Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks

Federal Deposit Insurance Corporation
June 2004

This study presents the FDIC's findings with regard to the associated risks of offshore outsourcing (also known as "offshoring") by financial institutions from a safety and soundness perspective and with particular emphasis on the threats posed to customer privacy.

EXECUTIVE SUMMARY AND RECOMMENDATIONS

Offshore Outsourcing or "Offshoring," a New Twist on a Traditional Outsourcing Model

Traditional outsourcing to domestic third-party service providers or domestic affiliates has been done by financial institutions in the United States for many years. However, the use of offshore contractors has grown dramatically in the past few years due to the flexibility offered by new information technology (IT) and the prospect of lower costs. At the same time, consumers have become more concerned about privacy, and the abuse of personal data has increased as instances of fraud, such as identity theft, have become commonplace.

Offshoring Background

The rapid increase in offshoring by many U.S. financial institutions and their data vendors is due in large part to the potential cost savings that are achievable as low-wage labor pools are tapped in foreign countries. Deloitte Consulting, LLP estimates that financial institutions that offshore achieve average cost savings of 39 percent, with one in four institutions surveyed achieving savings of more than 50 percent. Typically, financial institutions offshore non-core job functions, such as IT (specifically, software development and maintenance), administration, human resources, contact centers, call centers, and telemarketing.

Deloitte estimates that $356 billion, or 15 percent, of the financial service industry's current cost base is expected to move offshore within the next five years. Further, the range and number of offshored job functions within individual institutions is expected to increase, with the average number growing from two to four functions per institution. In particular, the traditional focus on IT alone, which accounts for 70 percent of current offshore activity, will change to a business-process emphasis. Competitive pressures are the primary motivator for financial institutions to move higher-risk functions offshore.

Offshoring Risks

Domestic outsourcing and offshoring share most risk characteristics. However, the more complicated chain of control incurred when offshoring financial services and related data may create new risks when compared to domestic outsourcing. Offshoring also introduces an element of country risk to the outsourcing process. In particular, geographic distance from the function and timing lags in reporting heighten the potential risk exposures. Significant offshoring risk areas include:

Country Risk: political, socio-economic, or other factors may amplify any of the traditional outsourcing risks, including those listed below.
Operations/Transaction Risk: weak controls may affect customer privacy.
Compliance Risk: offshore vendors may not have adequate privacy regulations.
Strategic Risk: different country laws may not protect "trade secrets."
Credit Risk: a vendor may not be able to fulfill its contract due to financial losses.

Privacy Concerns Raised by Offshoring

Few legal restrictions exist on financial service companies sending customer data to foreign countries. Financial institution customers may not opt out of these information transfers to nonaffiliated service providers if the transfer is for a purpose described in section 502(e) of the Gramm-Leach-Bliley Act (GLBA). For example, the opportunity to opt out does not apply where the information transfer is to: (1) service or process a financial product or service that the customer requested or authorized; or (2) maintain or service the customer's account.

However, GLBA does provide important protections that cover both domestic and offshore outsourcing. GLBA establishes affirmative and continuing obligations for financial institutions to respect customer privacy and protect customer personal information against reasonably foreseeable internal or external threats to its security, confidentiality, and integrity. The Federal Banking Agencies have extended these obligations to include the monitoring of the activities of those service providers to which financial institutions transfer customer information.

Privacy risks vary by job type. For instance, relatively lower-risk activities include computer source-coding or application development and maintenance, whereas higher-risk activities include any function using personal data, such as call centers or transaction processing. At present, financial institutions are primarily offshoring low-risk IT work in addition to higher-risk, customer data-base type work, including mortgage servicing and customer-assistance/help-desk services.

Recommendations Arising from this Study

- **Encourage Identification of Undisclosed Third-Party Contracting Arrangements:** Undisclosed third-party contracting arrangements may increase risk in outsourcing relationships. This potential increase in risk occurs regardless of whether the undisclosed third party resides domestically or offshore; however, inherent outsourcing risks may be amplified due to unique country risk when the third party is an offshore vendor. Our recommendation is that financial institutions that outsource data to domestic vendors should be aware when domestic vendors have in turn subcontracted out that same work to overseas or domestic third parties. This practice has not always been the case; the May 2004 edition of the American Bankers Association's *Banking Journal* discusses an instance where subcontracting to an offshore vendor occurred without the knowledge of the financial institution.[1] It is currently standard FFIEC examination procedure for examiners to review outsourcing arrangements during examinations.[2] Part of a standardized procedure should include:
    - Identifying and reviewing contracts between financial institutions and data service providers that allow for subcontracting or subsequent outsourcing to occur;
    - Determining whether subsequent outsourcing has in fact occurred as indicated in the contract or outside the terms of the contract;

[1] Steve Cocheo, "Global Think? Or Job Shrink?" *ABA Banking Journal*, May 2004.
[2] 1996 FFIEC IS Examination Handbook.

- Determining if the financial institution is aware of the subsequent outsourcing and the location of the outsourcing; and
- Determining if the financial institution has procedures for monitoring all outsourcing arrangements to ensure adequate controls are in place or the service provider has proper procedures and controls to monitor their outsourcing arrangements.

- **Consider Enhancing Bank Service Company Act (BSCA) Retention Procedures through Creation of a Central Database:**
  To assist in measuring and monitoring the systemic risk posed by foreign technology service providers, the Federal financial institution regulators should consider enhancing their BSCA retention procedures. Section 7(c)(2) of the BSCA states that any regulated financial institution that has services performed by a third party "shall notify such (appropriate Federal banking agency) of the existence of the service relationship within 30 days after the making of such service contract or the performance of the service, whichever occurs first." Currently those notices are not aggregated in a central location. The agencies should conduct a cost/benefit analysis of establishing one shared, central repository of institution notices of outsourcing arrangements for use in analysis, monitoring, and tracking by the Federal Financial Institutions Examination Council.

TABLE OF CONTENTS

BACKGROUND

The use of offshore contractors has grown dramatically in the past few years due to the flexibility offered by new information technology and the prospect of lower costs. At the same time, consumers have become more concerned about privacy and the potential for abuse of personal data as instances of fraud, such as identity theft, have become commonplace. In light of these developments, the purpose of this study is to gauge the risk to personal privacy posed by the offshoring of those financial institution functions that require customer data, focusing on:

1. The business forms of offshoring employed by financial institutions,
2. The types of work that financial institutions offshore,
3. The risks associated with offshoring, and
4. Strategies employed by financial institutions and regulators to identify, measure, monitor, and control the risk to personal data.

During the course of this study, FDIC staff reviewed existing publications and articles; and also met with other regulators and industry representatives, consulting firms and research organizations that are monitoring this topic. Despite the scope of this inquiry and research, little data was available on the precise amount of work presently being offshored by financial institutions. As such, this study endeavors to frame pertinent issues and identify areas warranting increased focus and data collection.

Trends in Offshoring

Financial institutions have outsourced functions to domestic third-party service providers or domestic affiliates for many years. In recent years, the growth of low-cost, well-educated labor pools and the development of low-cost data transmission capabilities have led to a significant amount of work going to offshore concerns. Businesses are now able to take advantage of huge, low-cost labor pools such as the well-educated work force in India. A host of other countries are also commonly used for offshoring. These locations are listed in Appendix A.

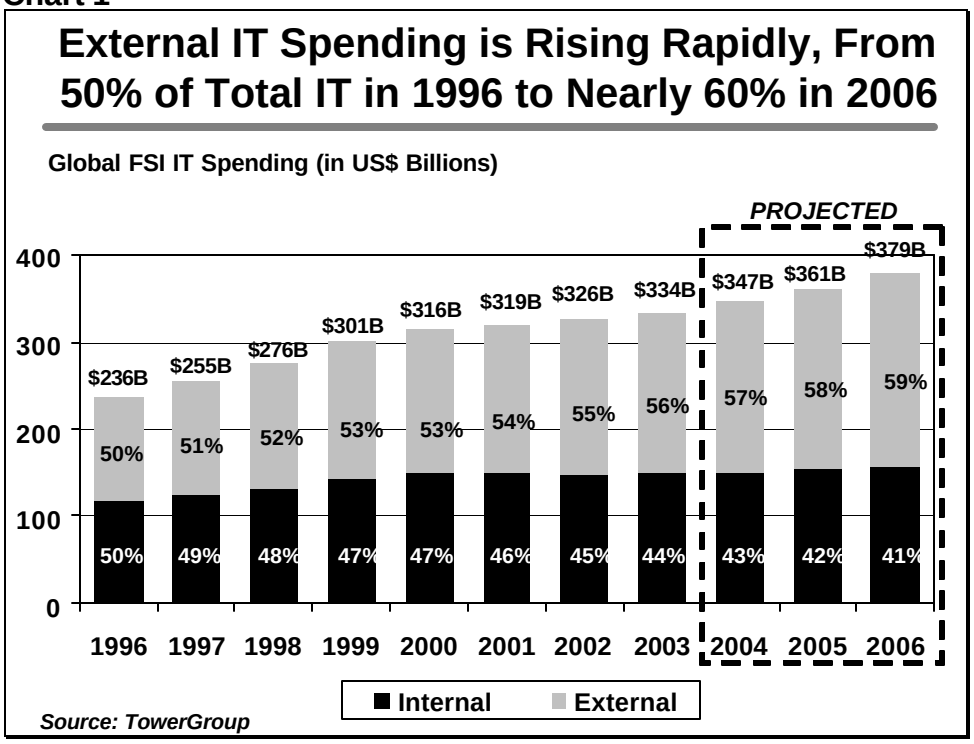
Estimates concerning the extent of offshoring and its prospective growth are difficult to reconcile. A recent study by Deloitte Consulting projects that 15 percent of the U.S. financial services industry cost base will move offshore within the next five years.[3] Another survey conducted by the Tower Group, focusing on different statistics, indicates more moderate growth will occur. According to the Tower Group, growth should not exceed 15 percent of financial institution outsourcing in the next eight to ten years.[4]

In spite of different estimates of growth levels, most believe that offshoring will continue to increase for the foreseeable future. As shown in Chart 1, the Tower Group estimates that the share of offshored global financial services IT spending has steadily increased, from 50 percent

[3] Deloitte Consulting (2003)
[4] Tower Group (2004)

in 1996 to 56 percent in 2003. While difficult to project with certainty, there are strong indications that offshoring will continue to grow into the future.

Chart 1



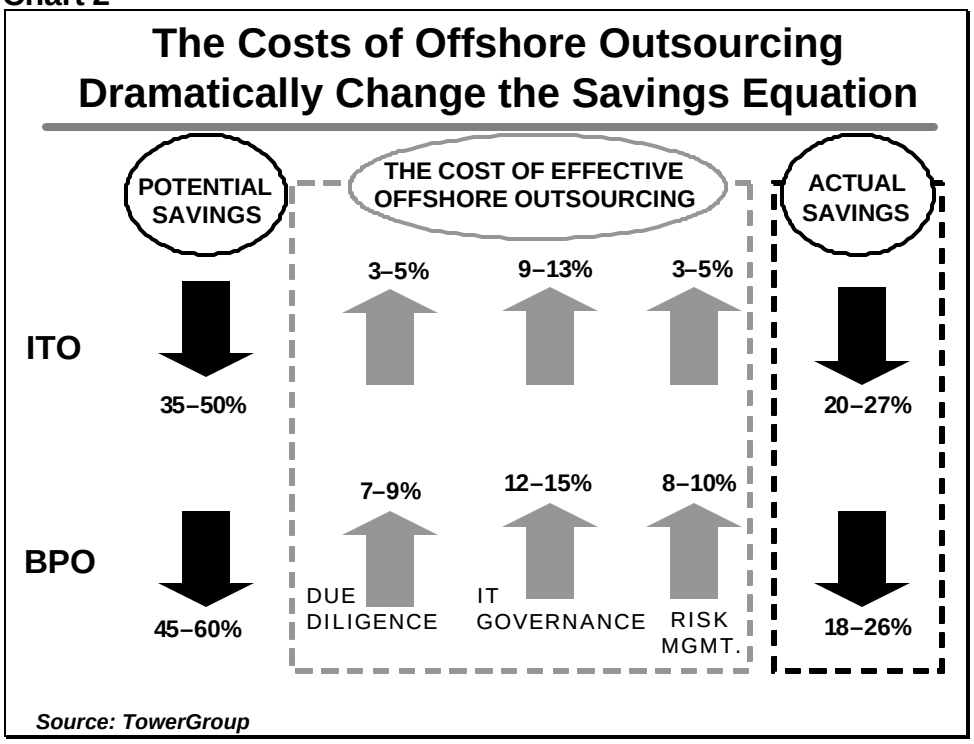
Reasons for Offshoring

The increasing instances of offshoring by many U.S. financial institutions and their data vendors are due in large part to the potential cost savings that are achievable as low-wage labor pools are tapped in foreign countries. The Gartner Group estimates that offshore software development cost savings can be as much as 75 percent when compared to the cost of similarly skilled local labor and technical resources with those available overseas.[5] Deloitte Consulting, LLP, estimates that financial institutions that offshore functions achieve an average cost savings of 39 percent, with one in four institutions surveyed achieving savings of more than 50 percent through offshoring.[6] One data vendor reports cost savings of greater than 50 percent in their offshored program development work.

As shown in Chart 2, the Tower Group estimates large potential cost savings are available for offshore outsourcing of both Information Technology Operations (ITO) as well as Business Process Operations (BPO). Although potential cost savings of 35 to 60 percent are said to exist, the net savings falls to somewhere within half of that range after deducting associated costs, chief among which is IT governance.

[5] Conference call with Gartner Group on April 29, 2004.
[6] Deloitte Consulting LLP, "Offshoring and Cross-Border Outsourcing by Banks", March 30, 2004 presentation.

Chart 2



Another reason for the growth in offshoring is that companies have found it desirable to be able to continue their operations virtually around the clock—when a day's operations are closing down in the United States, they are just beginning in India. Other reasons companies choose to offshore include the desire to:

- Improve company focus;
- Free up resources for other projects;
- Gain access to world-class capabilities;
- Access resources not available internally;
- Accelerate reengineering benefits;
- Reduce time to market; and
- Remain competitive.

The decision to choose offshoring is creating its own momentum. Because of the large number of firms that are offshoring their work, other firms are also being forced to choose this option in order to remain competitive.

Finally, by offshoring non-core functions, management can improve company focus and concentrate clearly and effectively on "core" function areas. When done correctly, offshoring can allow management to focus on those core functions that give them a competitive edge and have the highest potential returns. Financial institutions are already outsourcing many non-core job functions and are reviewing the prospects of outsourcing all non-core functions, which include:

- Information technology (IT), specifically programming;
- Administration;
- Human resources; and
- Contact centers/Call centers/Telemarketing.

The percentage of institutions running offshore functions is predicted to increase dramatically within the next few years. Further, the range and number of job functions within individual institutions that will be offshored is expected to increase, with the average number growing from two to four functions per institution. The traditional focus on IT alone, which accounts for 70 percent of the current movement of offshore activity, will evolve toward a business-process emphasis.

OFFSHORING BUSINESS MODELS AND RISKS

Offshoring Business Models

This study reviewed the four basic forms of offshoring: captive direct, joint venture, direct third-party, and indirect third-party. Each form of conducting offshore outsourcing poses different operational risks for financial institutions and different potential privacy risks for consumers.

Captive Direct – In the captive-direct offshoring form, financial institutions use their own organizations in lower-cost, offshore locations, known as captive centers. Because captive centers require a sizeable up-front investment, only larger institutions have the necessary resources to use this form. In theory, captive-direct offshoring poses lesser risks to an organization than any of the other forms, because dedicated management from the parent company directly oversees the offshore operations. Companies such as ABN Amro, American Express, General Electric, JP Morgan Chase, Mellon Financial, Standard Chartered, and Citibank have wholly-owned captive centers in India and other countries.

Joint Venture – This form of offshoring occurs when domestic institutions partner with a foreign entity for shared control of foreign operations. In general, because control is shared with the foreign enterprise, this method of offshoring has higher risk potential than the wholly-owned, foreign, captive-direct form. Still, because of ability to exercise control through majority ownership of the venture (or partial control with a 50 percent or less share of ownership), this form, in general, has less risk associated with it than the direct and indirect third-party contracting forms described below.

Direct Third Party – In the direct third-party form, institutions outsource operations to a third-party vendor located offshore. Institutions such as Bank of America, Deutsche Bank, and Merrill Lynch have established direct third-party arrangements with vendors in India. Because financial institutions have no ownership authority in this form, their controls over this working arrangement are limited to the contract terms agreed to with the third-party vendor, thereby making this form potentially more risky than either the captive or joint venture forms.

Indirect Third Party – The indirect third-party form of offshoring typically occurs when a domestic financial institution enters into a contract with a domestic data vendor, who then subcontracts out all or a part of the work to an offshore company. (Typical data vendor contracts often contain provisions that allow for subsequent subcontracting of work. See Appendix B.) As a result, data can be sent overseas at the discretion of the domestic third-party vendor without further notification to the domestic financial institution. This offshoring form has the highest associated risk and potential for breaches of privacy rules, because controls may not exist to preserve the integrity of customer and bank data.

Outsourcing/Offshoring Risks

Some of the risks that may emerge when financial institutions use a third party data or other service provider are presented in this section. Appendix C contains a more detailed listing of

risks from outsourcing and offshoring. It is important to recognize that among the different risks posed by outsourcing, only country risk is unique to offshoring; however, offshoring can introduce additional complications to standard outsourcing risks.

Country Risk - Includes the political infrastructure, socio-economic conditions, and related issues pertaining to a particular country and how a change in any of these might affect the ability of an offshore third party to fulfill their contract obligations. This type of risk could also be influenced by the relationship between the U.S. and the host-country bank supervisor and the concern that the current relationship can always change in the future.

Some specific areas with potential for offshore fraud were identified in the course of this study. It is worth noting that these examples of potential fraud could as well occur domestically as offshore. Still, institutions need to be aware of the potential for heightened exposures that exist for these riskier activities. Beyond just the risk for loss of data privacy, the risk of funds diversion exists because of the nature of the information being handled by subcontractors. Some examples, identified by data service providers we spoke with include:

- Letters of Credit exception handling. In this scenario, workers are provided full access to bank account numbers of the parties involved and all other documentation associated with the Letter of Credit.
- Back office processing of foreign exchange. In this subcontracted activity, offshore workers have processing responsibilities along with full access to all relevant information needed to transact non-automated currency settlements and clearings.
- Administration of commercial lending. Offshore workers have processing responsibilities along with full access to loan data throughout the life of the loan.

Staff compiling this study were also informed by one data vendor that a specific form of country risk exists in the case of foreign organized crime activities. These criminal elements reportedly have targeted foreign offshore enterprises in attempts to gain access to the data they process. Reportedly, one foreign organized crime group has attempted to buy existing call centers, set up their own call centers and tried to bribe workers to gain access to data and information.

Reputation Risk – Is the risk to earnings or capital arising from negative public opinion. This affects an institution's ability to establish new relationships or services or to continue servicing existing relationships. This risk is present in activities such as outsourcing and particularly in the offshore-outsourcing of work.

Operations/Transactional Risk – Includes the risk to earnings or capital that arises from problems with service or product delivery. The lack of an effective business resumption plan and appropriate contingency plans increase transaction risk.

Compliance Risk – Is the risk to earnings or capital that arises from violations of laws or regulations or nonconformance with internal policies or ethical standards. This risk exists when the activities of a third party are not consistent with the law, policies, or ethical standards of the financial institution. Also, the risk is exacerbated by an inadequate oversight and audit function.

Strategic Risk – Is the risk to earnings or capital that may arise from adverse business decisions or improper implementation. The use of a third party to perform banking functions or to offer products or services that do not help the financial institution achieve corporate strategic goals and provide an adequate return on investment expose the financial institution to strategic risk.

Credit Risk – Is the risk to earnings or capital that arise from the obligor's failure to meet the terms of any contract with the financial institution or to otherwise perform as agreed. The basic form of credit risk involves the financial condition of the third party itself. Appropriate monitoring by the financial institution of the third party's activity is necessary to ensure that credit risk is understood and remains within board-approved limits.

Consumer Privacy and Other Operational Risks Will Vary By Institution, Business Model, and Type of Function That Is Offshored

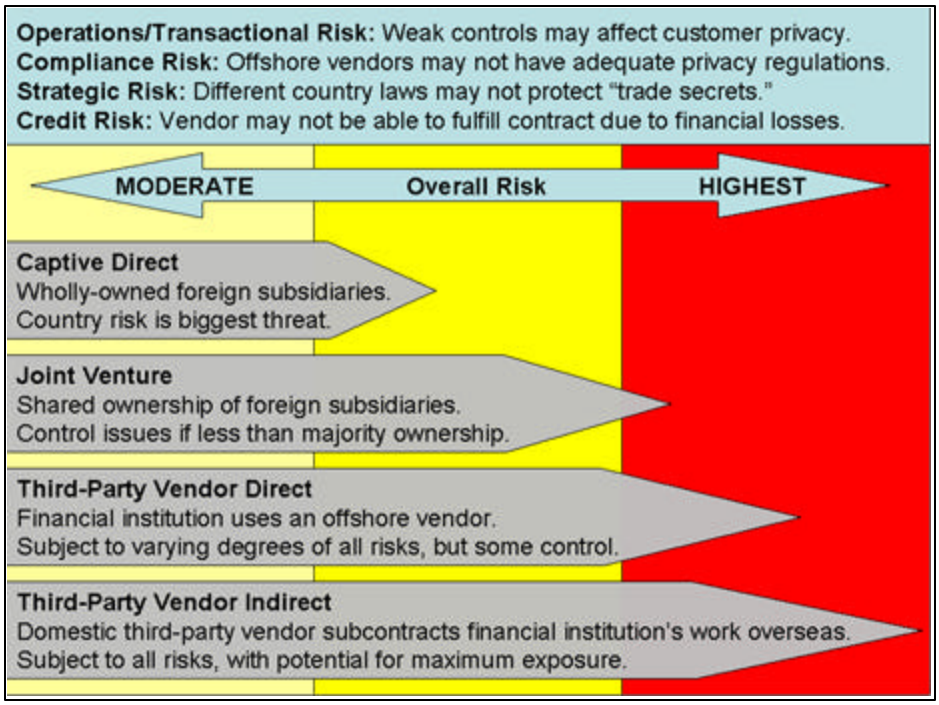
There is a heightened exposure to reputation risk for financial institutions that jeopardize the security and integrity of private consumer data at any point in the chain of the work being offshored. Such risks cannot be fully assessed without a complete understanding of the resulting arrangement; which in itself, may be a function of factors intrinsic to the individual financial institution, contractual arrangement, or business situation. Insufficient management and control of these risks may have significant financial ramifications, including high legal costs, credit losses, increased operating costs, loss of business, and other direct and indirect costs. It is important that management understand and evaluate these potential risks so that a thorough assessment can be made before deciding to enter into a third-party agreement.

Specific risk exposures may include problems related to inadequate contractual provisions governing control, security, and audit responsibilities. Various employee-risk issues differ significantly in different offshore arrangements. For instance, background checks of employees involving credit-bureau information, criminal records, or even drug testing results are standard requirements in the United States. The ability to obtain the same types of reviews in many other countries is questionable.

Financial institutions may also have intrinsic characteristics that mitigate risk. Some institutions may have previous experience working in a particular country. Multinational financial institutions may already have offices in the country where offshoring takes place, providing better access to legal, operational, and managerial expertise. Also, the location of sensitive data affects an institution's risk exposure. Data that is physically located at a U.S. facility, even if it is accessed by overseas vendors, may provide greater control over security.

As illustrated in Chart 3 the principal offshoring business models hold varying amounts of risk.

Chart 3: Forms of Offshoring and Their Associated Risks



Source: FDIC

Also, privacy risks vary by job type. For instance, relatively lower-risk activities include computer source-coding or application development and maintenance; whereas higher-risk activities include any function using personal data, such as call centers or transaction processing.[7] At present, financial institutions offshore IT work in addition to higher-risk, customer data-based type work including mortgage servicing and customer-assistance/help-desk services.

Protections for Customer Information Sent Offshore

For each form of offshoring (captive, joint venture, direct third party, and indirect third party) nothing precludes the offshore transfer of customer data by a financial institution or one of its service providers. Financial institution customers may not opt out of these information transfers to nonaffiliated service providers if the transfer is for a purpose described in section 502(e) of the Gramm-Leach-Bliley Act (GLBA). For example, the opportunity to opt out does not apply where the information transfer is to:

- service or process a financial product or service that the customer requested or authorized; or
- maintain or service the customer's account.

[7] Even relatively lower-risk activities such as source-coding or software development may pose operations risks and threats to privacy of data should offshore, contract programmers operate with malicious intent.

However, GLBA does provide important protections that cover both domestic and offshore outsourcing. GLBA establishes affirmative and continuing obligations for financial institutions to respect customer privacy and protect customer personal information against reasonably foreseeable internal or external threats to its security, confidentiality, and integrity. The Federal Banking Agencies (FBAs) have extended these obligations to include the monitoring of the activities of those service providers to which financial institutions transfer customer information.

§ 501(a): It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

§ 501(b): In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards.

The FBAs issued identical Guidelines pursuant to § 501(b). Those Guidelines provide that each financial institution shall: (1) exercise appropriate due diligence in selecting service providers; (2) require them by contract to implement appropriate measures designed to meet the objectives of the Guidelines; and (3) where indicated based upon the institution's risk assessment, monitor the service providers to confirm that they implement the procedures required by the Guidelines. 12 CFR 364.101, App. B ¶ III.D.

Responsibilities of Directors and Officers

Financial institution directors and management remain liable for their responsibilities to the institution and the consequences of all outsourcing decisions. The board of directors and management have the responsibility to make sure systems and controls are established and maintained for the security and integrity of outsourced data, whether the service provider is domestic or foreign. Institutions that transfer internal services to third parties have the same risk management, security, privacy, and other consumer protection responsibilities as if the institution conducted the activities itself. The board of directors and management have the responsibility to ensure that the third-party activity is conducted in a safe and sound manner and is in compliance with policies and applicable laws.

SUPERVISORY REGULATIONS, GUIDELINES, IMPLICATIONS, AND APPROACHES

Despite the relative newness of offshoring, many offshoring issues from a regulatory perspective are covered by previously released regulatory guidance regarding outsourcing. Relevant regulatory guidance is contained in releases from the Federal Financial Institutions Examination Council, the FDIC, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the National Credit Union Administration. See Appendix D for detailed listings and summaries of outsourcing-related guidance.

Lessons Learned and Best Practices

Drawing from discussions with other regulators, industry participants, data vendors, and consultants, the following is a compilation of necessary components of a well-structured risk management process for institutions that are considering the offshoring decision:

- Risk assessments must be performed to identify the financial institution's needs and requirements.
- Proper due diligence must be done to identify and select a third-party provider.
- Written contracts must be developed that fully outline duties, obligations, and responsibilities of both parties and identify the choice of which country law will prevail in the event of contract disputes.
- Contracts should include a termination provision allowing the financial institution to end outsourcing arrangements if they are not satisfied with any aspects of the performance or work product of the offshore firm upon reasonable notice and without penalty.
- Contracts with foreign-based service providers should contain a provision acknowledging the authority of the U.S. financial institution regulator to examine the provider's performance of services.
- The contract should also include a provision that enables the financial institution to terminate the contract in the event that a U.S. regulator formally objects to the particular third-party arrangement.
- There should be ongoing oversight of all third parties and third-party activities.
- There should be maintenance of effective documentation of the third-party relationship.
- An information security program compliant with Sections 501 (a) and (b) of GLBA must be followed. As such, a well-structured risk management process will protect the privacy, confidentiality, and security of customer non-public, personal information from threats including, but not limited to leaks of confidential information and unlawful transfers of personal data.

In addition, a list of recommendations and best practices primarily for ongoing programs is as follows:

- **Country Risk**
  - Financial institutions must closely monitor foreign government policies as well as political, social, economic, and legal conditions in countries where they have a contractual relationship with a service provider.

  - The risk assessment process should take into consideration relevant country risk factors and establish sound procedures for addressing country risk problems, including the development of appropriate contingency plans and exit strategies.

- **Compliance Risk**
  - A financial institution'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 retention of records, such as the Bank Secrecy Act, the national sanctions and embargo programs of the U.S. Treasury's Office of Foreign Assets Control, and other relevant U.S. consumer protection laws and regulations.

  - Financial institutions 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 possible conflicts can be managed.

- **Due Diligence**
  - The due diligence process should include an evaluation of the foreign-based service provider's ability—operationally, financially, and legally—to meet the financial institution's servicing needs given the foreign jurisdiction's laws, regulatory requirements, local business practices, accounting standards, and legal environment.

  - The due diligence process should also 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 financial institution or service provider to fulfill the contract.

  - The due diligence process should provide that an appropriate monitoring and oversight system is ready for implementation by the financial institution prior to executing the contract with the service provider.

- **Contracts**
  - Contracts between the financial institution and a foreign-based service provider should take into account business requirements and key factors identified during the financial institution's risk assessment and due diligence processes. In particular, financial institution management should insert contract provisions that will protect the privacy of customers and the confidentiality of financial

institution records given U.S. law and the foreign jurisdiction's legal environment and regulatory requirements.

- Contracts with third-party service providers should contain a provision indicating that the provider agrees that the services it performs for a financial institution are subject to exam by U.S. Federal financial institution regulatory agencies.

- Choice of Law: Before entering into an agreement or contract with a foreign-based service provider, financial institutions 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.

- Confidentiality of Information: Financial institution management should ensure that any contract with a foreign-based third-party service provider prohibits the service provider from disclosing or using financial institution data or information for any purpose other than to carry out the contracted services.

- Local Legal Review: Contracts with foreign third-party service providers should be reviewed by counsel experienced in that country's laws to determine the enforceability of all aspects of any contract, including choice of law and jurisdictional provisions.

- **Monitoring and Oversight**
  - As with a domestic outsourcing arrangement, financial institutions should implement an effective oversight program to monitor the foreign-based service provider's ongoing financial condition and performance.

  - The financial institution must determine that the service provider maintains adequate physical and data security controls, transaction procedures, business resumption, continuity planning and testing, contingency arrangements, insurance coverage, and compliance with applicable laws and regulations.

  - The financial institution should evaluate independent audit reports prepared by the service provider's audit staff, external audits and reviews (for example, "SAS 70 reviews"), and internal reports provided by the financial institution's own auditors.[8]

- **Access to Information**
  - Financial Institution Access to Information: Critical data or other information related to services provided by a foreign-based third-party service provider to a financial institution must be readily available, in English, at the financial

[8] "SAS 70" refers to The American Institute of Certified Public Accountants Auditing Standards (SAS) Original Pronouncements 70: Reports on the Processing of Transactions by Service Organizations. This Statement provides guidance on the factors an independent auditor should consider when auditing the financial statements of an entity that uses a service organization to process certain transactions.

institution's U.S. office(s). Information should include copies of contracts, due diligence, oversight and audit reports, and appropriate contingency plans.

- Regulatory Access to Information: A financial institution'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 primary U.S. regulator's ability to examine the financial institution's operations.

- **Supervision by U.S. Regulators**
  - Emphasize the responsibility of the serviced financial institution 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 should be on the results of the financial institution'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 financial institution.

  - If warranted, the regulator may examine a financial institution's outsourcing arrangement with a foreign-based service provider. If the provider is a regulated entity, then the regulator may arrange through the appropriate foreign supervisor(s) to obtain information related to the services provided to the financial institution and, if significant risk issues emerge, to examine those services.

RECOMMENDATIONS

The following are preliminary recommendations formulated by the staff in conducting this review of offshore outsourcing:

- **Encourage Identification of Undisclosed Third-Party Contracting Arrangements:** Undisclosed third-party contracting arrangements may increase risk in outsourcing relationships. This potential increase in risk occurs regardless of whether the undisclosed third party resides domestically or offshore; however, inherent outsourcing risks may be amplified due to unique country risk when the third party is an offshore vendor. Our recommendation is that financial institutions that outsource data to domestic vendors should be aware when domestic vendors have in turn subcontracted out that same work to overseas or domestic third parties. This practice has not always been the case; the May 2004 edition of the American Bankers Association's *Banking Journal* discusses an instance where subcontracting to an offshore vendor occurred without the knowledge of the financial institution.[9] It is currently standard FFIEC examination procedure for examiners to review outsourcing arrangements during examinations.[10] Part of a standardized procedure should include:
    - Identifying and reviewing contracts between financial institutions and data service providers that allow for subcontracting or subsequent outsourcing to occur;
    - Determining whether subsequent outsourcing has in fact occurred as indicated in the contract or outside the terms of the contract;
    - Determining if the financial institution is aware of the subsequent outsourcing and the location of the outsourcing; and
    - Determining if the financial institution has procedures for monitoring all outsourcing arrangements to ensure adequate controls are in place or the service provider has proper procedures and controls to monitor their outsourcing arrangements.

- **Consider Enhancing Bank Service Company Act (BSCA) Retention Procedures through Creation of a Central Database:**
  To assist in measuring and monitoring the systemic risk posed by foreign technology service providers, the Federal financial institution regulators should consider enhancing their BSCA retention procedures. Section 7(c)(2) of the BSCA states that any regulated financial institution that has services performed by a third party "shall notify such (appropriate Federal banking agency) of the existence of the service relationship within 30 days after the making of such service contract or the performance of the service, whichever occurs first." Currently those notices are not aggregated in a central location. The agencies should conduct a cost/benefit analysis of establishing one shared, central repository of institution notices of outsourcing arrangements for use in analysis, monitoring, and tracking by the Federal Financial Institutions Examination Council.

[9] Steve Cocheo, "Global Think? Or Job Shrink?" *ABA Banking Journal*, May 2004.
[10] 1996 FFIEC IS Examination Handbook.

APPENDIX A
MOST WIDELY-USED OFFSHORING LOCATIONS

This appendix provides analysis of the legal privacy foundations of countries that are the most likely choices for offshore locations. Not done independently but taken from current offshoring and privacy-related publications, this analysis is not intended to be definitive with respect to the ability of each country's legal system to handle potential privacy disputes. We note, however, that none of the countries currently have privacy laws equivalent to those of the European Union or the United States, and, therefore, as discussed previously, we recommend that financial institutions take care to analyze choice of law issues.

India

No general data protection law exists, although some limited provisions exist in regulations that support statutes dealing with consumer protection and the prevention of terrorism. Under the Information Technology Act of 2000, "hacking"[11] entails imprisonment up to three years. In 1998, a national information technology (IT) task force recommended that the government should draft and pass regulations based on the United Kingdom Data Protection Act that are designed to oversee the handling of computerized data. That law, which is being drafted by the Ministry of Information Technology and the National Association of Software and Service Companies (NASSCOM), has yet to be enacted.

General characteristics:

- Very strong information technology (IT) and outsourcing industries are already in place.
- Poor national infrastructure.
- Generally low-cost base.
- Bangalore and Mumbai (formerly Bombay) are India's premier IT locations, but each has recently seen double-digit labor wage increases.
- Mumbai is India's major financial market; however, it suffers from high real estate costs, congestion, and pollution.
- Strong English language skills

China

No general data protection law exists. The freedom and privacy of network users is protected by law. Very few laws limit government interference with the collection, use, and disclosure of personal information.

[11] The Information Technology Act of 2000 defines someone who commits hacking as "Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means..."

General characteristics:

- Recently admitted to the World Trade Organization.
- Bureaucracy of non-democratic government can be a hindrance.
- Large labor pool, but language barriers exist.

Philippines

No general data protection law exists, although the Information Technology and E-Commerce Council recently proposed a data privacy law expected to adhere to European Union standards of data privacy. The Electronic Commerce Act of 2000 mandates a minimum fine and prison term of six months to three years for unlawful and unauthorized access to computer systems. Bank records are protected by the Bank Secrecy Act and the Secrecy of Bank Deposits Act.

General characteristics:

- Excellent English-speaking and high-tech skills.
- Low-cost base with moderate infrastructure.
- Potential for political instability with risks to foreign nationals.
- The skilled labor often seeks employment abroad.

Singapore

No general data protection law exists, and there is only a small division within the Ministry of Finance responsible for privacy and data protection. In 2002, the National Internet Advisory Committee released a draft "Model Data Protection Code for the Private Sector" that incorporates internationally recognized standards. The Code is available for self-regulatory adoption by the private sector. Privacy legislation has been under consideration for over a dozen years. The Banking Act prohibits disclosure of financial information without the permission of the customer.

General characteristics:

- Very strong financial services skills.
- Excellent infrastructure.
- High salaries and real estate costs.

Australia

The main statute is the Privacy Act of 1988, which created eleven Information Privacy Principles that are based on those in guidelines issued by the multinational Organization for Economic Cooperation and Development. The fourth of these eleven principles relates to storage and security of personal information.

In 2001, the private-sector amendments to the Privacy Act became operative. The new provisions provide for ten National Privacy Principles (NPP). Under the fourth NPP, an organization must take "reasonable steps" to protect the personal information it holds from misuse and loss and from unauthorized access, modification, or disclosure. There have been criticisms over the general descriptions of the ten NPPs and their enforcement, for example, over the fact that privacy complaints are handled initially by an industry-appointed authority.

General characteristics:

- Very strong financial services skills and availability.
- Costs are high relative to most of region.
- Very strong infrastructure.

Malaysia

No general data protection law exists, and there is no data protection agency. The Communications and Multimedia Act of 1988 contains a number of provisions on privacy, including a prohibition on unlawful interception of communications. The Banking and Financial Institutions Act of 1989 contains provisions on privacy with respect to banking information. The Ministry of Energy, Communications, and Multimedia is currently drafting the Personal Data Protection Act, a more comprehensive statute covering the collection, possession, processing, and use of and security of personal data.

General characteristics:

- Promising new technology corridor and government IT focus.
- Fair levels of infrastructures relative to Asia.
- Low cost of labor and real estate.

South Africa

No general data protection law exists. In 2002, the Law Commission began a project to draft a general national Privacy Act. Also in 2002, the Electronic Communications and Transaction Act was enacted. The Act contains statutory provisions on cyber crime including unauthorized access to data, the interception of or interference with data, and hacking. Personal privacy provisions have been deferred until the passage of the Privacy Act. Therefore, privacy protection currently relies on voluntary adoption by data collectors. Financial privacy is similarly covered by a code of conduct for banks issued by the Banking Council.

General characteristics:

- Very low real estate prices and low labor costs.
- Possess some specific industry skills.

Additional Sources for Country Risk Information

Table 1 lists different sources for country risk information. Additionally, 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.

Table 1: Sources for Country Risk Information

	Country Risks							
	Political	Economic	Transfer	Sovereign Default	Bond Ceilings	Bank Deposit Ceilings	Business Environment	General Country Risk
Control Risks Group	Y							
OECD			Y					
Fitch				Y	Y			
Moody's				Y	Y	Y		
S&P				Y				
Business Monitor International	Y	Y					Y	Y
Coface								Y
World Markets Research Centre	Y	Y					Y	Y
Economist Intelligence Unit	Y	Y	Y					Y
AM Best								Y
PRS International Country Risk Guide	Y	Y	Y					Y
Selected Risk Descriptions								
Political	Government stability, socioeconomic conditions, conflict, ethnic tensions, democratic accountability							
Economic	Growth, inflation, budget balance, current account balance							
Transfer	Foreign debt/GDP, debt service/exports, current account/exports, exchange rate stability							
Business Environment	Infrastructure, corruption, bureaucracy, legal framework, property rights, tax regime, capital markets, investment rules							
Source: FDIC. Developed as of April 2004 from recent publications and data suppliers.								

APPENDIX B
SUBCONTRACTING LANGUAGE FROM A TYPICAL DATA VENDOR CONTRACT

The following is an example of subcontracting language (emphasis added) from a data vendor contract.

3. CONDITIONS AND LICENSES

3.1 Performance by Subcontractors. Customer understands and agrees that the actual performance of the Services may be made by (Data Vendor), one or more Affiliates of (Data Vendor), **or subcontractors of any of the foregoing Entities (collectively, the 'Eligible providers').** For purposes of this Agreement, performance of the Services by any Eligible Provider shall be deemed performance by (Data Vendor) itself. (Data Vendor) shall remain fully responsible for the performance or non-performance of the Services by any Eligible Provider, to the same extent as if (Data Vendor) itself performed or failed to perform such services. **Customer agrees to look solely to (Data Vendor), and not to any Eligible Provider, for satisfaction of any claims, Customer may have arising out of this Agreement or the performance or nonperformance of Services.** However, in the event that Customer contracts directly with a Third Party for any products or services, (Data Vendor) shall have no liability to Customer for such Third Party's products or services, even if such products or services are necessary for Customer to access or receive the Services hereunder.

APPENDIX C
OUTSOURCING/OFFSHORING RISKS

The following is a summary of risks that are related to the issue of outsourcing. It should be noted that of the eight risk types identified below, only the first one, country risk uniquely pertains to outsourced work to another country. All the rest pertain equally to any outsourced work whether the work is performed domestically or not.[12]

1. Country Risk
   - Assets might be confiscated by one or more governments.
   - Confiscatory tax rates or assessments could be imposed.
   - Employee risk-related issues.
     - Background checks, etc.

2. Reputation Risk
   - Risks to earnings or capital could arise from negative public opinion.
     - Arises from poor service, disruption of service, or violations of consumer law.
     - Occurs when third-party interaction with bank customers is not consistent with the bank's policies or standards.
     - Occurs when there is negative publicity about adverse events involving the bank.

3. Operations/Transactional Risk
   - Risks to earnings or capital arise from problems with service or product delivery. The lack of an effective business resumption plan and appropriate contingency plans increase transaction risk.
     - Occurs when products, services, delivery channels, and processes do not fit with the bank's systems, customer demands, or strategic objectives.
     - Weak control over technology used in the third-party arrangement may result in threats to security and the integrity of systems and resources.
     - Can be the result of fraud or error by the third party.
     - Arises from inadequate capacity, technology failure, or lack of effective business resumption and contingency planning by the third party.
     - Possible risks include liquidity, interest rate, price, and foreign currency transaction risk.
     - Loss of trade secrets is possible when an outsource company also does work with competitors.

4. Compliance Risk
   - Risk to earnings or capital arises from violations of laws or regulations or nonconformance with internal policies or ethical standards. This risk exists when the activities of a third party are not consistent with law, policies, or ethical standards of

[12] Risk descriptions for numbers one through seven were derived from the FDIC, the OCC, the FRB, the OTS or the FFIEC.

the financial institution and the financial institution's country. This risk is exacerbated by an inadequate oversight and audit function.
  - Offshore vendors do not have the same privacy regulations as those that exist in the United States.
  - Can be due to improper review of products, services, or systems with respect to consumer law or other regulatory compliance matters.
  - Can occur if the bank's oversight program fails to include appropriate audit and control features.
  - Can occur if the vendor fails to adequately protect the privacy of nonpublic customer information.

5. Strategic Risk
   - This is a risk to earnings or capital arising from adverse business decisions or improper implementation. The financial institution is also exposed to strategic risk when it uses a third party to perform banking functions or to offer products or services that do not help the financial institution achieve corporate strategic goals and provide an adequate return on investment.
     - Occurs when banking functions or products or services are offered that are not compatible with the bank's strategic goals.
     - Can occur when third-party relationships are used without fully performing due diligence reviews.
     - Can occur when risk management's scope or depth is not commensurate with the activity.
     - Can occur when the bank does not possess the adequate expertise to oversee the third party.
     - Financial institutions face the potential for loss of trade secrets if poor controls exist when a vendor performs work for competitors in the same outsource location.

6. Credit Risk
   - This is a risk to earnings or capital that arise from the obligor's failure to meet the terms of any contract with the bank or to otherwise perform as agreed. The basic form of credit risk involves the financial condition of the third party itself. Appropriate monitoring of the activity of the third party is necessary to ensure that credit risk is understood and remains within board-approved limits.
     - Receivables quality declines as the third party performs inadequate account management, customer service, or collection activity.
     - Can occur when there is improper oversight of third parties who solicit and refer customers, conduct underwriting analysis, or set up other credit-related product programs.
     - Can occur when there is inadequate financial capacity by a third party to fulfill its contract with the bank.

7. Other Risks
   - Personnel security.
   - Network Security.

- Business continuity.
- Technology.
- Infrastructure (fragile, technical infrastructures that may be inordinately susceptible to physical disruptions).
- Information Security.
- Contractual.
- Legal.

8. Event Risk (Source: Financial Services Technology Consortium 2004).
    - Disruption in Telecommunications
        - Severing of lines, destruction of infrastructure, failure of a telecommunications company, capacity problems in the grid, equipment or software failure, virus attack, human error, etc.
    - Disasters at a facility
        - Fire, building collapse, employee violence, hazardous material transportation accident, long-term water or electrical outage, etc.
    - Natural Calamity
        - Hurricane, flood, tornado, earthquake, landslides, ice storms, heavy snowfall, extreme cold, etc.
    - Health Restrictions
        - Flu epidemic, SARS, Ebola, Aids, food poisoning, anthrax, biological weapons, plague, other infectious diseases.
    - Nuclear and chemical threats
        - Chemical spills and plant accidents, nuclear or chemical terrorism.
    - Visa Restrictions
        - Government applies a quota or limit to visas that is lower then normal, processing time increases because of background checks, increased rejection of visa applications, etc.
    - Travel Restrictions/Aviation Accidents

APPENDIX D
OUTSOURCING-RELATED GUIDANCE

Despite their relative newness, offshoring issues from a regulatory perspective are covered by previously released regulatory guidance regarding outsourcing. Relevant regulatory guidance comes in the form of guidelines from the Federal Financial Institutions Examination Council, the FDIC, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the National Credit Union Administration, and include the following:

FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

Guidance

- **Risk Management of Outsourced Technology Services** (November 28, 2000). This guidance outlines the processes banks should use to manage the risks associated with outsourcing technology services.

Guidance in Draft Form

- **FFIEC Update of "Information Technology Outsourcing Booklet."** This will discuss how institutions should manage outsourced information technology relationships, from an initial risk assessment through on-going monitoring.

FEDERAL DEPOSIT INSURANCE CORPORATION

Guidance

- **FIL-49-99: Bank Service Company Act** (June 3, 1999). This FIL reminds FDIC-supervised institutions of the reporting requirements contained in Section 7 of the Bank Service Company Act, and provides a standard form to facilitate compliance.

- **FIL-81-2000: Risk Management of Technology Outsourcing** (November 29, 2000). This FIL provides interagency guidance on managing the risk exposure an institution faces when it contracts with an information technology service provider.

- **FIL-50-2001: Bank Technology Bulletin: Technology Outsourcing Information Documents** (June 4, 2001).
  - Attachments:
    "Effective Practices for Selecting a Service Provider"
    - Provides banks with information and suggestions regarding Selection of a competent and qualified service provider.

    "Tools to Manage Technology Providers' Performance Risk: Service Level Agreements."
    - This brochure discusses the Service Level Agreement as an effective tool for managing the risks associated with technology outsourcing and

describes practices for measuring and monitoring service providers' performance.

"Techniques for Managing Multiple Service Providers."

- This document serves as a resource for banks in addressing specific challenges relating to selecting an information technology service provider. The content was prepared not as examination procedures or official guidance but as an informational tool for community bankers.

- **FDIC FIL-23-2002: Country Risk** (March 11, 2002). This FIL describes the elements of an effective country risk management process and is intended to guide examiners when they evaluate the management of country risk in internationally active banks.

Guidance in Draft Form

- **FDIC FIL: "Guidance Concerning Bank Use of Foreign-Based Third-Party Service Providers."** This FIL provides guidance on specifically managing the risk exposure an institution faces when it contracts with a foreign information technology service provider.

FEDERAL RESERVE BOARD

Guidance

- **SR 00-4 (SUP), Outsourcing of Information and Transaction Processing** (February 29, 2000). This letter reiterates and clarifies the Federal Reserve's expectations regarding the management of outsourced information and transaction processing activities by banks, either to affiliated institutions or third-party service providers.

- **SR 00-17 (SPE) Guidance on the Risk Management of Outsourced Technology Services** (November 30, 2000). This letter informs institutions of the guidance issued by the FFIEC to financial institutions regarding risk management of outsourced technology services.

White Paper

- **FRBNY White Paper: "Outsourcing Financial Services Activities: Industry Practices to Mitigate Risks"** (August 29, 1999). This paper summarizes industry practices to identify, measure, monitor, and control applicable risks. It reviews outsourcing as a business strategy.

OFFICE OF THE COMPTROLLER OF THE CURRENCY

Guidance

- **OCC Bulletin 2002-16: Bank Use of Foreign-Based Third-Party Service Providers** (May 15, 2002). This bulletin provides guidance to national banks on

managing risks that may arise from their outsourcing relationships with foreign-based third-party service providers.

- **OCC Bulletin 2002-10: Country Risk** (March 11, 2002). This statement describes the elements of an effective country risk management process and is intended to guide examiners when they evaluate the management of country risk in internationally active banks.

- **OCC Bulletin 2001-8: Guidelines Establishing Standards for Safeguarding Customer Information** (February 15, 2001). The purpose of this bulletin is to alert National Banks, Service Providers and Software Vendors of the joint-agency issuance of the guidelines establishing standards for safeguarding customer information and to highlight provisions of the guidelines. The guidelines describe the OCC's expectations for the creation, implementation, and maintenance of a comprehensive information security program.

- **OCC Bulletin 2001-47: Third-Party Relationships** (November 1, 2001). This bulletin provides guidance to national banks on managing the risks that may arise from their business relationships with third parties. A bank's use of third parties to achieve its strategic goals does not diminish the responsibility of the board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws.

- **OCC Bulletin 2000-21: Privacy of Consumer Financial Information** (June 20, 2000). In June 2000, the OCC published jointly with the FRB, the FDIC and the OTS a new regulation, 12 CFR Part 40 to implement privacy provisions of the Gramm-Leach-Bliley Act (GLBA). This bulletin contains a copy of the final rule as it appeared in the *Federal Register* and contains a summary of the final rule that the OCC prepared to assist national banks in their compliance efforts.

White Paper

- **OCC White Paper: "Cross-Border Outsourcing and Risk Management for Banks"** (August 13, 2003). This article outlines the risk management challenges banks face when information technology and business processes are outsourced to offshore locations.

OFFICE OF THRIFT SUPERVISION

Guidance

- **Thrift Bulletin 82: Third-Party Arrangements** (March 18, 2003). This document provides guidance on third-party arrangements, whether they occur between affiliated or unaffiliated entities. The bulletin informs institutions that the OTS expects directors and management to effectively manage risks that arise from all types of third-party arrangements. It also notifies thrifts that OTS examiners will review internal controls and management of third-party arrangements during the course of

regularly recurring safety and soundness examinations, and will request appropriate corrective action, when needed, to ensure that the arrangements satisfy safety and soundness standards.

- **CEO Letter 113: Internal Controls** (July 14, 1999). This memorandum issued for CEO of thrifts reminds management of the importance of maintaining strong internal controls and that each savings association must have internal controls and an internal audit appropriate to the size of the association and the nature and scope of its activities.

- **CEO Letter 133: Risk Management of Technology Outsourcing** (November 29, 2000). This letter informs thrift CEO of the guidance issued by the FFIEC to financial institutions regarding risk management of outsourced technology services.

- **Thrift Activities Handbook: Section 340, Internal Control Program**. Examination guidelines were issued in February 2002 as part of the OTS Regulatory Handbook establishing the objectives and procedures for assessing institutions' internal control systems.

- **Thrift Activities Handbook: Section 341, Technology Risk Controls**. Examination guidelines were issued in January 2002 as part of the OTS Regulatory Handbook establishing the objectives and procedures for assessing institutions' technology risk controls.

NATIONAL CREDIT UNION ADMINISTRATION

Guidance

- **NCUA Letter to Credit Unions No. 02-CU-17: E-Commerce Guide for Credit Unions**. This letter provides NCUA's e-Commerce Guide for credit unions. It offers information to assist credit unions engaging in, or considering, e-Commerce activities in the form of electronic delivery of financial services via the Internet.

- **NCUA Letter to Credit Unions No. 01-CU-20: Due Diligence over Third-Party Service Providers**. This letter reminds credit union officials that they are responsible for planning, directing, and controlling the credit union's affairs. It establishes the requirement of due diligence review prior to entering into any arrangements with a third party.

- **NCUA Letter to Credit Unions No. 00-CU-11: Risk Management of Outsourced Technology Services**. This letter informs credit unions of the guidance issued by the FFIEC to financial institutions regarding risk management of outsourced technology services.

SOURCES

A.T. Kearney, Inc. 2004. "A.T. Kearney's 2004 Offshore Location Attractiveness Index. Making Offshore Decisions". April 2004.

———. 2004b. Conference call discussing trends and privacy risks relative to the offshoring of financial institution functions. April 22, 2004.

———. 2004b. What to Move Offshore? Selecting IT Activities for Offshore Locations. Gartner Paper. March, 2004.

Adrian, B. 2003. Make Sure Outsourcing is a Good Idea for your Call Center. Gartner Research Note, June 18, 2003.

Bank Service Company Act. 1962. 12 U.S.C. §§ 1861-1867(c).

Banking Industry Technology Secretariat ("BITS"). 2004. Meeting with BITS staff discussing privacy risks relative to the offshoring of financial institution functions. Additional discussion related to discussion of the BITS Framework . . . (referenced below). April 13, 2004.

———. 2004a. Conference call with BITS staff discussing privacy risks relative to the offshoring of financial institution functions. April 8, 2004.

———. 2004b. BITS IT Service Provider Expectations Matrix (Washington, DC). January 2004.

———. 2003. BITS Framework for Managing Technology Risk for IT Service Provider Relationships (Washington, DC). November 2003.

Basel Committee on Banking Supervision. 2003. Management and Supervision of Cross-Border Electronic Banking Activities. July 2003.

Cocheo, Steve. 2004. Global Think? Or Job Shrink?. ABA Banking Journal. May 2004: 41-42 and 64-65.

Cournoyer, Susan. 2003. Financial Services Providers Steer IT Spending Toward Outsourcing and Business Process Expertise. Gartner Research Note, May 9, 2003.

———. 2003a. FSPs Forge Ahead with IT and Business Process Outsourcing. Gartner Research Note, June 20, 2003.

———. 2003b. Midsize Banks Seek Answers About Outsourcing. Gartner Research Note, December 9, 2003.

DeLotto, Richard. 2002. Financial Service Providers: Plan for the Unthinkable. Gartner Research Note, June 13, 2002.

———. Some U.S. Outsourcing Risks are Often Overlooked. Gartner Research Note, June 17, 2003.

Earley, Annemarie. 2003. FSP Outsourcing Grows beyond Tactics to Strategies. Gartner Research Note, June 24, 2003.

Electronic Data Systems. 2004. Conference call with EDS staff discussing privacy risks relative to the offshoring of financial institution functions. May 15, 2004.

Federal Deposit Insurance Corporation. 2004. Meeting with New York Regional Office bank examination staff discussing privacy risks relative to the offshoring of financial institution functions. April 26, 2004.

———. 2004. Conference call with bank examination staff discussing the operations of data service provider Jack Henry. April 14, 2004.

———. 2004. Conference call with bank examination staff discussing the operations of data service provider Metavante. April 9, 2004.

Financial Services Technology Consortium. 2004. Minimum Required Practices for Outsourcing Production Support of an Application to an Offshore Provider. January 2004.

Free, Don. 2003. Core Banking Vendors are Going Offshore. Gartner Research Note, June 18, 2003.

———. Core Banking Vendors are Going Offshore. 2003. Gartner Research Note, June 18, 2003.

Galati, Joseph L. Federal Reserve Bank of New York. 2004. Offshoring: Supervisory Implications and Approaches. A presentation at the International Supervision Conference for Developed Nations. March 31, 2004.

Garcia, Virginia. 2004. Offshore Outsourcing Gets Political: FSIs Armor Up, Talk Less, and Do More. Tower Group Viewpoint, iss. 83, March 2004.

Gartner Group. 2004. Conference call discussing trends and privacy risks relative to the offshoring of financial institution functions. April 29, 2004.

Jones, Wendell. 2002. Competitive Supplier Strategies for the Global Marketplace. Cutter Consortium Executive Report. Sourcing Vol.3, No. 4.

Knox, M. Financial Services Risk Management. 2003. Gartner Research Note, September 30, 2003.

Karamouzis, Frances. 2003. A Look at India for Offshore Sourcing Options. Gartner Research Note, July 29, 2003.

Kelly, Hugh. Office of the Comptroller of the Currency. 2004. Cross Border Outsourcing: A Regulatory Perspective. A presentation at the International Supervision Conference for Developed Nations. March 31, 2004.

Litan, Avivah and Knox, Mary. 2003. Outsourcing is now a Strategic Issue in Financial Services. Gartner Research Note, June 24, 2003.

Lowes, Peter and Woosley, Frank. Deloitte Group. 2004. Offshoring and Cross-Border Outsourcing by Banks. A presentation at the International Supervision Conference for Developed Nations. Much of the material in the presentation related to Deloitte's 2003 FSI Offshore Survey. March 30, 2004.

McCarthy, John C. 2004. Near-Term Growth of Offshoring Accelerating. Forrester Research, Inc., May 14, 2004.

Metavante. 2004. Conference call with Metavante staff discussing privacy risks relative to the offshoring of financial institution functions. April 26, 2004.

Morello, Diane. 2003. The Organizational Implications of Offshore Outsourcing, Gartner Research Note, October 24, 2003.

Office of Thrift Supervision. 2004. Meeting with examination policy staff regarding the oversight of offshoring and their database used to track outsourcing relationships at thrifts. April 26, 2004.

Organisation for Economic Co-Operation and Development. 1980. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, revised 2002 (Paris, France).

Terdiman, Rita. 2000. Offshore Programming: Country Issues. Gartner Research Note, September 28, 2000.

———. 2002. Analysis of India: Today's Dominant Offshore Outsourcer. Gartner Research Note, January 16, 2002.

Stokes, Bruce. 2004. And Away They Go. National Journal, March 27, 2004: 940-956.

Tower Group. 2004. Conference call discussing trends and privacy risks relative to the offshoring of financial institution functions. April 23, 2004.

U.K. Financial Services Authority. 2001. Interim Prudential Sourcebook for Banks. Principles of Outsourcing, sec. 4, p. 1. June 2001.

U.S.A. Patriot Act. 2001. Pub. L. No. 107-56. 107th Cong. 2nd sess., October 26, 2001.

World Bank, World Bank 2003 Banking Survey, March 2004 (http://www.worldbank.org/research/interest/2003_bank_survey/wb_banking_survey_032904.xls).