LJN LAW JOURNAL NEWSLETTERS

THE PRIVACY & DATA PROTECTION LEGAL REPORTER™

Volume 1, Number 1 • November 2005 ALM

Privacy and Security Obligations of Banks and Financial Institutions

An Overview of Federal Requirements

By Mark E. Plotkin and B.J. Sanford

Businesses and regulators alike are re-evaluating policies, procedures, and systems for protecting private data in light of recent high-profile security breaches. In addition to increased scrutiny from the public at large, financial institutions face a growing body of law addressing the privacy and security of customer data.

Federal, state, and foreign legislators and regulators have contributed to that growing body of law. State and foreign initiatives have received considerable attention. California, for example, created a stir in 2002 by passing SB 1386, which requires any company that stores customer data electronically to notify its California customers of security breaches that affect those customers' personal information. Cal. Civ. Code §1798.82. Less recent but no less prominent, Directive 95/46/EC of the European Union set forth a wide range of privacy and security principles affecting businesses operating in the EU member states and has now been implemented, with variations, by every member state. Council Directive 95/46/EC 1995 O.J. (L 281); *see also* European Commission, Data Protection, at *http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm*. This article focuses on federal sources of data security obligations for financial institutions, which have received less recent attention than state and foreign sources.

Federal statutory and regulatory initiatives addressing the privacy and security of customer data have generally come in two forms: consumer rights initiatives, such as notice and disclosure requirements that grant customers increased control over nonpublic personal information, and security obligations that seek to protect against unauthorized access to that information. Commentators have written extensively about the former; this article focuses on the latter. *See, e.g.*, Charles M. Horn, *Financial Services Privacy at the Start of the 21st Century: A Conceptual Perspective*, 5 N.C. Banking Inst. 89 (2001); *see also* Michael A. Benoit & Elena A. Lovoy, *Recent Federal and State Consumer Financial Privacy Developments*, 57 Bus. Law. 1209 (2002).

A number of federal statutes directly or indirectly prescribe data security obligations for financial institutions. Additionally, and of greater practical importance, federal agencies implementing those statutes have set forth detailed regulations and guidelines regarding data security. Finally, various federal statutes and regulations not directed primarily at financial institutions nonetheless affect the data security obligations of those financial institutions within their scope.

The Data Security Statutory Regime

The most basic security obligations for financial institutions under federal law date back to the Bank Protection Act of 1968 ("BPA"). 12 U.S.C. §§1881-84. The BPA required the financial institutions regulatory agencies ("agencies") to establish minimum standards for security devices and procedures for financial institutions in order to discourage and better investigate robberies, burglaries, and larcenies. For purposes of this article, the financial institutions regulatory agencies include: the Federal Deposit Insurance Corpor-ation ("FDIC"); the Board of Governors of the Federal Reserve System ("Federal Reserve Board" or "FRB"); the Office of the Comptroller of the Currency ("OCC"); and the Office of Thrift Supervision ("OTS").

More recently, Congress has focused its attention specifically on the privacy and security of customers' nonpublic personal information. In 1999, Congress passed the Gramm-Leach-Bliley Act ("GLBA"), which contained substantial notice and disclosure requirements but also authorized the agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards. Even more recently, the Fair and Accurate Credit Transactions Act ("FACTA") required the agencies to issue regulations requiring proper disposal of consumer information derived from consumer reports for a business purpose. 15 U.S.C. §§6801-09, 6821-27.

In addition to statutes that explicitly relate to data security obligations, financial institutions should be aware of the various federal statutes that prescribe obligations related to data security. For example, the Right to Financial Privacy Act, 12 U.S.C. §§3401-22, bars financial institutions from releasing the financial records of a customer to the federal government except under specified circumstances. The Fair Credit Reporting Act, 15 U.S.C. §1681, regulates the compila-

tion, use, and disclosure of consumer reports. And the Bank Secrecy Act, 31 U.S.C. §§5311-32, amended by the anti-money laundering provisions of the USA PATRIOT Act, sets forth substantial financial recordkeeping and reporting requirements. While these statutes and their implementing regulations do not explicitly specify data security obligations, financial institutions must take them into account in designing their data security policies, procedures, and systems.

The Data Security Regulatory Regime

General Security Obligations

Pursuant to the BPA, the various financial institutions' regulatory agencies have established substantially similar minimum standards for security devices and procedures. 12 C.F.R. pt. 21; 12 C.F.R. §208.61; 12 C.F.R. pt. 326; 12 C.F.R. pt. 568. These standards focus on the security of the physical plant, but protect against unauthorized physical access to customers' personal data as well. Now, more than 3 decades since its passage, financial institutions are well aware of their general security obligations under the BPA and its implementing regulations.

Information Security Programs

More specifically addressing data security, the agencies have together published the Interagency Guidelines Establishing Information Security Standards ("Guidelines"), implementing the data security provisions of the GLBA and FACTA. 12 C.F.R. pt. 30; 12 C.F.R. pt. 208; 12 C.F.R. pt. 211; 12 C.F.R. pt. 225; 12 C.F.R. pt. 263; 12 C.F.R. pt. 308; 12 C.F.R. pt. 364; 12 C.F.R. pt. 568; 12 C.F.R. pt. 570; *cf.* 16 C.F.R. pt. 314 (applying similar standards to financial institutions under the jurisdiction of the Federal Trade Commission). When first published, the Guidelines were known as the Interagency Guidelines Establishing Standards for Safeguarding Customer Information. The Guidelines require each financial institution to adopt a written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities. A financial institution must coordinate all elements of its information security program. A financial institution must also ensure that its subsidiaries are subject to comprehensive information security programs, either by sweeping them within the scope of the parent institution's program or by ensuring that subsidiaries establish their own information security programs.

Financial institutions must design their information security programs to fulfill the objectives of the GLBA and FACTA. Specifically, information security programs must: 1) ensure the security and confidentiality of customer records and information; 2) protect against threats or hazards to the security or integrity of those records; 3) protect against unauthorized access to or use of those records; and 4) ensure proper disposal of customer and consumer information.

The Guidelines set forth five general requirements for a financial institution's information security program. First, a financial institution's board of directors must be involved. The board, or a committee of the board, must approve the institution's information security program as well as oversee its development, implementation, and maintenance. At least annually, an institution must detail its information security program and its compliance with the Guidelines in a report to the board.

The second general requirement sets forth that a financial institution must affirmatively assess data security risks. An institution must identify reasonably foreseeable internal and external threats that could lead to unauthorized use or destruction of customer information. In doing so, an institution must assess the likelihood and potential damage of those threats, taking into account the sensitivity of customer information, and assess the sufficiency of policies, procedures, and systems designed to address those threats.

Third, a financial institution must manage and control identified data security risks. An institution must design its information security program to control those risks, including appropriate measures to dispose of customer and consumer information. An institution must also train its staff to implement its information security program and conduct regular, independent tests of the key controls, systems, and procedures. The Guidelines specify a number of security measures for financial institutions to consider for managing and controlling risks, including: 1) access controls to customer information systems, including authentication controls; 2) access restrictions to physical locations containing customer information; 3) encryption of electronic customer information; 4) procedures for modifying customer information systems consistent with other requirements; 5) dual control procedures, segregation of duties, and background checks for employees with access to customer information; 6) monitoring systems to detect attacks on or intrusions into customer information systems; 7) response programs for unauthorized access to customer information, including reports to regulatory and law enforcement agencies; and 8) measures to protect against loss of customer information due to environmental hazards, such as fire damage, water damage, or technological failures.

For the fourth Guidelines general requirement, a financial institution must oversee arrangements with its service providers. An institution must exercise appropriate due diligence in selecting service providers and require by contract that the service providers implement policies, procedures, and systems consistent with the Guidelines. If a financial institution's risk assessment calls for it, an institution must monitor its service providers to ensure their compliance with the Guidelines.

And finally, a financial institution must monitor, evaluate, and, as appropriate, adjust its information security program. Evaluations and adjustments should take into account changes in technology, the sensitivity of customer information, threats to that information, and the institution's own business arrangements, such as mergers and acquisitions.

Specific Data Security Obligations — Designing Information Security Programs

Both collectively and individually, the agencies have set forth further details to assist financial institutions in designing their information security programs. To understand the full range of data security obligations, financial

institutions must consult a number of sources, among them the Code of Federal Regulations, the Federal Financial Institutions Examination Council's ("FFIEC") *Information Security Booklet*, and specific enforcement actions taken by and interpretive guidance issued by the agencies. FFIEC, Information Technology Examination Handbook, Information Security Booklet (2002), available at *www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm*. The FFIEC is a formal interagency body that makes recommendations to promote uniformity in the supervision of financial institutions and prescribes uniform principles, standards, and report forms for examinations of financial institutions performed by the FDIC, FRB, OCC, OTS, and the National Credit Union Administration ("NCUA"). The FFIEC's *Information Security Booklet* is an especially useful source, as it sets forth requirements and suggestions for virtually all elements of information security programs and provides guidance to the agencies' field examiners in evaluating the adequacy of particular programs.

Since it is impossible to describe the entire spectrum of data security obligations in a few pages, this article highlights some important and widely applicable guidance derived from the various sources. Among these are interagency guidance on response programs, interagency and individual agency guidance on authentication, and interagency and individual agency guidance on information technology.

1) *Interagency Guidance on Response Programs*

Interpreting the GLBA and the Guidelines, the agencies have together published the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Guidance on Response Programs). 12 C.F.R. pt. 30, app. B; 12 C.F.R. pt. 208, app. D-2; 12 C.F.R. pt. 225, app. F; 12 C.F.R. pt. 364, app. B; 12 C.F.R. pt. 570, app. B. The Guidelines require that financial institutions consider implementing response programs as part of their information security programs in order to better manage and control risks, but the Guidance on Response Programs gives further details on exactly what response programs should include.

The Guidance on Response Programs sets forth five procedures that a financial institution's response program should contain, at a minimum. First, a response program should contain a procedure for assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused. Second, a response program should call for prompt notification of a financial institution's primary federal regulator. Third, a response program should contain steps for notifying appropriate law enforcement authorities. Fourth, a response program should contain a procedure for containing and controlling an incident to prevent further unauthorized access to or use of customer information while preserving evidence — for example, by monitoring, freezing, or closing affected accounts. Finally, a response program should contain steps for notifying customers of unauthorized access to their information.

The FFIEC's *Information Security Booklet* gives further guidance on detecting and responding to data security breaches. It describes three representative intrusion detection systems that financial institutions may adopt or use for comparison with their own systems. It also lists a number of elements for financial institutions to consider in devising programs to respond immediately to data security breaches, to contain and limit the damage of such breaches, and to restore customer information and customer information systems.

2) *Interagency and Individual Agency Guidance on Authentication*

In 2001, the FFIEC issued interagency guidance titled Authentication in an Electronic Banking Environment ("Authentication Guidance"). FFIEC, Authentication in an Electronic Banking Environment (Aug. 8, 2001), available at *www.ffiec.gov/ffiecinfobase/resources/info_sec/frb-sr-01-20-ffiec guidance_authentication.pdf*. The Authentication Guidance reviews risks and risk management controls for a number of authentication tools used to authenticate existing customers that access electronic banking services, complementing certain elements of the Guidelines. The Authentication Guidance also addressed steps to initially verify the identity of new customers, which have been largely superseded by implementing regulations of the USA PATRIOT Act's amendments to the BSA. *See, e.g.*, 31 C.F.R. pt. 103. It describes the various uses of three factors in authentication: 1) something the user knows, such as a password or PIN; 2) something the user possesses, such as an ATM card or smart card; and 3) something the user is, such as a biometric characteristic like a fingerprint or retinal pattern. The Authentication Guidance calls for financial institutions to conduct risk assessments and adopt an institutionwide approach to authentication commensurate to identified risks. It further calls for financial institutions to consider using multifactor or other similarly complex authentication systems to respond to new or changing risks. Finally, the Authentication Guidance describes four specific authentication methods financial institutions might adopt — 1) passwords and PINs; 2) digital certificates using public key infrastructure; 3) tokens and smart cards; and 4) biometrics — and their relative strengths and weaknesses.

Individual agencies have updated their recommendations in the midst of changing risks and technologies. For example, the FDIC recently published a study on unauthorized access to consumer information and how the financial industry and its regulators can mitigate associated risks. FDIC, Putting an End to Account-Hijacking Identity Theft, 22-37 (Dec. 14, 2004), available at *www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf*; *see also* FDIC, *Putting an End to Account-Hijacking Identity Theft Study Supplement*, at *www.fdic.gov/consumers/consumer/idtheftstudysupp/toc.html* (last updated June 27, 2005). The study reviewed the relative strengths and weaknesses of authentication methods in detail, including additional authentication methods that have developed over the past few years. Among other things, the FDIC concluded that two-factor authentication should be considered a "new security baseline" for electronic authentication in light of increased risks. Reaching a

similar conclusion, the OCC responded to the recent increase in e-mail fraud and fraud threats by suggesting that financial institutions adopt some of the stronger authentication methods described in the Authentication Guidance. OCC, Customer Identity Theft: E-Mail-Related Fraud Threats, Alert 2003-11 (Sept. 12, 2003), available at *www.occ.treas.gov/ftp/alert/2003-11.doc*.

3) *Interagency and Individual Agency Guidance on Information Technology*

The FFIEC's *Information Security Booklet* is the most comprehensive source for guidance on the information technology obligations of financial institutions. Though many of the specific details are beyond the scope of this article, the *Information Security Booklet* addresses such technology concerns as: protecting network hardware and software from unauthorized access and environmental hazards; using various types of encryption to further protect information stored in improperly accessed systems; protecting against malicious code through tools such as anti-virus software and firewalls; "hardening" software applications by installing additional security controls and patches; and collecting data from secure log files to monitor network use and identify security breaches. Faced with rapid changes in technology, however, the FFIEC sets forth general guidance and examples in its *Information Security Booklet* rather than prescribing specific technological requirements.

Though the FFIEC has issued most of the agencies' guidance on information technology, by way of its *Information Security Booklet*, the individual agencies have also weighed in on information technology standards. The OTS, for example, has included a section addressing management and technology risk controls in its *Thrift Activities Handbook*. OTS, Regulatory Handbook: Thrift Activities §341 (2002), available at *www.ots.treas.gov/pagehtml.cfm?catNumber=105&an=9*. While the technology risk controls section of the *Thrift Activities Handbook* addresses many of the same issues and contains many of the same recommendations as the *Information Security Booklet*, it tailors its recommendations to thrift associations and may be more directly useful than the *Information Security Booklet* to those financial institutions under the jurisdiction of the OTS. The FDIC's Guidance on Managing Risks Associated with Wireless Networks and Wireless Customer Access ("Wireless Guidance"), on the other hand, addresses a specific technology largely ignored by the *Information Security Booklet*. FDIC, Guidance on Managing Risks Associated with Wireless Networks and Wireless Customer Access, FIL-8-2002 (Feb. 1, 2002), available at *www.ffiec.gov/ffiecinfobase/resources/info_sec/fdi-fil-8-2002-wireless_networks_and_cus tomer_access.pdf*. The Wireless Guidance addresses data security risks unique to wireless networks and wireless Internet devices, as well as recommendations for testing, evaluating, and managing those risks.

Additional Data Security Obligations

Some financial institutions are subject to additional federal data security obligations under statutes and regulations directed at activities within the larger business community. For example, the Health Information Portability and Accountability Act ("HIPAA)" and its implementing regulations require additional safeguards for customer health information. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections throughout U.S.C.). Some financial institutions qualify as "business associates" of covered entities or "health care clearinghouses" under HIPAA. Such institutions must take HIPAA's requirements into account in designing and implementing their information security programs. Other statutes that affect data security obligations for some financial institutions include the Children's Online Privacy Protection Act (15 U.S.C. §§6501-06) and the USA PATRIOT Act. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections throughout U.S.C.).

Conclusion

Financial institutions must look to a variety of federal sources to determine their federal data security obligations. At the same time, financial institutions must regularly monitor and update their data security policies, procedures, and systems in order to respond to rapidly changing risks and technologies. Adequate and effective data security thus requires expertise in law, business, general security, and information technology.

—❖—