that the use of a foreign-based service provider must not impair compliance with applicable U.S. laws and regulations or the agencies' ability to monitor it. These include requirements concerning accessibility and retention of records, such as the Bank Secrecy Act, 12 U.S.C. 1867(c), the national sanctions and embargo programs of U.S. Treasury's Office of Foreign Assets Control, and applicable consumer protection laws and regulations.[17]

Although compliance risk applies to all aspects of a service provider's activities, regulatory agencies have stressed

6. FIL 81-2000, at 1.
7. OCC Bulletin 2001-47: Third-Party Relationships (November 1, 2001), at 2 ("OCC Bulletin 2001-47").
8. See, *e.g.*, OCC White Paper: Cross-border outsourcing and risk management for banks (August 13, 2003) ("OCC White Paper").
9. OCC Bulletin 2001-47, at 4.
10. OCC White Paper.
11. OTS, Thrift Bulletin 82: Third-Party Arrangements (March 18, 2003), at 5.
12. FDIC FIL-23-2002: Country Risk (March 11, 2002), at 1 ("FDIC FIL-23-2002); OCC Bulletin 2002-16: Bank Use of Foreign-Based Third-Party Service Providers (May 15, 2002), at 2 ("OCC Bulletin 2002-16"); OCC Bulletin 2001-47.
13. FDIC FIL-23-2002, at 1.
14. OCC Bulletin 2002-16, at 2.
15. FDIC FIL-23-2002, at 1; OCC Bulletin 2002-10: Country Risk (March 11, 2002); OTS, Thrift Bulletin 82: Third-Party Arrangements (March 18, 2003) ("TB 82").
16. OCC Bulletin 2002-16, at 2.
17. OCC Bulletin 2002-16, at 2-3.

the need for special vigilance with respect to the "privacy of consumer and customer records."[18] Moreover, special care should be taken to ensure that a foreign country's laws do not conflict with any U.S. privacy laws or regulations.[19]

Reputational Risk

Finally, outsourcing presents substantial reputational risks.[20] This risk is especially acute where a service provider's employees interact directly with the financial institution's customers, such as in customer call centers, often appearing as if they worked for the financial institution itself.[21]

Despite a financial institution's best efforts, some of these risks may be difficult to control. "For example, if the service provider has a highly visible problem with one client institution, the adverse publicity of that situation may have contagion effects for other client institutions."[22] This reputational risk highlights the importance of having a careful service provider selection process B as discussed in the section that follows.

SELECTION AND DUE DILIGENCE OF OUTSOURCE PROVIDERS

As discussed above, the regulatory agencies stress the importance of risk evaluation prior to entering into an outsourcing relationship.[23] After conducting such an evaluation, a financial institution may move forward with selecting a service provider. The regulatory agencies, however, have stressed that financial institutions must exercise appropriate due diligence in selecting a third party to perform services on its behalf.[24]

Such due diligence includes, among other things, evaluation of the service provider's technical and industry expertise, operations and controls, and financial condition.[25] It may also include a review of the adequacy of the service provider's insurance provisions and privacy protections.[26] Finally, due diligence "includes probing for information on intangibles, such as the third party's business strategies and goals . . . [and] service philosophies."[27]

Technical and Industry Expertise

Before entering into any outsourcing relationship, a financial institution must ensure that the service provider has sufficient expertise.[28] Among the issues the financial institution should evaluate are the service provider's systems and experience in performing the anticipated functions.[29] The financial institution should also ensure that the service provider has the ability to respond to service disruptions.[30] Special scrutiny should be given to the extent a service provider itself proposes to outsource any functions.[31]

The regulatory agencies encourage on-site visits prior to the selection of a service provider.[32] Among the topics that should be explored is the service provider's "knowledge of the regulations that are relevant to the services that they are providing," such as consumer privacy laws and the Bank Secrecy Act.[33]

Operations and Controls

In evaluating operations and controls, financial institutions are encouraged to look at a service provider's facilities management and security provisions, and the manner in which it performs employee background checks.[34] Consideration should also be given to whether the service provider maintains adequate security, including firewalls, encryption and customer identity authentication.[35] In this regard, a financial institution should evaluate previous audit reports of the servicer's operations and controls.[36]

18. OCC Bulletin 2001-47, at 5.
19. OCC Bulletin 2002-16, at 3.
20. Federal Reserve Bank of New York White Paper: "Outsourcing Financial Services Activities: Industry Practices to Mitigate Risks" (August 29, 1999), at 6 ("FRBNY White Paper").
21. OCC Bulletin 2001-47, at 4.
22. FRBNY White Paper, at 6.
23. TB 82, at 9.
24. FIL 81-2000, at 2; OCC Bulletin 2002-16, at 3.
25. FFIEC, Risk Management, at 6-7; FIL 81-2000, at A-1.
26. NCUA Letter to Credit Unions No. 01-CU-20: Due Diligence over Third-Party Service Providers (November 2001).
27. OCC Bulletin 2001-47, at 9.
28. FIL-81-2000, at A-1.
29. FIL-81-2000, at A-1.
30. FFIEC, Risk Management, at 6.
31. TB 82, at 10.
32. FFIEC, Risk Management, at 6.
33. FFIEC, Risk Management, at 7.
34. FFIEC, Risk Management, at 7.
35. FFIEC, Risk Management, at 7; FIL-81-2000, at A-1; OTS, Thrift Activities Handbook; Section 341, Technology Risk Controls.
36. FIL891-2000, at A-1.

Financial Condition

The review of a service provider's financial condition includes an assessment of any available financial statements as well as consideration of how long the service provider has been in business. The financial institution should also consider the service provider's market share and assess the "significance of the proposed contract on the service provider's financial condition."[37]

In addition, the financial institution should evaluate whether the proposed service provider has sufficient financial capacity to make investments in the technology needed to function at an acceptable level and ensure the proper implementation of consumer protections such as information security.[38]

CONTRACT ISSUES

After selecting a potential service provider and completing the due diligence process, a financial institution will enter into a written contract with a service provider. The regulatory agencies have indicated that care must be taken in drafting this document. In particular, an outsourcing contract should adequately document the scope of service, should contain adequate performance standards, should provide for security and confidentiality, should require adequate controls, and should provide for periodic reporting and audit.[39]

As one agency has noted, "[t]he written contract between the institution and the service provider should clearly specify, at a level of detail commensurate with the source and risks of the outsourced activity, all relevant terms, conditions, responsibilities, and liabilities of both parties."[40] In addition, financial institutions are encouraged to use service level agreements B "contractually binding clauses documenting the performance standard and service quality agreed to by the bank and service provider."[41]

37. FIL-81-2000, at A-2; FFIEC, Risk Management.
38. FFIEC, Risk Management, at 7.
39. FFIEC, Risk Management, at 8-10; OCC Bulletin 2001-8, at 10.
40. FRB, SR 00-4 (SUP), Outsourcing of Information and Transaction Processing (February 29, 2000), at 2 ("SR 00-4 (SUP)").
41. FDIC, FIL-50-2001: Bank Technology Bulletin: Technology Outsourcing Information Documents app. (June 4, 2001) (Tools to Manage Technology Providers' Performance Risk: Service Level Agreements). According to the FDIC, this document is for "informational purposes only and should not be considered examination procedures or official guidance."

Financial institutions should keep their regulatory agency well informed of any contracts with third-party service providers. FDIC-supervised institutions, for example, are required to notify their regulatory agency in writing of certain outsourcing agreements, as defined in Section 3 of the Bank Service Company Act.[42] Likewise, institutions regulated by the OTS must notify that agency of arrangements with all third party providers.[43]

Contract Duration

Financial institutions have been cautioned to limit the duration of their outsourcing agreements. The Federal Reserve has noted, for example, that outsourcing contracts may outlive business needs and environments, creating business as well as legal uncertainty.[44] This caution is especially important for technology-based services, which "may be subject to rapid change and a shorter-term contract may prove beneficial."[45] Consequently, "[m]anagement should consider whether the contract is flexible enough to allow for changes in technology and the financial institution's operations."[46]

Confidentiality Provisions

Financial institutions should "ensure that any contract with a foreign-based third-party service provider prohibits the service provider from disclosing or using bank data or information for any purpose other than to carry out the contracted services."[47] Essentially, the policies, procedures and controls used by the service provider must be "analogous to those that the [financial] institution would utilize if the activity were performed internally."

Thus, to the extent the service provider receives nonpublic personal information with respect to a financial institution's customers, it must have adequate controls to prevent improper disclosure. The terms of outsourcing contracts should therefore address the provider's responsibility for security and confidentiality of the institution's resources with attention to the provisions of the Gramm-Leach-Bliley Act, and should prohibit the provider and its

42. FDIC, FIL-49-99, Bank Service Company Act (June 3, 1999), at 1.
43. TB 82, at 3.
44. FRBNY White Paper.
45. FFIEC, Risk Management.
46. FIL-81-2000, at 3.
47. OCC Bulletin 2002-16, at 4; FFIEC, Risk Management, at 9.

agents from using or disclosing the institution's information except as necessary to or consistent with contracted services.[48]

Right to Audit

Finally, any contract with a service provider should facilitate adequate oversight and monitoring B topics that are discussed in detail below.[49] Consequently, a contract should specify audit frequency and the rights of the financial institution to obtain the results of the audit, which may be internal or external.[50] Based on the level of risk, the financial institution should consider requiring the service provider to undertake a comprehensive external audit, such as a SAS Type I or II review.[51]

MONITORING AND OVERSIGHT

Regardless of the level of care a financial institution puts into the selection of a service provider and the drafting of a service agreement, ongoing monitoring and oversight of the provider's controls, condition and performance are critical.[52] Financial institutions are thus expected to demonstrate adequate oversight of service providers' controls, condition and performance, such as through comprehensive audits conducted by the provider's internal or external auditors, the institution's own auditors, or foreign bank supervisory authorities.[53] Moreover, the regulatory agencies stress the need for "intensified oversight efforts" to the extent a financial institution is relying on third-party service providers.[54]

It is particularly important to ensure that the provider maintains adequate physical and data security controls, transaction procedures, business resumption and continuity planning and testing, contingency arrangements, insurance coverage and compliance with applicable laws and regulations. Information security should extend not only to "customer information," but to all data held by the service provider.[55] The evaluation of independent audit reports prepared by the service provider's audit staff, external audits and reviews (for example, SAS 70 reviews), and internal reports by the financial institution's auditors is essential to this oversight function.[56]

Finally, information related to services provided by a foreign-based third-party service provider must be readily available in English at the financial institution's U.S. offices.[57] Such information includes copies of contracts, due diligence documents, and oversight and audit reports. Financial institutions should also bear in mind that their regulatory agency may well exercise its right to review outsourced operations. Thus, as the FRB has indicated, "[o]utsourcing to jurisdictions where full and complete access to information may be impeded by legal or administrative restrictions on information flows will not be acceptable unless copies of records pertaining to U.S. operations are also maintained at the institution's U.S. office."[58]

Monitoring of Financial Condition and Operations

Financial institutions must monitor the financial condition and operations of third-party service providers. This includes review of access control reports for suspicious activity, audit reports, confirmation of insurance policies, on-site inspections, and follow-up on any deficiencies turned up in audits and reviews. It is advisable to conduct such evaluations at least annually, "and more frequently when risk is high or moderate and increasing."[59] Such evaluations "should be as comprehensive as the ongoing credit analysis the bank would conduct of its borrowers."[60]

In addition, financial institutions must assess the quality of service and support, with responsibility for the administration of each service provider relationship clearly assigned.[61] This includes a regular review of reports documenting performance, timely follow-up on any service problem, attention to adequacy of training, and regular meetings with contract parties to discuss performance

48. OCC Bulletin 2000-21: Privacy of Consumer Financial Information (June 20, 2000); 12 CFR Part 40; OCC Bulletin 2002-16, at 4.
49. FIL-81-2000, at 3.
50. FIL-81-2000, at A-3; SR 00-4 (SUP), at 3.
51. FIL-81-2000, at A-3.
52. FIL-81-2000, at 3.
53. SR 00-4 (SUP); OCC Bulletin 2001-8; TB 82; FFIEC, Risk Management, at 4.
54. OCC Bulletin 2001-47, at 7.
55. OCC Bulletin 2001-8, at 1-2.
56. OCC White Paper.
57. SR 00-4 (SUP), at 4; OCC Bulletin 2002-16.
58. SR 00-4 (SUP), at 4.
59. OCC Bulletin 2001-47, at 13; TB 82, at 16.
60. OCC Bulletin 2001-47, at 13.
61. NCUA Letter to Credit Unions No. 02-CU-17: E-Commerce Guide for Credit Unions (December 2002).

and operational issues. Financial institutions should also monitor contract compliance and revision needs and maintain business resumption contingency plans (annually or even more frequently for critical services).[62] As with the initial due diligence, it is recommended that ongoing oversight include on-site inspections, "where practical and necessary."[63]

Monitoring of Controls

Financial institutions should also carefully monitor the controls implemented by service providers with which they do business. In this regard, service providers' policies should be periodically re-evaluated, and audit reports should be obtained and reviewed.[64] In conducting such reviews, financial institutions should focus on service providers' internal controls with respect to compliance with the Bank Secrecy Act, fair lending, and other consumer protection laws and regulations, to the extent applicable.[65]

Monitoring of Performance

A financial institution should regularly review reports that document the service provider's performance.[66] Part of this review will involve an assessment of the service provider's success in meeting objective measurements (*e.g.*, response time to service requests). In addition the financial institution should track and focus on customer complaints relating to the services provided by the service provider.[67]

Documentation

Finally, financial institutions are encouraged, and in some cases, required, to "document the administration of the service provider relationship."[68] This documentation will be of benefit to the financial institution in connection with all aspects of service administration as well as contract re-negotiation. In addition, it will help a financial institution demonstrate that it has exercised due care in managing its outsourcing relationships.

The OCC, for example, has noted that its examination focus "will be placed on the results of the bank's due diligence, risk assessment, and ongoing oversight program as well as the internal and/or external audits arranged by the service provider or the bank."[69] Likewise, the OTS has indicated that regulated institutions should be prepared to document their due diligence procedures, and even information on other outsourcing bids that they may have received.[70] In sum, financial institutions will want to ensure that they are in a position to document to their regulator that they have performed the recommended steps to mitigate outsourcing risk.

CONCLUSION

Although the benefits of outsourcing are becoming widely understood by the agencies that regulate U.S. financial institutions, so also are the risks and responsibilities for those institutions becoming more clearly defined. By focusing on risk assessment; service provider due diligence, contract terms and oversight and monitoring of service providers, financial institutions can mitigate outsourcing risk and ensure compliance with regulatory expectations. ■

62. FIL 81-2000; FRB, SR 00-17 (SPE), Guidance on the Risk Management of Outsourced Technology Services (November 30, 2000); OCC 2001-47; OTS CEO Letter 113: Internal Controls (July 14, 1999).
63. FIL-81-2000, at A-6.
64. OCC Bulletin 2001-47, at 14.
65. OCC Bulletin 2001-47, at 14.
66. FIL-81-2000, at A-6.
67. FIL-81-2000, at A-6.
68. FFIEC, Risk Management, at 4.
69. OCC Bulletin 2002-16, at 5.
70. TB 82, at 18.