OCC 2002-16

OCC BULLETIN

Comptroller of the Currency
Administrator of National Banks

Subject: Bank Use of Foreign-Based Third-Party Service Providers

Description: Risk Management Guidance

To: Chief Executive Officers of All National Banks, Federal Branches and Agencies, Service Providers, Software Vendors, Department and Division Heads, and All Examining Personnel

Purpose

This bulletin provides guidance to national banks on managing the risks that may arise from their outsourcing relationships with foreign-based third-party service providers.[1] It also addresses the need for a national bank to establish relationships with foreign-based third-party service providers in a way that does not diminish the ability of the OCC to access, in a timely manner, data or information needed to effectively supervise the bank's operations.

This bulletin supplements previously issued OCC and interagency guidance on outsourcing relationships with third parties.[2]

Background

National banks are increasingly using third-party servicers to provide support for core information and transaction processing functions, including loan and deposit processing, electronic funds transfer, payroll processing, merchant processing, mortgage servicing and customer call centers. With the rapid evolution of financial technology, many national banks also are using third-party relationships to implement new business applications, such as Internet banking services, electronic bill payment and presentment, account aggregation, and digital certification.

---

[1] The term "foreign-based third-party service providers" refers to third parties whose servicing operations are located in a foreign country and subject to the law and jurisdiction of that country. Accordingly, this definition would not include a U.S.-based subsidiary of a foreign firm because its servicing operations are subject to U.S. laws. It would include U.S. service providers to the extent that their actual servicing operations are located in or outsourced *(e.g.,* subcontracted) to entities domiciled in a foreign country and subject to the law and jurisdiction of that country. Also, this bulletin applies to international branches of U.S. national banks that use third-party service providers domiciled in the same foreign country or in another foreign country.

[2] This bulletin should be used in conjunction with the following OCC issuances: OCC Bulletin 2001–47, "Third-Party Relationships: Risk Management Principles" (November 2001); OCC Advisory Letter 2000–12, "FFIEC Guidance on Risk Management of Outsourced Technology Services" (November 2000); and OCC Bulletin 2001–8, "Guidelines Establishing Standards for Safeguarding Customer Information" (February 2001).

Although national banks generally use domestic third-party service providers, the increasing globalization and cross-border linkages of the financial services industry may lead some banks to look to make greater use of foreign-based service providers for processing information and transactions with respect to both domestic and international customers.

Although generally permissible, a national bank's use of foreign-based third-party service providers may raise unique strategic, reputation, credit, liquidity, transaction, country, and compliance risk issues that require additional risk management oversight efforts. As discussed below, national banks should take into account the need for appropriate risk assessment, due diligence, protective contract provisions, and monitoring and oversight processes before entering into a contract with a foreign-based third-party service provider.

Policy on National Bank Use of Foreign-Based Third-Party Service Providers

As with domestic outsourcing arrangements, the board of directors and senior management are responsible for understanding the risks associated with the bank's outsourcing relationships with foreign-based service providers and ensuring that effective risk management practices are in place. In addition, management should assess how the relationship with a foreign-based service provider supports the bank's strategic goals and how the bank will manage the relationship on an ongoing basis.

Specifically, before a national bank contracts for the services of a foreign-based service provider, it should properly assess the associated risks and exercise appropriate due diligence, including careful consideration of contract matters and choice of law and forum provisions. Additionally, the bank should have in place sufficient risk management policies, performance monitoring and oversight processes, expertise, and access to critical information to enable it to properly oversee the risks of the outsourcing relationship, including country and compliance risks.

Country Risk

In outsourcing to a foreign-based service provider, a bank may be exposed to country risk, which is the possibility that economic, social, and political conditions and events in a foreign country might adversely affect the bank. Such conditions and events could prevent the foreign-based service provider from carrying out the terms of its agreement with the bank. To manage country risk, a bank 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. The bank's risk assessment process should take into consideration relevant country risk factors and establish sound procedures for dealing with country risk problems, including having appropriate contingency plans and exit strategies.[3]

Compliance Risk

A bank's use of a foreign-based service provider must not inhibit its ability to comply with all applicable U.S. laws and regulations. These include requirements concerning accessibility and

[3] The *Comptroller's Handbook* "Country Risk Management" (October 2001), and the Interagency Statement on "Sound Risk Management Practices for Country Risk" (March 2002) describe the elements of an effective country risk management process.

retention of records, such as the Bank Secrecy Act,[4] the national sanctions and embargo programs of U.S. Treasury's Office of Foreign Assets Control (OFAC),[5] and other relevant U.S. consumer protection laws and regulations. National banks that use a foreign-based service provider should consider how foreign data privacy laws or regulatory requirements may interact with U.S. privacy laws and regulations and how any possible conflicts can be managed.[6]

Due Diligence

As with domestic outsourcing arrangements, bank management should conduct due diligence of foreign-based service providers before selecting and contracting with the provider.[7] The due diligence process should include an evaluation of the foreign-based service provider's ability—operationally, financially and legally—to meet the bank's servicing needs given the foreign jurisdiction's laws, regulatory requirements, local business practices, accounting standards, and legal environment. The due diligence also should consider the parties' respective responsibilities in the event of any regulatory changes in the U.S. or the foreign country that could impede the ability of the bank or service provider to fulfill the contract.

Contracts

Contracts between the national bank and a foreign-based service provider should take into account business requirements and key factors identified during the bank's risk assessment and due diligence processes. In particular, bank management should consider inserting contract provisions that will protect the privacy of customers and the confidentiality of bank records given U.S. law and the foreign jurisdiction's legal environment and regulatory requirements.[8] In addition, contracts with third-party service providers should contain a provision indicating the provider agrees that the services it performs for a national bank are subject to OCC examination.[9]

Choice of Law. Before entering into an agreement or contract with a foreign-based service provider, national banks should carefully consider which country's law they wish to control the relationship and then insert choice of law covenants and jurisdictional covenants that provide for resolution of all disputes between the parties under the laws of a specific jurisdiction. Contracts that include choice of law and jurisdictional covenants will help to ensure continuity of service, to maintain access to data, and to protect nonpublic customer information. Such contracts and covenants, however, can be subject to interpretation of foreign courts relying on

---

4 In this regard, national banks using foreign-based service providers should be aware of Section 319 of the USA Patriot Act, Pub.L. No. 107–56 (Oct. 26, 2001) that requires banks to make information on anti-money laundering compliance by the bank or its customers available within 120 hours of a government request.

5 The Office of Foreign Assets Control of the U.S. Department of the Treasury administers and enforces economic and trade sanctions against targeted foreign countries, organizations sponsoring terrorism, and international narcotics traffickers based on U.S. foreign policy and national security goals. For more information, refer to the OFAC Web site at [http://www.treas.gov/ofac/].

6 Banks should be aware that some foreign jurisdictions may have data privacy laws or directives that apply to information transferred from the United States to that foreign jurisdiction over the Internet or to information "collected" within the foreign jurisdiction using automated or other equipment in that jurisdiction.

7 OCC Bulletin 2001–47 and OCC Advisory Letter 2000–12 identify factors that banks should consider when performing due diligence on potential third-party service providers.

8 OCC Bulletin 2001–47 provides additional guidance on factors that national banks should consider when entering into a binding contract.

9 12 USC 1867(c) sets forth OCC's authority to examine third-party service providers.

local laws. These local laws may substantially differ from U.S. laws in how they apply and enforce choice of law covenants, what they require of banks, and how they protect bank customers. Therefore, as part of its due diligence process, a bank before entering into a proposed contract with a foreign-based service provider should obtain a legal review from someone experienced in that country's laws regarding the enforceability of all aspects of the subject contract and any other legal ramifications.

Confidentiality of Information. Bank management 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. The contract should state that all information shared by the bank with the foreign-based third-party service provider, regardless of how the service provider processes, stores, copies, or otherwise reproduces it, remains solely the property of the bank. Also, any sharing of nonpublic customer-related information from U.S. offices with a foreign-based third-party service provider must comply with the OCC's privacy regulation, including requisite disclosures to and agreements with customers who would be affected by the bank's relationship with that provider.[10] Further, contracts between a national bank and a foreign-based service provider must include a provision requiring the service provider to implement security measures that are designed to safeguard customer information.[11]

The bank should not share any nonpublic OCC information, such as an examination report, with a foreign-based service provider except with express OCC approval. Such nonpublic OCC information remains the OCC's property, and the bank should take all required measures to protect the information's confidentiality.

Monitoring and Oversight

As with domestic outsourcing arrangements, national banks should implement an effective oversight program to monitor the foreign-based service provider's ongoing financial condition and performance.[12] In addition, the bank must determine that the service 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.

Bank management should ensure that it has sufficient expertise to perform the oversight function. As part of this function, the bank should evaluate independent audit reports prepared by the service provider's audit staff, external audits and reviews (for example, SAS 70 reviews[13]), and internal reports provided by the bank's own auditors.[14]

---

[10] See OCC Bulletin OCC 2000–21, "Privacy Rules and Regulations" (June 20, 2000); and 12 CFR Part 40, "Privacy of Consumer Financial Information," which was published in the *Federal Register* on June 1, 2000 at 65 FR 35162.

[11] See section 501(b) of the Gramm–Leach–Bliley Act, 15 USC 6801(b), and the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" contained in 12 CFR Part 30, appendix B.

[12] OCC Bulletin 2001–47 and OCC Advisory Letter 2000–12 provide additional guidance regarding oversight of third-party relationships.

[13] AICPA Statement of Auditing Standards 70, "Reports of Processing of Transactions by Service Organizations," known as SAS 70 Reports, are one form of external review. Type II SAS 70 reports review the service provider's policies and procedures and provide tests of actual controls against policies and procedures.

Access to Information

Bank Access to Information. Critical data or other information related to services provided by a foreign-based third-party service provider to a national bank must be readily available at the bank's U.S. office(s).[15] Such information should include copies of contracts, due diligence, and oversight and audit reports. In addition, the bank should have an appropriate contingency plan to ensure continued access to critical information and service continuity and resumption in the event of unexpected disruptions or restrictions in service resulting from transaction, financial, or country risk developments.

OCC Access to Information. A national bank's use of a foreign-based third-party service provider and the location of critical data and processes outside U.S. territory must not compromise the OCC's ability to examine the bank's operations. Accordingly, the OCC expects a national bank to establish such a relationship in a way that does not diminish the OCC's access to data or information needed to supervise the bank.

For this reason, a national bank should not outsource any of its information or transaction processing to third-party service providers that are located in jurisdictions where the OCC's full and complete access to data or other information may be impeded by legal, regulatory, or administrative restrictions unless copies of all critical records also are maintained at the bank's U.S. offices.

Further, copies of the results of the bank's due diligence efforts and regular risk management oversight, performance and audit reports on the foreign-based third-party service provider, as well as all policies, procedures, and other important documentation relating to the bank's relationship with the service provider, should be maintained in English for review by examiners at the bank's office(s).

OCC Supervision

The OCC's supervisory approach to cross-border outsourcing will emphasize the responsibility of the serviced national bank to conduct adequate due diligence, manage risks appropriately, comply with applicable laws, and ensure access to critical information with respect to the services being provided by a foreign-based third party. 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. If any of these risk management processes are found deficient, then the OCC will require the bank to take the necessary steps to strengthen risk management controls or terminate the outsourcing relationship.

If circumstances warrant, the OCC may examine a national bank's outsourcing arrangement with a foreign-based service provider. If the provider is a regulated entity, then the OCC may arrange

---

[14] Based upon the bank's own risk assessment, the bank should monitor its service providers to confirm that they adequately safeguard bank customer information. As part of this monitoring, a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers. See 12 CFR 30, appendix B, III.D.3.

[15] In instances where the national bank's foreign branches have outsourced local operations or services cross-border to third-party service providers domiciled in another foreign country, copies of such records can be maintained at the bank's foreign branch office.

through the appropriate foreign supervisor(s) to obtain information related to the services provided to the bank and, if significant risk issues emerge, to examine those services.

Summary

As with outsourcing relationships with domestic third-party service providers, a national bank's board of directors and management are responsible for ensuring that the bank effectively oversees any relationships with foreign-based third-party service providers. Before a bank contracts for the services of such a provider, it should properly assess the associated risks and carry out appropriate due diligence, including careful consideration of contract matters and choice of law and forum provisions. Additionally, the bank should have sufficient policies, practices, expertise, and access to critical information to enable it to oversee the risks of the outsourcing relationship, including ensuring compliance with U.S. and foreign laws.

Questions regarding this bulletin should be addressed to Hugh Kelly, Special Advisor for Global Banking, Global Banking & Financial Analysis at (202) 874-4730, or John Carlson, Senior Advisor, Bank Technology Division at (202) 874-5920.

_____

Emory W. Rushton
Senior Deputy Comptroller and Chief National Bank Examiner

_____

Jonathan L. Fiechter
Senior Deputy Comptroller for International and Economic Affairs