Order Code RS21809
Updated June 9, 2004

Financial Services Industry Outsourcing and Enforcement of Privacy Laws

M. Maureen Murphy and Angie A. Welborn
Legislative Attorneys
American Law Division

Summary

Concerns about enforcement of customer privacy laws across international boundaries have been raised as the perception grows that more U.S. financial service companies are outsourcing to foreign service providers. This report addresses some frequently asked questions about the enforcement of federal laws requiring the safeguarding of customer financial information in the context of this outsourcing. This report will be updated as events warrant.

What is Outsourcing? Outsourcing refers to a business practice of securing outside providers for functions once performed internally or for new functions that support or augment internal operations and otherwise would be performed inside the business, itself. Retaining core functions and farming out peripheral operations is known as strategic outsourcing and is usually a means of maintaining a "competitive edge."[1]

What Functions May Be Outsourced? Unless a statute, regulatory mandate, a company's charter, or other legal constraint precludes it, outsourcing of any function or operation is possible. Financial services companies, particularly depository institutions, are accustomed to close regulatory scrutiny and have been provided with various forms of regulatory guidance on outsourcing.[2] Functions that are commonly outsourced are "core processing; information and transaction processing and settlement and activities for lending; deposit-taking, funds transfer, fiduciary, or trading activities; Internet related services; security monitoring; systems development and maintenance; aggregation services; digital certification services; and call centers.... [and] human resources administration and internal audit."[3] Among the few functions that may not be outsourced

[1] Ann H. Spiotto and James E. Spiotto, "The Ultimate Downside of Outsourcing: Bankruptcy of the Service Provider," 11 *Am. Bankr. Inst. L. Rev.* 47 (2003).

[2] See, e.g., Federal Financial Institutions Examination Council (FFIEC), FFIEC TSP, "Supervision of Technology Service Providers (March 2003).

[3] Julie L. Williams and James. F. E. Gillespie, Jr., "The Impact of Technology on Banking: The (continued...)

are those which must be performed by officers or personnel of the institution (e.g., certification of the accuracy of annual reports, as required under the Sarbanes-Oxley Act of 2002.)[4]

What Financial Institutions Outsource Customer Information? Virtually any financial institution (e.g., any bank, thrift, credit union, securities firm, insurance company, tax preparation service, credit bureau, accounting firm, money transmitting business, and check cashing business) is likely to have some arrangement with outside entities to process data, either in lieu of processing it in-house or as a back-up in emergency situations. Banks, for example, rely on outside firms for printing checks, issuing credit cards, processing transactions, preparing billing statements, operating call centers and other customer service centers, and processing customer payments.

What Legal Arrangements Do Financial Institutions Make for Outsourcing? Typically, a financial institution's outsourcing arrangement will involve a contract. The contract may be with a wholly independent company or a separately incorporated subsidiary or a service company in which the institution maintains a capital investment; or, it may take the form of a joint venture with another company. The contract generally will specify the duties and rights of each of the parties, the remedies for any breach, the law that is to be applied to interpret the contract, and any other agreements of the parties.

What Foreign Entities Provide Services Outsourced By Financial Institutions? Third-party[5] foreign- or domestic- based businesses may perform outsourced functions for financial institutions. They may be independent of the financial institution or in some way subject to the oversight of the financial institution by way of a capital investment, a joint venture partnership, a corporate affiliation, or other form of arrangement.[6] If the operations or services provided are performed in a foreign jurisdiction, the third-party service provider is likely to be subject to the laws of that jurisdiction, whether or not it is a subsidiary of a U.S. company or incorporated in the foreign jurisdiction.[7] India and other South Asian countries are emerging centers of outsourced technology and services.[8]

---

[3] (...continued)
Effect and Implications of 'Deconstruction' of Banking Functions," 5 *N.C. Banking Institute* 135 140 (April 2001). [Hereinafter, *Impact of Technology*].

[4] P.L. 107-204 § 302; 116 Stat.745, 777; 15 U.S.C. § 7241.

[5] The customer and the institution are considered the primary parties in this context.

[6] See *Impact of Technology*, at 142, indicating an emerging trend toward investing in technology service providers, rather than merely contracting with them.

[7] OCC Bulletin OCC 2002-16, "Bank Use of Foreign-Based Third-Party Service-Providers," (May 15, 2002), 2002 OCC CB LEXIS 36 (May 15, 2002).

[8] A report by Chris Gentle for Deloitte Consulting Firm, predicted that "future offshore activity will be spread around the Indian Ocean Rim, from South Africa through the Indian sub-continent to China, Malaysia and down to Australia." Gale Group, Inc., Financial Services Distribution (June 1, 2003), LEXIS;BANKNG Library, CURNWS file, avail. Mar. 25, 2004.

Where May the Outsourced Service Be Performed? Whether the provider is a domestic or foreign, the service may be performed either in or outside the United States, provided it is not performed in violation of existing terrorist or country sanctions under programs administered by the Office of Foreign Assets Control[9] or any applicable export control law.

What Governs the Confidentiality of Financial Institution Customer Information? Until the 1970's, confidentiality requirements for financial institutions were generally imposed under state law. Since then, with the passage of the Fair Credit Reporting Act (FCRA)[10] and Title V of the Gramm-Leach-Bliley Act (GLBA),[11] the financial service industry is subject to broadly applicable federal confidentiality requirements that may, to some extent, be supplemented by state law. FCRA sets forth responsibilities for credit bureaus and the entities that furnish consumer information to them. It preempts state law on, and sets standards for, sharing of customer information among affiliated companies. GLBA sets the standards for sharing of nonpublic customer information by financial institutions with nonaffiliated third parties. It does not preempt state laws that provide more consumer protection.

What Safeguards Are in Place to Protect the Privacy of Customer Information Outsourced by Financial Institutions? GLBA requires the regulators of financial institutions[12] to issue rules "relating to administrative, technical, and physical safeguards ... to insure the security and confidentiality of customer records and information ... and ... to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." Banking institutions, thrifts, and credit unions are required by law to notify their federal regulator of any contract or arrangement with a third-party service provider.[13] Each of the federal financial institution regulators has issued a safeguards rule[14] that addresses the outsourcing of such information, emphasizing that the confidentiality obligation remains with the financial institution. The federal banking regulators have issued guidance on

---

[9] [http://www.treas.gov/offices/eotffc/ofac/sanctions/index.html].

[10] 15 U.S.S. §§ 1681 et seq.

[11] P.L. 106-102, 113 Stat. 1338, 1436, 15 U.S.C. §§6801 et seq.

[12] These are the: Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), Federal Reserve Board (FRB), Office of Thrift Supervision (OTS), Securities and Exchange Commission (SEC), National Credit Union Administration (NCUA), with respect to the depository institutions which they regulate, and the Federal Trade Commission (FTC), with respect to all other entities coming under the definition of "financial institution" in GLBA's privacy title, except for insurance companies. The safeguards standards for insurance companies are to be administered by state insurance authorities.

[13] 12 U.S.C. § 1867(c); 12 U.S.C.§ 1464(d)(7)(D)(ii).

[14] Federal depository institution regulators' documents can be found at the FFIEC Website. [http://www.ffiec.gov/exam/InfoBase/toc_s/02-ffi-table_of_contents_select.html]. The SEC and FTC safeguards rules are 17 C.F.R. § 248.30 and 16 C.F.R., Part 314. See also, 68 *Fed. Reg.* 47954 (Aug. 12, 2003), proposing "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice."

third-party relationships or on outsourcing, particularly outsourcing technology.[15] Generally, these guidelines require adequate due diligence and risk management assessment, as well as contractual provisions, to assure that service providers are capable of, take steps to, and actually implement safeguards to protect customer information.[16] Examiners of depository institutions are required to evaluate the measures taken by the institutions to oversee service providers.[17]

Is A Financial Institution Liable for Breaches of Security by Service Providers? Any financial institution that is subject to a state or federal statutory duty of maintaining confidentiality of customer information may not avoid that responsibility by contracting out or otherwise shifting the operation to another entity. Not only does GLBA[18] require that any contractual or joint venture agreement with a third-party service provider cover the confidentiality of nonpublic personal customer information, but the actions of the contractor will be attributed to the financial institution under the law of agency.

What Regulatory Tools Are Available To Monitor Service Providers? There is a range of regulatory, criminal, and private enforcement options available depending upon the particular situation. All third-party service providers of federally regulated depository institutions may be examined by the appropriate federal banking agencies,[19] even in foreign countries.[20] Federal regulators may police privacy

---

[15] *Id.* The FFIEC Website assembles some of the guidelines applicable to depository institutions by regulatory agency.

[16] See, e.g., FRB, SR 00-4(SUP), "Outsourcing of Information and Transaction Processing" (Feb. 29, 2000). Among other things, such contracts must provide for compliance with regulatory requirements and for access by federal regulators. OCC Bulletin OCC 2002-16 (May 15, 2002), addresses "Bank Use of Foreign-Based Third-Party Service Providers." It requires that the contract "state that all information shared by the bank with a foreign-based third-party service provider, regardless of how the service provider processes, stores, copies, or otherwise reproduces it, remains solely the property of the bank." *Id.*, at 4. It provides that "[a] bank's use of a foreign-based service provider must not inhibit its ability to comply with all applicable U.S. law and regulations. These include requirements concerning accessibility and retention of records ... and other U.S. consumer protection laws and regulations." *Id.*, at 3. The guidance suggests contract provisions protecting customer privacy and requires a provision authorizing OCC examination of the third-party service provider. It also mandates provisions prohibiting the redisclosure of bank data or information, compliance with OCC privacy regulations, and implementation of security measures to maintain confidentiality.

[17] "Examination Procedures to Evaluate Compliance With the Guidelines to Safeguard Customer Information." [http://www.ffiec.gov/exam/InfoBase/toc_s/02-ffi-table_of_contents_select.html].

[18] 15 U.S.C. § 6802(2).

[19] 12 U.S.C. § 1867(c).

[20] OTS requires 30-day advance notice from thrifts contemplating third-party service arrangements with foreign service providers and requires them to include in any contract a provision that the services are subject to OTS examination. Thrift Bulletin TB 82, at 5 (March 18,2003). The OCC guidance has a similar requirement. OCC Bulletin OCC 2002-16, at 5-7. It states that "a national bank should not outsource any of its information or transaction processing to third-party service providers that are located in jurisdictions where the OCC's full and complete access to data or other information may be impeded by legal, regulatory, or

(continued...)

requirements administratively with fines, cease and desist orders, prohibitions on further dealings, and various other strictures on operations.[21] Transgressions that involve criminal activity such as computer or wire fraud or larceny may be prosecuted under federal and state criminal laws.[22] Victims may be able to resort to a federal or state law that authorizes civil suits to recover damages.[23] Contractors of federally regulated depository institutions fall within the definition of "institution-affiliated parties" and may be prosecuted for knowingly or recklessly participating in violating a law, regulation, or fiduciary duty or contributing to an unsafe or unsound practice. 12 U.S.C. § 1813(u).

What Obstacles May Arise in Enforcement Actions Involving Foreign Outsourcing? Foreign outsourcing involves risks that the foreign law will change or that the foreign government will not cooperate in enforcement of U.S. laws, requests for judicial process, or for extradition. These can be ameliorated by contractual provisions and by treaty arrangements with the foreign governments. To discharge their privacy obligations, U.S. financial institutions must require third party service providers to adhere to the applicable provisions of GLBA, including those on redisclosure and security of information.[24] Before entering into contracts with service providers based in foreign countries, financial institutions must assess the political, social and economic stability of the foreign country and its legal framework, including the privacy regime and the financial institution's ability to enforce U.S. privacy laws. Contractual provisions that address choice of law issues, such as which country's law is to apply to the various elements of the contract; which courts will have jurisdiction over any contract claim; and alternative dispute resolution options are means by which the financial institution may ameliorate some of the risks associated with conducting business with a party operating

---

[20] (...continued)
adminstrative restrictions unless copies of all critical records also are maintained at the bank's U.S. offices....If circumstances warrant, the OCC may examine a national bank's outsourcing arrangement with a foreign-based service provider. If the provider is a regulated entity, then the OCC may arrange through the appropriate foreign supervisor(s) to obtain information related to the services provided to the bank and, if significant risk issues emerge, to examine those services."

[21] Banking regulators have at their disposal a comprehensive array of administrative tools, most of which are found in section eight of the Federal Deposit Insurance Act (FDIA) and range from informal actions, formal cease and desist orders, and civil money penalties. 12 U.S.C. § 1818. Among the administrative enforcement remedies available are: termination of deposit insurance; cease and desist orders; temporary cease and desist orders; removal orders; and civil money penalties. OCC has used this authority to enforce the GLBA privacy requirements. On April 7, 2003, the agency assessed civil money penalties of $20,000 and $10,000 against two former national bank employees and issued an order requiring their permanent removal from banking for unauthorized e-mailing of customer data, and electronic loan files.

[22] Some offenses may involve federal mail fraud, 18 U.S.C. § 1342; wire fraud, 18 U.S.C.§ 1343; or computer fraud, 18 U.S.C. § 1030 , and may act as predicate offenses for racketeering, 18 U.S.C. §§ 1961, et seq., or money laundering, 18 U.S.C. § 1956, prosecutions.

[23] California's financial privacy law imposes more requirements on joint marketing agreements with third-party providers than does GLBA and provides for individual lawsuits to enforce its provisions. See CRS Report RS21614, *Comparison of California's Financial Information Privacy Act of 2003 With Federal Privacy Provisions.*

[24] 15 U.S.C. §§ 6802(c) and 6801(b).

in a foreign country. Nonetheless, since the activity is to be conducted on territory over which a sovereign other than the United States has jurisdiction, there is always the possibility that the laws of the other sovereign, including any changes in the foreign law, may have an effect upon the performance or interpretation of the contract.[25] Contracts, thus, often include clauses indicating the allocation or assumption of the risks associated with nonperformance in such situations.[26] Enforcement of U.S. criminal laws extraterritorially involves: (1) a valid basis of extraterritorial enforcement,[27] (2) statutory authority for extraterritorial enforcement,[28] and (3) cooperation of the foreign government through treaties or other agreements for assistance in law enforcement matters.[29] For further information, see FDIC's *Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks* at [http://www.fdic.gov /regulations/examinations/offshore/index.html] (June 2004).

What Remedies Are Available to Victims of Identity Theft Resulting From Outsourcing? Victims of identity theft resulting from the outsourcing of financial information would have the same remedies available to them as victims under other circumstances. There are no laws specifically aimed at preventing identity theft or assisting victims when financial information has been outsourced. Thus, victims would need to use the generally applicable laws discussed in CRS Report RL31919, *Remedies Available to Victims of Identity Theft*, to clear their credit records of inaccurate information resulting from the theft and challenge unauthorized charges on credit and debit cards.

---

[25] According to Comment (a), relating to subsection (1) of § 441 of the *Restatement (Third) of the Foreign Relations Law of the U.S.* (1986), which addresses foreign state compulsion,: "a state may not, absent unusual circumstances, require a person, even one of its nationals, to do abroad what the territorial state [foreign country] prohibits."

[26] See, *Restatement (Second) Conflict of Laws* § 201 (1971).

[27] If the offense is committed outside the United States, jurisdiction may be predicated on the occurrence of a significant effect within the United States. See, C. L. Blakesley, "Extraterritorial Jurisdiction," in M. Cherif Bassiouni, *International Criminal Law* 33, 50 (2d ed. 1999).

[28] The federal money laundering statute provides jurisdiction, if conduct by a non-U.S. citizen occurs in part in the U.S. and the transaction involves $10,000 or more. 18 U.S.C. § 1956(f). For further information, see CRS Report RS21306, *Terrorism and Extraterritorial Jurisdiction in Criminal Cases: Recent Developments in Brief*, at 4.

[29] For further information about this topic, including lists of: (1) the jurisdictional bases for extraterritorial application of a nation's criminal laws, (2) federal criminal statutes that include provisions for extraterritorial enforcement, see CRS Report 94-166A, *Extraterritorial Application of American Criminal Law*.