Guidance for Financial Institutions on the Use of Foreign-Based Third-Party Service Providers

Financial institutions have traditionally used domestic third-party service providers to handle their technology, data processing and other needs, such as call center services. However, with increasing frequency, institutions have been presented with opportunities to enter into contractual arrangements with foreign-based third-party service providers (FBTSPs) to fulfill those needs. Moreover, U.S.-based third-party service providers are subcontracting substantial portions of their operations to entities located outside of the United States. In its 2004 study of offshore outsourcing of data services to identify both consumer and safety and soundness risks associated with offshore data processing,[1] the FDIC learned that financial institutions may be unaware of such subcontracting arrangements or, if they are aware, are not adequately monitoring the relationship.

The increased use of FBTSPs by U.S. financial institutions and U.S. third-party service providers is due, in large part, to the potential cost savings that are achievable as low-wage, yet highly qualified, labor pools are tapped in foreign countries. However, as with any sound business decision, financial institutions cannot accept the benefits while ignoring the potential risks.

The use of FBTSPs raises country, reputational, operational/transactional, compliance and strategic risks. To address those risks, the appropriate managers of the financial institution need to conduct a risk assessment, exercise due diligence in the selection process, consider protective contract provisions, and establish monitoring and oversight procedures in connection with the arrangements, as explained in this guidance.

Risk Management in the Use of Foreign-Based Third-Party Service Providers

Responsibilities of Directors and Officers

Institutions that transfer internal processes or data to third-party service providers have the same risk management, security, privacy, and other consumer protection responsibilities that they would have if they were conducting the activities themselves. The board of directors and senior management have a responsibility to ensure that third-party service provider activity is conducted in a safe and sound manner in compliance with policies and applicable laws. Their responsibilities include ensuring that systems and controls are established and maintained for the security and integrity of outsourced data, whether the third-party service provider is domestic or foreign.

An institution's board of directors and senior management are responsible for recognizing the risks associated with the institution's outsourcing relationships with FBTSPs and adopting and implementing an effective risk management strategy. Of primary importance at the outset is assessing whether a relationship with a FBTSP is consistent with the financial institution's overall business strategy.

Before a financial institution executes a contract with a FBTSP, it should assess the associated risks, exercise appropriate due diligence and consider various contract issues, including choice of law and jurisdictional matters. In order to properly oversee the risks of the outsourcing relationship, including country and compliance risks, the financial institution should have in place sufficient risk management policies, performance monitoring and oversight processes, legal and technical expertise, and access to critical information. Risk management includes the following: the ability to address the exposure introduced by the relationship with a FBTSP; and appropriate contingency plans and exit strategies to ensure continued access to critical information, as well as service continuity and resumption in the event of unexpected disruptions or restrictions in service resulting from transaction or country risk developments.[2]

Risk Categories

Country Risk

Country risk is the exposure to the economic, social and political conditions and events in a foreign country that may adversely affect the ability of the FBTSP to meet the level of service required by the arrangement, resulting in harm to the financial institution. In extreme cases, this exposure could result in the loss of data, research and development efforts, or other assets. Contracting with a FBTSP exposes a financial institution to country risk, a unique characteristic of these arrangements. Managing country risk requires the ability to gather and assess information regarding a foreign government's policies, including those addressing information access, as well as local political, social, economic, and legal conditions.

Reputational Risk

Reputational risk is the risk that potential negative publicity about a financial institution's business practices will cause a decline in the customer base, costly litigation, or the loss of revenue. A financial institution's reputation, particularly the level of trust afforded to it by customers, consumers, and counterparties, can be seriously tarnished due to perceived or real breaches in its ability to conduct business securely and responsibly. Financial institutions are also responsible for risks associated with the activities of FBTSPs with which they contract. For example, deficiencies in security and privacy policies that result in the release of customer information by a FBTSP may cause damage to the financial institution's reputation.

Operational/Transactional Risk

Operational/transactional risk is the risk of incurring a financial loss because of various types of human or technical error and fraud. Operational/transactional risk arises from fraud, processing errors, systems disruptions or other unanticipated events that impact the financial institution's ability to deliver timely products or services. This risk is evident in each product and service offered. Operational/transactional risk includes the risks associated with the failure of communications, transportation or data processing, such as the breakdown of some components of the hardware, software or communication systems; internal control system deficiencies;

human errors; or management failure. As a result, the financial institution could experience delays or disruptions in processing, clearing, and settling retail payment transactions. The level of operational/transactional risk is affected by the structure of the financial institution's processing environment, including the types of services offered and the complexity of the processes and supporting technology.

The key to controlling operational/transactional risk is by adopting effective polices, procedures, and controls to meet the new risk exposures introduced by the relationship with a FBTSP. Basic internal controls, including background checks, segregation of duties, dual controls, and reconcilements, remain important. Information security often represents the most significant control area requiring additional procedures, tools, expertise, and testing. Institutions should determine the appropriate level of security controls, including the use of encryption, based on their assessment of the sensitivity of the information to the customer and the financial institution and the financial institution's risk tolerance level.

As part of its assessment of operational/transactional risk, the financial institution needs to determine the frequency with which it should obtain backup files and updated escrow agreements to the application source code from the FBTSP.

Compliance Risk

Compliance risk assessment is intended to ensure that the financial institution's arrangement with a FBTSP does not interfere with the institution's compliance with applicable U.S. laws and regulations. This assessment includes the financial institution's compliance with applicable consumer protection, privacy, and information security laws and regulations, as well as requirements concerning accessibility and retention of records, such as in the Bank Secrecy Act.[3] Institutions engaging FBTSPs should also familiarize themselves with the national sanctions and embargo programs of U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC),[4] and restrictions on the commercial exportation of encryption.[5] In addition, the financial institution should consider the potential impact of foreign data privacy laws or regulatory requirements, how they differ from U.S. privacy laws and regulations, and any operational procedures necessary to address those conflicts.[6]

Strategic Risk

Strategic risk is the risk associated with the financial institution's future business plans and strategies. This risk category includes plans for entering new business lines, expanding existing services through mergers and acquisitions, and enhancing infrastructure (e.g., physical plant and equipment, information technology and networking). Managing strategic risk requires financial institutions to develop strategic plans to grow market share through new products and services, while managing additional research and development, marketing, and operational costs. Strategic risk assessment involves a planning process that demonstrates an understanding of the risks, appropriate procedures to mitigate those risks, and the financial institution's capability to provide the service.

Risk Management

Due Diligence

Selecting a FBTSP begins with management applying the same level of due diligence it applies when initiating a domestic outsourcing arrangement. An appropriate level of due diligence includes an evaluation of the FBTSP's financial condition, references, and recent audit reports. However, in this context, due diligence also should include an evaluation of the potential impact of the foreign jurisdiction's laws and legal environment, regulatory requirements, local business practices, and accounting standards, as well as the degree to which any rapid decline in the local economy, or political stability, would affect the FBTSP's ability to meet the financial institution's servicing needs. The due diligence should consider the parties' respective responsibilities in the event changes in the law or regulations of the United States or the foreign country make it difficult or impossible for the FBTSP to fulfill the contract.

Contracts

Any contract between the financial institution and a FBTSP should address the risk factors identified during the financial institution's risk assessment and due diligence processes. In addition, the Bank Service Company Act[7] requires the financial institution to advise the FDIC that it has entered into a contract with a third-party service provider, including one located outside the United States, within 30 days of doing so.[8]

Privacy. Management must seriously consider the inclusion of provisions that will protect the privacy of customers and the confidentiality of records given U.S. law and regulations. For example, FDIC regulations call for third-party service provider contracts to include provisions requiring the third-party service provider to implement procedures that meet the objectives of the customer information security guidelines.[9] In this connection, the financial institution should consider the inclusion of requirements that the FBTSP notify the financial institution in the event of an unauthorized access to data or other information security-related events. In addition, the financial institution may wish to include provisions about the FBTSP's obligation to preclude disclosure of any customer information to nonaffiliated third parties other than as permitted under U.S. privacy laws, and to use the information only to provide those services described in the contract. [10]

Examination of a FBTSP. Arrangements with FBTSPs should always be established in a way that permits the FDIC to access facilities and examine the services performed by the FBTSP pursuant to the Bank Service Company Act. Moreover, the financial institution should not share FDIC examination reports with either a foreign regulatory authority or a FBTSP without the FDIC's express written approval. Contracts establishing relationships with FBTSPs should permit the enforcement of such arrangements in all jurisdictions in which they are intended to apply.

Choice of Law. As part of its risk assessment, a financial institution should carefully consider whether it wants U.S. law or the law where the FBTSP is located to apply in the resolution of

contract disputes or other legal issues between the parties. Any contract with the FBTSP might include choice of law and other provisions that specify which law is to apply and the court system in which disputes will be heard. Those provisions will assist the financial institution in maintaining continuity of service, access to data, and protection of customer information. In this regard, institutions should consider carefully the impact of any provision in an agreement presented by the FBTSP that states that the FBTSP has no presence or conducts no business within the United States.

In addition, those contract provisions may be subject to interpretation by foreign courts applying local laws. Those laws may not recognize choice of law provisions, or differ from U.S. law with respect to what they require of financial institutions or the degree to which they protect customers. Any analysis of local law obtained as part of a financial institution's due diligence from counsel experienced in that country's laws might include a discussion about the enforceability of all aspects of any contract, including choice of law and jurisdictional provisions.

Ownership of Information and Intellectual Property. It is appropriate that any agreement with a FBTSP require that all data transferred to the FBTSP remain the property of the financial institution, regardless of how the data are processed, stored, copied, or reproduced, and that the data be returned to the financial institution upon termination of the contract. In addition, service agreements should contain provisions that protect the financial institution's rights in any intellectual property such as design, graphics or code created by the FBTSP in order to meet the requirements of the agreement.

Monitoring and Oversight

When an arrangement with a FBTSP has been established, a financial institution should monitor both the FBTSP and the conditions within the country in which it is located. Among the areas to be considered in developing an oversight program are the FBTSP's:

- level of performance,
- financial condition,
- data security procedures,
- business recovery plans and testing,
- adequacy of insurance coverage, and
- compliance with applicable laws and regulations.

The financial institution should arrange to receive and evaluate any reports prepared by independent outside auditors and the FBTSP's staff as well as any reports prepared by its own auditors.[11] In addition, the financial institution should monitor economic and governmental conditions within the country in which the FBTSP is based in order to determine whether changes in those conditions are likely to adversely affect the ability of the FBTSP to perform under the arrangement.

Undisclosed Foreign-Based Subcontracting Arrangements

Undisclosed foreign-based subcontracting arrangements occur when a domestic third-party service provider subcontracts all or part of the work for a financial institution to an offshore company without prior notice to or consent from the financial institution. Third-party service provider contracts often permit subcontracting. However, the transfer of data overseas without any notification to the financial institution may increase risk in an outsourcing relationship.

Standard Federal Financial Institutions Examination Council (FFIEC) examination procedures include a review of outsourcing arrangements to determine whether:

- subcontracting is employed either under or outside the terms of the contract;
- the financial institution is aware of the subcontracting and the vendor's location; and
- the financial institution has procedures for monitoring all outsourcing arrangements to ensure adequate controls are in place or the third-party service provider has proper procedures and controls to monitor its subcontracting arrangements.

The financial institution should consider including contract provisions that require a third-party service provider to notify the financial institution of and obtain approval for changes to significant subcontracting relationships, whether the subcontracted entity is domestic or foreign-based. Further, contract provisions allowing the financial institution to monitor the primary contractor's risk management activities related to foreign-based subcontractors should be considered.

Access to Information

A financial institution should not establish an arrangement with a FBTSP located in any jurisdiction in which local laws or regulations or administrative procedures would interfere with the FDIC's full and complete access to data or other relevant information as required by the Bank Service Company Act. Any analysis of local law obtained from counsel experienced in the law and practices of that jurisdiction might include a discussion as to whether there are any provisions or practices, including data transfer restrictions that would impair the FDIC's access to information or ability to examine the financial institution's operations.

Critical data or other information related to services provided by a FBTSP to a financial institution must be readily available at the financial institution's U.S. office(s). A financial institution must maintain, in the files of a U.S. office, appropriate documentation to support all arrangements with FBTSPs. Appropriate documentation typically includes a copy of the contract establishing the arrangement, supporting legal opinions, due diligence reports, audits, financial statements, performance reports, and other critical data or information, including any related transactions.

FDIC Supervision

The FDIC may examine a financial institution's outsourcing arrangement with a FBTSP or – in the case of a regulated entity – obtain information through the appropriate supervisory agency in the FBTSP's home country. The FDIC's examination procedures will cover the adequacy of the financial institution's due diligence efforts in the selection of a FBTSP, its risk assessment and the steps taken to manage those risks. This will include an assessment of relevant contract provisions and the financial institution's periodic review of internal/external audits or testing to assure compliance with applicable laws and to ensure access to critical information.

---

[1] See, Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Risks, FDIC, June 2004.

[2] See, Country Risk Management FIL 23-2002, March 11, 2002; Bank Technology Bulletin on Outsourcing, FIL 50-2201, June 4, 2001; Security Standards for Customer Information, FIL 22-2001, March 14, 2001; Risk Management of Technology Outsourcing, FIL 81-2000, Nov. 29, 2000.

[3] In this regard, institutions using FBTSPs should be aware of Section 319 of the USA Patriot Act, Pub. L. No. 107-56 (Oct. 26, 2001) that requires an institution to make information on anti-money laundering compliance by the institution or its customers available within 120 hours of a government request.

[4] 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 www.treas.gov/offices/eotffc/ofac/.

[5] Export controls on commercial encryption products are administered by the Bureau of Industry and Security, part of the Department of Commerce. You may be an exporter if you provide encryption software to a FBTSP. Export administration regulations regarding encryption are contained in 15 CFR §§ 740.13, 740.17, & 742.15. See, www.bis.doc.gov.

[6] An institution should identify and understand the application of any laws within a foreign jurisdiction 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] 12 USC § 1867(c)(1).

[8] 12 USC § 1867(c)(2).

[9] 12 CFR 364, Appendix B, ¶ III.D.2.

[10] See, e.g. 12 CFR 332.11 & 13.

[11] Based upon the bank's own risk assessment, the bank should monitor its third-party 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 third-party service providers. See 12 CFR 364, Appendix B,¶ III.D.3.