Order Code RL34120

CRS Report for Congress

Information Security and Data Breach Notification Safeguards

July 31, 2007

Gina Marie Stevens
Legislative Attorney
American Law Division

Prepared for Members and Committees of Congress

Congressional Research Service

Information Security and Data Breach Notification Safeguards

Summary

Information security and breach notification requirements are imposed on some entities that own, possess, or license sensitive personal information. Information security standards are designed to protect personally identifiable information from compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or other situations where unauthorized persons have access or potential access to personally identifiable information for unauthorized purposes. Data breach notification laws require covered entities to provide notice to affected persons (e.g., cardholders, customers) about the occurrence of a data security breach involving personally identifiable information. Data security breaches occur when fraudulent accounts are created, laptops or computers are stolen or hacked, passwords are compromised, insiders or employees steal data, or discs or back-up tapes are misplaced.

Information security laws require covered entities to establish information security programs to ensure the security and confidentiality of information; establish administrative, technical, and physical safeguards; protect against any anticipated threats or hazards to information security which could result in substantial harm, embarrassment, inconvenience, or unfairness; protect against unauthorized access to or use of such records or information; conduct periodic assessments of the risk and magnitude of harm that could result from a security breach; limit the amount of information collected, maintained, or processed to the minimum amount necessary; maintain accurate, relevant, timely, and complete information; establish rules of conduct and training for persons authorized to access records or information; develop procedures for detecting, reporting, and responding to security incidents; notify appropriate authorities, officials, and congressional committees of security incidents; require contractors, business associates, or service providers to contractually agree to provide information security; perform annual audits of the security program; and comply with other security requirements.

Many data breach notification laws require covered entities to implement a breach notification policy, and include requirements for incident reporting and handling and external breach notification. Breach notification policies address whether breach notification is required, the time when notice should be given, who should provide notice, the level or risk that will trigger external notification, the contents of the notification, the means of providing the notification, and who should receive notification. In addition, such laws generally require a covered entity or a designated party to conduct a risk assessment of the likely risk of harm caused by the data breach and an assessment of the level of risk for potential misuse of information. Breach notification policies may also address when notification may be delayed and exemptions from external notification for information that is encrypted.

The following report analyzes the Privacy Act, the Federal Information Security Management Act, Office of Management and Budget Guidance, the Veterans Affairs Information Security Act, the Health Insurance Portability and Accountability Act, and the Gramm-Leach-Bliley Act. This report will be updated.

Contents

Background 1

Safeguards for Personal Information 5

The Federal Sector 7
- Privacy Act 7
- Federal Information Security Management Act 8
  - Office of Management and Budget "Breach Notification Policy 9
- Veterans Affairs Information Security Act 12

The Private Sector 16
- Health Insurance Portability and Accountability Act 16
  - HIPAA Privacy Standard 17
  - HIPAA Security Standards 17
- Gramm-Leach-Bliley Act 19
  - GLBA Privacy Rule 19
  - FTC Safeguards Rule 20
  - Information Security Standards 20

Conclusion 22

GalleryWatch.com http://www.crsdocuments.com Penny Hill Press

Information Security and Data Breach Notification Safeguards

Background

Information security and breach notification requirements are imposed on some entities that own, possess, or license sensitive personal information. Information security standards are designed to protect personally identifiable information from compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or other situations where unauthorized persons have access or potential access to personally identifiable information for unauthorized purposes. Data breach notification requirements obligate covered entities to provide notice to affected persons (e.g., cardholders, customers) about the occurrence of a data security breach involving personally identifiable information.

The first data breach notification law was enacted in 2002 — S.B. 1386, the California Security Breach Notification Act.[1] It requires any state agency, person, or business that owns or licenses computerized personal information to disclose any breach of a resident's personal information. S.B. 1386 was the model for subsequent data breach notification laws enacted by many states and Congress. California's law and other similar federal and state laws require the disclosure of security breaches of personal information. Major data security breaches have been disclosed by the nation's largest information brokerage firms, retailers, companies, universities, and government agencies.[2] From February 2005 to December 2006, 100 million personal records were reportedly lost or exposed.[3] Massive data security breaches in 2005, 2006, and 2007 have heightened interest in the security of personal information;[4] in

---

[1] S. B. 1386 requires a state agency or any person or business that owns or licenses computerized data that includes personal information to disclose any security breach of data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Cal. Civ. Code § 1798.82.

[2] See generally CRS Report RL33199, *Personal Data Security Breaches: Context and Incident Summaries*, by Rita Tehan.

[3] Tom Zeller, "An Ominous Milestone: 100 Million Data Leaks," *New York Times*, December 18, 2006, p. C3.

[4] See Kenneth M. Siegel, *Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age*, 111 Penn St. L. Rev. 779 (2007); Kamaal Zaidi, *Identity Theft and Consumer Protection: Finding Sensible Approaches to Safeguard Personal Data in the United States and Canada*, 19 Loy. Consumer L. Rev. 99 (2007).

the business and regulation of data brokers;[5] in the liability of retailers, credit card issuers, payment processors, banks, and furnishers of credit reports for third party companies' costs arising from data breaches;[6] and in remedies available to individuals whose personal information was accessed without authorization.[7]

Data security breaches often occur when fraudulent accounts are created, laptops or computers are stolen or hacked, passwords are compromised, insiders or employees steal data, or discs or back-up tapes are misplaced. Data security breaches illustrate the risks associated with collecting and disseminating large amounts of electronic personal information. The potential risk of harm to individuals from data breaches include identity theft and financial crimes (e.g., credit card fraud, check fraud, mortgage fraud, identification document fraud, and health-care fraud). According to a June 2007 GAO report, there is no clear correlation between data security breaches and identity theft.

> The extent to which data breaches have resulted in identity theft is not well known, largely because of the difficulty of determining the source of the data used to commit identity theft. However, available data and interviews with researchers, law enforcement officials, and industry representatives indicated that most breaches have not resulted in detected incidents of identity theft, particularly the unauthorized creation of new accounts.[8]

Are data brokers and other companies that collect or maintain sensitive personal information taking adequate steps to protect the information they possess? What steps should they take when data is acquired by unauthorized individuals? The relationship of state laws to federal law and whether new federal laws should preempt or supercede similar state laws is an important question. These questions figure prominently in solutions posed to prevent and remedy data breaches.

---

[5] This report uses the term data brokers to describe companies that collect and distribute personal information, however other terms such as information broker or information reseller or information solutions provider are also commonly used. See CRS Report RS22137, *Data Brokers: Background and Industry Overview*, by Gina Marie Stevens.

[6] Six states have reportedly introduced bills designed to strengthen merchant security and/or hold companies liable for third party companies' costs arising from data breaches (California, Connecticut, Illinois, Massachusetts, Minnesota, and Texas). See Timothy P. Tobin, *In Response To TJX Data Breach, One State Enacts Legislation Imposing New Security and Liability Obligations; Similar Bills Pending in Five Other States*, at [http://privacylaw.proskauer.com/]. The Minnesota bill was signed into law on May 21, 2007. 2007 Minn. Laws Ch. 108, H.F. 1758.

[7] The criminal liability of persons responsible for unauthorized access to computer systems is discussed in CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws,* by Charles Doyle.

[8] U.S. Government Accountability Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, (June 2007) at [http://www.gao.gov/new.items/d07737.pdf].

Information security[9] and breach notification[10] requirements are imposed on some entities that own, possess, or license sensitive personal information. Congress, the Executive Branch, the states, and the courts continue to confront the problem of data breaches. The 109th Congress reported six data security bills, and the 110th Congress will revisit data security legislation.[11] The Federal Trade Commission (FTC) has enforced consumer protection laws to enjoin and remedy lax information security practices.[12] The President's Identity Theft Task Force reported its final recommendations April 2007, including the establishment of national standards for entities to safeguard personal data and for notification to consumers of breaches that pose a significant risk of identity theft.[13] The payment card industry has also issued security standards and reporting requirements for organizations that handle bank cards.[14] The courts are also considering a number of lawsuits filed by consumers and banks based on the Federal Privacy Act and state common law breach of contract and

---

[9] Information security standards are designed to protect personally identifiable information from compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or other situations where unauthorized persons have access or potential access to personally identifiable information for unauthorized purposes.

[10] Breach notification laws require covered entities to provide notice to affected persons (e.g., cardholders, customers) about the occurrence of a data security breach. For further information, see Sean C. Honeywill, *Data Security and Data Breach Notification for Financial Institutions*, 10 N.C. Banking Inst. 269 (2006); Lilia Rode, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security?*, 43 Hous. L. Rev. 1597 (2007); Paul M. Schwartz and Edward J. Janger, *Notification of Database Security Breaches*, 105 Mich. L. Rev. 913 (2007);Thomas J. Smedinghoff, *Security Breach Notification — Adapting to the Regulatory Framework*, 21 The Review of Banking & Financial Services 115-124 (Dec. 2005).

[11] S. 1326 (Sessions) Notification of Risk to Personal Data Act, S. 1408 (Smith) Identity Theft Protection Act, S. 1789 (Specter) Personal Data Privacy and Security Act of 2005, H.R. 4127 (Stearns) Data Accountability and Trust Act , H.R. 3997 (LaTourette) Financial Data Protection Act of 2005, and H.R. 5318 (Sensenbrenner) Cyber-Security Enhancement and Consumer Data Protection Act of 2006. See See CRS Report RL33273, *Data Security: Federal Legislative Approaches* by, Gina Marie Stevens.

[12] FTC enforcement of consumer protection laws to remedy lax information security practices by private sector entities will be addressed in a separate report.

[13] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, April 2007 at [http://www.identitytheft.gov/reports/StrategicPlan.pdf].

[14] The Payment Card Industry (PCI) Data Security Standard (DSS) is an industry regulation developed by VISA, MasterCard, and other bank card distributors. It requires organizations that handle bank cards to conform to security standards and follow certain leveled requirements for testing and reporting. The core of the PCI DSS is a group of principles and accompanying requirements designed to build and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, monitor and test networks, and maintain an information security policy. Available at [https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf].

negligence claims.[15] State Attorneys General have also investigated data security breaches.[16]

Many states have enacted laws requiring notice of security breaches of personal data and consumer redress. As of January 2007, 35 states enacted data security laws requiring entities to notify persons affected by security breaches and, in some cases, to implement information security programs to protect the security, confidentiality, and integrity of data.[17] Congress and some states have enacted credit freeze and fraud alert laws.[18]

A newly enacted federal law and recently issued federal guidance require federal agencies that collect sensitive personal information to implement enhanced information security programs and provide notice to persons affected by data security breaches. The Veterans Affairs Information Security Act of 2006 and the 2007 Office of Management and Budget memorandum on "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" were enacted to prevent and respond to federal agency data breaches. Other federal laws, such as the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act, require private sector covered entities to maintain administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of personal information.

---

[15] See, "Contract Claim Against Card Processor Dismissed in BJ's Club Data Breach Case," *BNA Privacy Law Watch* (June 28, 2006); "Bank Files Lawsuit Over TJX Breach; Rep. Markey Calls for FTC Investigation," *BNA Privacy Law Watch* (Feb. 2, 2007); "TJX Faces More Customer Breach Lawsuits; FACT Act Credit Receipt Class Actions Filed," *BNA Privacy Law Watch* (June 12, 2007). In 2007 TJX Companies revealed that at least 46.2 million credit and debit cards may have been compromised in the breach of its computer network by unauthorized individuals. U.S. Securities and Exchange Commission, *Form 10-K Annual Report: The TJX Companies, Inc.,* available at [http://www.sec.gov/Archives/edgar/data/109198/000095013507001906/b64407tje10vk.htm].

[16] According to TJX's annual report, 37 states are involved in investigations by their attorneys general. *Id.*

[17] Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Vermont, Washington, and Wisconsin. *State Security Breach Notification Laws*, National Conference of State Legislatures at [http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm]. See also "New Data Security Laws Take Effect in Several States," 75 *U.S. Law Week* 2388 (Jan. 9, 2007); John P. Hutchins, *U.S. Data Breach Notification Law: State by State* (2007).

[18] "Security freeze" laws (also referred to as "credit freeze" laws) are a form of identity theft victim assistance. A security freeze law allows a consumer to block unauthorized third parties from obtaining his or her credit report or score. See CRS Report RL34028, *Identity Theft Laws: State Penalties and Remedies and Pending Federal Bills*, by Tara Alexandra Rainson. The Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. §§ 1681-1681x, amended the Fair Credit Reporting Act (FCRA), and added provisions designed to prevent and mitigate identity theft, including a section that enables consumers to place fraud alerts in their credit files.

Because of questions about the applicability of existing federal laws to all sensitive personal information and the adequacy of enforcement tools available to federal regulators,[19] this report provides an overview of federal information security and privacy laws.[20]

Safeguards for Personal Information

No single federal law or regulation governs the security of all types of personal information. Determining which federal laws, regulations, and guidance are applicable depends on three factors: the entity or sector that collected the information, the type of information collected, and the purpose for which the information was collected. Under federal law certain sectors are legally obligated to protect sensitive personal information. These obligations were created, in large part, when federal privacy legislation was enacted in the credit, financial services, health care, government, securities, and Internet sectors. Federal regulations were issued to require certain entities to implement information security programs and provide

---

[19] A recent study by the Government Accountability Office examined the effectiveness of key federal privacy laws in safeguarding sensitive data, and concluded that

> [The] Safeguarding provisions of FCRA [the Fair Credit Reporting Act] and GLBA [the Gramm-Leach-Bliley Act] do not apply to all sensitive personal information held by information resellers. To ensure that such data are protected on a more consistent basis, Congress should consider requiring information resellers to safeguard all sensitive personal information they hold. As Congress considers how best to protect data maintained by information resellers, it should also consider whether to expand more broadly the class of entities explicitly required to safeguard sensitive personal information.
>
> To ensure that the Federal Trade Commission has the tools it needs to most effectively act against data privacy and security violations, Congress should consider providing the agency with civil penalty authority for its enforcement of the Gramm-Leach-Bliley Act's privacy and safeguarding provisions.

U.S. Government Accountability Office, *Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data* 56, GAO-06-674, June 26, 2006 at [http://www.gao.gov/new.items/d06674.pdf]

[20] A discussion of Section 222 of the Communications Act of 1934, as amended (47 U.S.C. 222), which establishes a duty for telecommunications carrier to protect the confidentiality of customers' customer proprietary network information (CPNI), is included in CRS Report RL33287, *Data Security: Protecting the Privacy of Phone Records*, by Gina Marie Stevens. A discussion of Sections 302 and 404 of the Sarbanes-Oxley Act of 2002, P.L. 107-204, which require public companies to ensure that they have implemented appropriate information security controls with respect to their financial information, is included in CRS Report RS22482, *Section 404 of the Sarbanes-Oxley Act of 2002 (Management Assessment of Internal Controls): Current Regulation and Congressional Concerns*, by Michael V. Seitzinger.

breach notice to affected persons.[21] Some critics say that current laws focus too closely on industry-specific uses of information, like credit reports or medical data, rather than on protecting the privacy of individuals.[22] Others believe the sectoral approach to the protection of personal information reflects not only variations in the types of information collected (e.g., government, private sector, health, financial, etc.), but also differences in the regulatory framework for particular sectors. Other critics advocate a national standard for all entities that maintain personal information in order to harmonize legal obligations throughout the nation.

Variations in the laws are common, however similarities are more prevalent. One area where a great deal of variation exists is the applicability of the law — who is covered. The applicability of a particular law depends in part on the information owner. Information security safeguards may either apply to all federal government agencies, a particular federal agency, private sector entities, health care plans, clearinghouses and providers, or financial institutions. This is what is commonly referred to as a sectoral approach to the protection of personal information.

The type of information collected determines in part whether a particular law is applicable. Information on individuals collected, maintained, or processed by a covered entity or on behalf of a covered entity (by a contractor or subcontractor) is regulated. In some cases a law's scope extends to information a covered entity creates, receives, maintains, or transmits. Another approach taken is where the law targets a specific category of information (e.g., agency, federal, medical, financial, sensitive, customer). The medium or format the information is kept in is also frequently relevant (electronic, paper, or other form). Only health information that is electronically transmitted is protected.

The laws typically cover "personally identifiable information" or "sensitive personal information" or "individually identifiable information." Generally included are an individual's name or another personal identifier, social security number, biometric records, date and place of birth, and mother's maiden name. Other information included in some laws is that which identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual, or information that can be used to distinguish or trace the individual's identity. In some cases, information about an individual's education, financial transactions, medical history, and criminal and employment history may be covered. The law governing financial institutions regulates nonpublic personal information. "Sensitive personal information" as defined by the federal banking regulators means

> a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that

---

[21] Thomas J. Smedinghoff, *The New Law of Information Security: What Companies Need To Do Now*, 22 The Computer & Internet Lawyer 9 (Nov. 2005).

[22] Tom Zeller Jr, *Breach Points Up Flaws in Privacy Laws*, N.Y. Times (Feb. 24, 2005).

would allow someone to log onto or access the customer's account, such as user name and password or password and account number.

The Federal Sector

Privacy Act

The Privacy Act of 1974[23] governs the collection, use, and dissemination of a "record"[24] about an "individual"[25] maintained by federal agencies in a "system of records."[26] The Privacy Act does not apply to private sector databases. The Privacy Act regulates federal government agency recordkeeping and disclosure practices, and prohibits the disclosure of any record maintained in a system of records to any person or agency without the written consent of the record subject, unless the disclosure falls within one of twelve statutory exceptions. The act allows most individuals to seek access to records about themselves, and requires that personal information in agency files be accurate, complete, relevant, and timely.[27] The subject of a record may challenge the accuracy of information. The Privacy Act requires that when agencies establish or modify a system of records, they publish a "system-of-records notice" in the Federal Register.[28]

Each agency is required to establish "rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of [the Privacy Act]...."[29] Each agency that maintains a system of records is also required to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could

---

[23] 5 U.S.C. § 552a.

[24] The act defines a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. 5 U.S.C. § 552a(a)(4).

[25] "The term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence." 5 U.S.C. § 552a(2).

[26] The act defines "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. *Id* at § 552a(a)(5).

[27] 5 U.S.C. § 552a(e)(5).

[28] The Federal Register notice must identify, among other things, the type of data collected, the types of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and correct personal information. The term "routine use" means (with respect to the disclosure of a record) the use of such a record for a purpose that is compatible with the purpose for which it was collected. 5 U.S.C. § 552a(a)(7).

[29] 5 U.S.C. § 552a(e)(9).

result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[30]

The Privacy Act also applies to systems of records created by government contractors. Subsection (m) of the Privacy Act states

> When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system....[31]

The Privacy Act provides legal remedies that permit an individual to seek enforcement of the rights granted under the act. The individual may bring a civil suit against the agency. The court may order the agency to amend the individual's record, enjoin the agency from withholding the individual's records, and may award actual damages of $1,000 or more to the individual for intentional or wilful violations.[32] Courts may also assess attorneys fees and costs. The act also contains criminal penalties; federal employees who fail to comply with the act's provisions may be subjected to criminal penalties.

The Office of Management and Budget (OMB) is required to prescribe guidelines and regulations for the use by agencies in implementing the act, and provide assistance to and oversight of the implementation of the act.[33]

Federal Information Security Management Act

Title III of the E-Government Act of 2002, the Federal Information Security Management Act of 2002 (FISMA),[34] requires federal government agencies to provide information security protections for agency information and information systems.[35] Agencies are required to develop, document, and implement an agency

---

[30] 5 U.S.C. § 552a(e)(10).

[31] 5 U.S.C. § 552(m).

[32] Shortly after the breach of the personal data of 26.5 million veterans in 2006 by the Department of Veterans Affairs, veterans groups filed a class-action lawsuit claiming that the U.S. Department of Veterans Affairs "flagrantly disregarded the privacy rights of essentially every man or woman to have worn a United States military uniform." The plaintiffs alleged violations of the Administrative Procedure Act and the Privacy Act. The lawsuit seeks declaratory and injunctive relief and damages of $1,000 for every person listed in the missing database files. *Vietnam Veterans of America, Inc. et al. V. Nicholson*, No. 1:06-cv-01038-JR (D. D.C. filed June 6, 2006).

[33] 5 U.S.C. § 552a(v). 40 Fed. Reg. 28976 (July 9, 1975).

[34] Title III of the E-Government Act of 2002, P.L. 107-347; 44 U.S.C. § 3541 *et seq.*; see CRS Report RL32357, *Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives*, by John Moteff.

[35] Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to

(continued...)

wide information security program "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency."[36] The agency's information security plan also must include procedures for detecting, reporting, and responding to security incidents, including mitigating risks associated with such incidents before substantial damage is done; notifying and consulting with the Federal information security incident center and with law enforcement agencies and relevant Offices of Inspector General.[37] FISMA requires agencies to comply with the information security standards developed by NIST.[38] FISMA also requires agencies to conduct, annually, an independent evaluation of their security programs which includes an assessment of the effectiveness of the program, plans, and practices and compliance with FISMA requirements. The evaluations are forwarded to the Director of the Office of Management and Budget, for an annual report to Congress.[39]

Office of Management and Budget "Breach Notification Policy." In response to recommendations from the President's Identity Theft Task Force,[40] the Office of Management and Budget issued guidance May 2007 for federal agencies on "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."[41] The OMB memorandum requires all federal agencies to implement a breach notification policy to safeguard "personally identifiable information" within 120 days of the date of the memorandum (by August 22, 2007) to apply to both electronic systems and paper documents.[42] To formulate their policy, agencies are

---

[35] (...continued)
provide integrity, confidentiality, and availability. 44 U.S.C. § 3542.

[36] 44 U.S.C. § 3544(a)(1)(A).

[37] 44 U.S.C. § 3544(b)(7).

[38] 44 U.S.C. § 3544(a)(1)(B). The National Institute of Standards and Technology (NIST) is responsible for developing standards and guidelines for providing adequate information security for all agency operations and assets, except for national security systems. 40 U.S.C. § 11331.

[39] See generally *Information Security: Agencies Report Progress, but Sensitive Data Remain at Risk: Hearings Before the Subcomms. of the House Comm. on Oversight and Government Reform*, 110th Cong. 6-8 (2007) (statement of Gregory C. Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office) available at [http://www.gao.gov/new.items/d07935t.pdf].

[40] The President's Identity Theft Task Force is composed of 18 federal agencies and departments, and was tasked with developing a strategic plan for the federal government to combat identity theft. Exec. Order No. 13,402, 71 FR 27945 (2006).

[41] Office of Management and Budget, Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007) available at [http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf].

[42] The memo defines the term "personally identifiable information"as "information which
(continued...)

directed to review existing privacy and security requirements, and include requirements for incident reporting and handling and external breach notification. In addition, agencies are required to develop policies concerning the responsibilities of individuals authorized to access personally identifiable information. Agencies are permitted to develop more stringent policies.

According to the OMB memo, an agency's failure to implement one or more of FISMA provisions or associated standards, policies, or guidance issued by OMB or the National Institute of Standards and Technology (NIST) would not constitute less than adequate protections required by the Privacy Act. Moreover, the new OMB requirements do not create any enforceable rights or benefits at law against the government.[43]

Attachment 1 of the OMB memorandum, Safeguarding Against the Breach of Personally Identifiable Information, reemphasizes agencies' responsibilities under existing law (e.g., the Privacy Act and FISMA), executive orders, regulations, and policy to safeguard personally identifiable information and train employees.[44] Two new privacy requirements and five new security requirements are established in attachment 1 of the OMB memorandum. To implement the new privacy requirements, agencies are required to review current holdings of all personally identifiable information to ensure that they are accurate, relevant, timely, and complete, and reduced to the minimum necessary amount. Within 120 days, agencies must establish a plan to eliminate the unnecessary collection and use of social security numbers within eighteen months. Agencies must implement the following five new security requirements (applicable to all federal information): encrypt all data on mobile computers/devices carrying agency data; employ two-factor authentication for remote access; use a "time-out" function for remote access and mobile devices; log and verify all computer-readable data extracts from databases holding sensitive information; and ensure that individuals and supervisors with authorized access to personally identifiable information annually sign a document describing their responsibilities.[45]

---

[42] (...continued)
can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

[43] OMB Memorandum M-07-16 at 4 n. 12.

[44] National Institute of Standards and Technology, Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*; FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, at [http://csrc.nist.gov/publications/fips/index.html]and NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*; and NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* at [http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf].

[45] The first four information security requirements were adopted in an earlier memorandum, See OMB Memo 06-16 "*Protection of Sensitive Agency Information*" at (continued...)

Attachment 2 of the OMB Memo, Incident Reporting and Handling Requirements, applies to the breach of personally identifiable information in electronic or paper format. Existing FISMA information security requirements are reviewed (implementation of procedures for detecting, reporting, and responding to security incidents, notifying and consulting with appropriate officials and authorities, and implementing NIST guidance and standards). Agencies are required to report all incidents involving personally identifiable information within one hour of discovery/detection; and publish a "routine use"[46] under the Privacy Act for appropriate systems of records applying to the disclosure of information to appropriate agencies, entities, and persons in connection with response and remedial efforts in the event of a data breach.[47]

Attachment 3, External Breach Notification, identifies the factors agencies should consider in determining when notification outside the agency should be given and the nature of the notification. Notification may not be necessary for encrypted information. Agency breach notification plans are required to address whether breach notification is required; the timeliness of the notification; the source of the notification; the contents of the notification; the means of providing the notification; and who receives notification. In addition, each agency is directed to establish an agency response team. Agencies must assess the likely risk of harm caused by the breach and the level of risk. Agencies are directed to consider the nature of the data elements breached, the number of individuals affected, the likelihood the personally identifiable information is accessible and usable, the likelihood the breach may lead to harm, and the ability of the agency to mitigate the risk of harm. Agencies should provide notification without unreasonable delay following the detection of a breach, but are permitted to delay notification for law enforcement, national security purposes, or agency needs. When the breach involves a federal contractor or an entity operating a systems of records for the agency, the agency must issue the notification and undertake corrective actions. Attachment 3 also includes specifics as to the content of the notice, criteria for determining the method of notification, and the types of notice that may be used.

Attachment 4, Rules and Consequences Policy, directs each agency to develop and implement a policy outlining the rules of behavior and identifying consequences and corrective actions available for failure to follow these rules. The particular facts and circumstances, including whether the breach was intentional, are to be considered in taking appropriate disciplinary action. Any action taken by supervisors must be consistent with law, regulation, applicable case law, and any relevant collective bargaining agreement. Supervisors may be subject to disciplinary action for failure to take appropriate action upon discovering the breach or failure to take required steps to prevent a breach from occurring. Each agency should have a documented

---

[45] (...continued)
[http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf].

[46] The Privacy Act defines a routine use to mean "with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected." 5 U.S.C. § 552a(a)(7).

[47] OMB Memorandum M-07-16 at p.11.

policy in place which applies to employees of the agency (including managers), and its contractors, licensees, certificate holders, and grantees, and that describes the terms and conditions affected individuals shall be subject to and identifies available corrective actions. Rules of behavior and corrective actions should address the failure to implement and maintain security controls for personally identifiable information; exceeding authorized access to, or disclosure to unauthorized persons of, personally identifiable information; failure to report any known or suspected loss of control or unauthorized disclosure of personally identifiable information; and for managers, failure to adequately instruct, train, or supervise employees in their responsibilities. Consequences may include reprimand, suspension, removal, or other actions in accordance with applicable law and agency policy.

Veterans Affairs Information Security Act

Title IX of P.L. 109-461,[48] the Veterans Affairs Information Security Act, requires the Veterans Administration (VA) to implement agency-wide information security procedures to protect the VA's "sensitive personal information" (SPI)[49] and VA information systems. P.L. 109-461 was enacted to respond to the May 2006 breach of the personal data of 26.5 million veterans caused by the theft of a VA employee's hard drive from his home.[50]

Pursuant to P.L. 109-461, the VA's information security program is to provide for the development and maintenance of cost effective security controls to protect VA information, in any medium or format, and VA information systems.[51] The information security program is required to include the following elements: periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of VA information and information systems; policies and procedures based on risk assessments that cost-effectively reduce security risks and ensure information security; implementation of security controls to protect the confidentiality, integrity, and availability of VA information and information systems; plans for security for

---

[48] The Veterans Benefits, Health Care, and Information Technology Act of 2006, P.L. 109-461 (Dec. 22, 2006); 38 U.S.C. §§ 5722 *et seq.*

[49] "The term "sensitive personal information", with respect to an individual, means any information about the individual maintained by an agency, including the following: (A) Education, financial transactions, medical history, and criminal or employment history. (B) Information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records." P.L. 109-461, § 902.

[50] See CRS Report RL33612, *Department of Veterans Affairs: Information Security and Information Technology Management Reorganization*, by Sidath Viranga Panangala. For lessons learned from the VA data breach and other similar federal data breaches, see U.S. Government Accountability Office, *Privacy: Lessons Learned about Data Breach Notification* GAO-07-657, April 30, 2007 at [http://www.gao.gov/new.items/d07657.pdf]; GAO, *Information Security: Leadership Needed to Address Weaknesses and Privacy Issues at Veterans Affairs,* GAO-06-897T, June 20, 2006 at [http://www.gao.gov/new.items/d06897t.pdf].

[51] 38 U.S.C. § 5722.

networks, facilities, systems, or groups of information systems; annual security awareness training for employees and contractors and users of VA information and information systems; periodic testing of security controls; a process for remedial actions; procedures of detecting, reporting, and responding to security incidents; and plans and procedures to ensure continuity of operations. Additionally, the VA Secretary is directed to comply with FISMA, and other security requirements issued by NIST and OMB. The law also establishes specific information security responsibilities for the VA Secretary, information technology and information security officials, VA information owners, other key officials, users of VA information systems, and the VA Inspector General.

P.L. 109-461 requires that in the event of a "data breach"[52] of sensitive personal information processed or maintained by the VA Secretary, the Secretary must ensure that as soon as possible after discovery that either a non-VA entity or the VA's Inspector General conduct an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information.[53] Based upon the risk analysis, if the Secretary determines that a reasonable risk exists of the potential misuse of sensitive personal information, the Secretary must provide credit protection services in accordance with regulations issued by the VA Secretary.[54]

The VA Secretary is required to report to the Veterans Committees the findings of the independent risk analysis for each data breach, the Secretary's determination regarding the risk for potential misuse of sensitive personal data, and the provision of credit protection services.[55] If the breach involved the sensitive data of DOD civilian or enlisted personnel the Secretary must also report to the Armed Services Committees.[56] In addition, quarterly reports are to be submitted by the VA Secretary to the Veterans Committees of Congress on any data breach of sensitive personal information processed or maintained by the VA during that quarter.[57] With respect to the breach of SPI that the VA Secretary determines to be significant, notice must be provided promptly following the discovery of such data breach to the Veterans Committees, and if the breach involved the SPI of DOD civilian or enlisted personnel also to the Armed Service Committees.[58]

P.L. 109-461 also requires the VA to include data security requirements in all contracts with private-sector service providers that require access to sensitive

---

[52] "Data breach means the loss or theft of, or other unauthorized access to, other than an unauthorized access incidental to the scope of employment, data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data." 38 U.S.C. § 5727(4).

[53] 38 U.S. C. § 5724(a)(1).

[54] 38 U.S. C. § 5724(a)(2).

[55] 38 U.S.C. § 5724(c)(1).

[56] 38 U.S.C. § 5724(c)(2).

[57] 38 U.S.C. § 5726.

[58] 38 U.S.C. § 5724(b).

personal information.[59] All contracts involving access to sensitive personal information must include a prohibition of the disclosure of such information unless the disclosure is lawful and expressly authorized under the contract; and the condition that the contractor or subcontractor notify the Secretary of any data breach of such information. In addition, each contract must provide for liquidated damages to be paid by the contractor to the Secretary in the event of a data breach with respect to any sensitive personal information, and that money shall be made available exclusively for the purpose of providing credit protection services.

P.L. 109-461 requires the Secretary of the VA within 180 days of enactment (by June 22, 2007) to issue interim regulations concerning notification, data mining, fraud alerts, data breach analysis, credit monitoring, identity theft insurance, and credit protection services.[60] Interim final regulations were issued by the VA Deputy Secretary on June 22, 2007 to address data breach security regarding sensitive personal information processed or maintained by the VA.[61] The VA interprets its regulations as consistent with OMB Memorandum M-07-16, "Safeguarding and Responding to Breaches of Personally Identifiable Information." The regulations do not supercede the requirements imposed by other laws such as the Privacy Act, the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act, and their implementing rules.

Section 75.114 of the regulations, Accelerated Response, permits the VA Secretary to provide prompt notice to record subjects of a data breach and/or offer credit protection services prior to the completion of a risk analysis if the VA Secretary determines that there is an immediate, substantial risk of identity theft and that providing notice may enable the record subjects to protect themselves and that credit protection services will assist in mitigation of possible harm; or that private entities would be required to provide notice under federal law if they experienced a breach involving the same or similar information. The Secretary is required to decide whether to issue prompt notice based upon the totality of the circumstances and information available to the Secretary at the time of the decision. The Secretary's exercise of this discretion is to be based on good cause and include several factors enumerated in the regulations.

Section 75.115 of the regulations, Risk Analysis, requires the VA Secretary to make sure that, as soon as possible after the data breach, a non-VA entity with relevant expertise in data breach assessment and risk analysis or the VA's Office of Inspector General conducts an independent risk analysis of the data breach. The preparation of the risk analysis may include data mining if necessary for the

---

[59] 38 U.S.C. § 5725.

[60] 38 U.S. C. § 5724(b).

[61] 72 Fed. Reg. 34395 (2007), 38 C.F.R. § 75, Subpart B. The interim final regulations implement the sections of P.L. 109-461 on data breaches, credit protections services, and reporting requirements. The 60 day public comment period on the interim regulations closes on August 22, 2007. A separate rulemaking will be commenced to issue regulations to implement sections of P.L. 109-461 requiring a VA information security program and establishing information security responsibilities for the VA Secretary, agency officials, and users of VA information systems. *Id.*

development of relevant information.[62] The risk analysis must include a finding with supporting rationale concerning whether the circumstances create a reasonable risk that sensitive personal information potentially may be misused. If the risk analysis concludes that the data breach presents a reasonable risk for the potential misuse of sensitive personal information, the risk analysis must also contain operational recommendations for responding to the data breach. To provide information that the Secretary will use in making determinations required under the regulations, this section requires that the risk analysis address identified factors relating to risks and potential harms.

Section 75.116 of the regulations, Secretary Determination, provides that the Secretary consider the risk analysis to determine, based on criteria in the regulation, whether a reasonable risk exists for the potential misuse of sensitive personal information involved in a data breach. If the Secretary finds that a reasonable risk exists for the potential misuse of sensitive personal information, the Secretary should take responsive action as specified based on the potential harms to individuals subject to a data breach. In making her or his decision, the Secretary is to consider all factors that she or he considers relevant, including identified factors related to the risk of harm.

Section 75.117 of the regulations, Notification, requires the Secretary to promptly provide written notification by first-class mail to individuals found to be subject to a reasonable risk for the potential misuse of any sensitive personal information. The notification should include a description of what happened, a description of the types of information involved; a description of what the agency is doing to investigate the breach, to mitigate losses, and to protect against further breaches; contact information for the agency; steps individuals can take to protect themselves from the risk of identity theft, including fraud alerts; and a statement whether the information was encrypted or otherwise protected. Provision is made for substitute notice where there is unreliable contact information. The Secretary is also permitted to provide notification over the telephone in urgent cases. Notification may be delayed pursuant to lawful written requests from other federal agencies to protect data or computer resources, or prevent interference with an investigation or data recovery.

Section 75.118, Other Credit Protection Services, permits the Secretary to offer individuals subject to a reasonable risk for potential misuse of SPI, one or more of the following credit protection services: one year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports; data breach analysis;[63] fraud resolution services (including dispute letters, fraud alerts, and credit freezes); and/or one year of identity theft insurance with $20,000 coverage and $0 deductible. The determination by the Secretary regarding whether

---

[62] In the regulations the VA solicits comments on use of data mining for the development of information to assist in preparation of risk analysis following a data breach, and on the purposes for which data mining would be appropriate and acceptable uses of the information resulting from data mining.

[63] "The term "data breach analysis" means the process used to determine if a data breach has resulted in the misuse of sensitive personal information." 38 U.S.C. § 5727(5).

any or all of these credit protection services will be offered to individuals subject to a data breach will depend on certain specified considerations.

The Private Sector

Although no single federal law or regulation governs the security of all personal information in the private sector, several federal laws and regulations address the security of specific types of personal information.

Health Insurance Portability and Accountability Act

Part C of the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[64] requires "the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[65] Such standards are required to be consistent with the objective of reducing the administrative costs of providing and paying for health care. These "Administrative Simplification" provisions require the Secretary of Health and Human Services to adopt national standards to: facilitate the electronic exchange of information for certain financial and administrative transactions; establish code sets for data elements; protect the privacy of individually identifiable health information; maintain administrative, technical, and physical safeguards for the security of health information; provide unique health identifiers for individuals, employers, health plans, and health care providers; and to adopt procedures for the use of electronic signatures.[66]

HIPAA covered entities — health plans, health care clearinghouses, and health care providers who transmit financial and administrative transactions electronically — are required to comply with the national standards and regulations promulgated pursuant to Part C.[67] Under HIPAA, the Secretary is required to impose a civil monetary penalty on any person failing to comply with the Administrative Simplification provisions in Part C.[68] The maximum civil money penalty (i.e., the fine) for a violation of an administrative simplification provision is $100 per violation and up to $25,000 for all violations of an identical requirement or prohibition during a calendar year.[69] HIPAA also establishes criminal penalties for any person who knowingly and in violation of the Administrative Simplification

---

[64] P.L. 104-191, 110 Stat. 1936 (1996), codified in part at 42 U.S.C. §§ 1320d *et seq.;* see CRS Report RL33989, *Enforcement of the HIPAA Privacy Rule*, by Gina Marie Stevens

[65] 42 U.S.C. §§ 1320d — 1320d-8.

[66] 42 U.S.C. §§ 1320d-2(a)-(d). HHS has issued final regulations to adopt national standards for transactions and code sets, privacy, security, and employer identifiers.

[67] 42 U.S.C. § 1320d-4(b) requires compliance with the regulations within a certain time period by "each person to whom the standard or implementation specification [adopted or established under sections 1320d-1 and 1320d-2] applies.

[68] 42 U.S.C. § 1320d-5(a).

[69] 42 U.S.C. § 1320d-5(a)(1).

provisions of HIPAA uses a unique health identifier, or obtains or discloses individually identifiable health information.[70] Enhanced criminal penalties may be imposed if the offense is committed under false pretenses, with intent to sell the information or reap other personal gain. The penalties include (1) a fine of not more than $50,000 and/or imprisonment of not more than one year; (2) if the offense is under false pretenses, a fine of not more than $100,000 and/or imprisonment of not more than five years; and (3) if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000 and/or imprisonment of not more than 10 years.[71] These penalties do not affect any other penalties that may be imposed by other federal programs.

HIPAA Privacy Standard. HIPAA requires health plans, health care clearinghouses, and health care providers who transmit financial and administrative transactions electronically to take steps to ensure the privacy of medical records and to prohibit the disclosure of certain information without patient consent.[72] The HIPAA Privacy Rule issued by HHS in 2002 requires a covered entity to maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule.[73] The Office of Civil Rights (OCR) in HHS is responsible for enforcing the Privacy Rule.[74]

HIPAA Security Standards. Regulations governing security standards under HIPAA require health care covered entities to maintain administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of electronic "protected health information"[75]; to protect against any reasonably anticipated threats or hazards to the security or integrity of such information, as well as protect against any unauthorized uses or disclosures of such

---

[70] 42 U.S.C. § 1320d-6.

[71] 42 U.S.C. § 1320d-6(b).

[72] 45 C.F.R. Part 164 Subpart E — Privacy of Individually Identifiable Health Information.

[73] 45 C.F.R. § 164.530(c).

[74] 65 Fed. Reg. 82381.

[75] "The term "individually identifiable health information" means any information, including demographic information collected from an individual, that - (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and - (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. 42 U.S.C. § 1320d(6).

information.[76] The Centers for Medicare and Medicaid Services (CMS) has been delegated authority to enforce the HIPAA Security Standard.[77]

The Security Rule applies only to protected health information in electronic form (EPHI), and requires a covered entity to ensure the confidentiality, integrity, and availability of all EPHI the covered entity creates, receives, maintains, or transmits. Covered entities must protect against any reasonably anticipated threats or hazards to the security or integrity of such information, and any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule; and ensure compliance by its workforce.[78]

The Security Rule allows covered entities to consider such factors as the cost of a particular security measure, the size of the covered entity involved, the complexity of the approach, the technical infrastructure and other security capabilities in place, and the nature and scope of potential security risks. The Security Rule establishes "standards" that covered entities must meet, accompanied by implementation specifications for each standard.

The Security Rule identifies three categories of standards: administrative, physical, and technical. Administrative safeguards primarily address the policies and procedures a covered entity must have to insure the confidentiality, integrity, and availability of EPHI. Physical safeguards focus on the physical security measures in place to secure EPHI. Technical safeguards detail the standards for access control, auditing, user authentication and the other technical measures involved in securing stored and transmitted EPHI.

The Security Rule requires covered entities to enter into agreements with business associates who create, receive, maintain or transmit EPHI on their behalf. Under such agreements, the business associate must: implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the covered entity's electronic protected health information; ensure that its agents and subcontractors to whom it provides the information do the same; and report to the covered entity any security incident of which it becomes aware. The contract must also authorize termination if the covered entity determines that the business associate has violated a material term. A covered entity is not liable for violations by the business associate unless the covered entity knew that the business associate was engaged in a practice or pattern of activity that violated HIPAA, and the covered entity failed to take corrective action.

---

[76] HIPAA Security Standards for the Protection of Electronic Personal Health Information, 45 C.F.R. Part 164 (Feb. 20, 2003); see CRS Report RL30620, *Health Information Standards, Privacy, and Security: HIPAA's Administrative Simplification Regulations*, by C. Stephen Redhead.

[77] See generally, Centers for Medicare and Medicaid Services, *Security Materials* at [http://www.cms.hhs.gov/EducationMaterials/04_SecurityMaterials.asp#TopOfPage].

[78] 45 C.F.R. § 164.306(a).

Gramm-Leach-Bliley Act

Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA) requires financial institutions to provide customers with notice of their privacy policies, and requires financial institutions to safeguard the security and confidentiality of customer information, to protect against any anticipated threats or hazards to the security or integrity of such records; 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. Financial institutions are defined as businesses that are engaged in certain "financial activities" described in Section 4(k) of the BankHolding Company Act of 1956 and accompanying regulations.[79] Such activities include traditional banking, lending, and insurance functions, along with other financial activities. Financial institutions are prohibited from disclosing "nonpublic personal information"[80] to non-affiliated third parties without providing customers with a notice of privacy practices and an opportunity to opt-out of the disclosure. A number of statutory exceptions are provided to this disclosure rule, including that financial institutions are permitted to disclose nonpublic personal information to a non-affiliated third party to perform services for or functions on behalf of the financial institution. To the extent that data brokers fall within GLBA's definition of "financial institution," they are required to maintain reasonable security for customer information.

GLBA Privacy Rule. Regulations implementing GLBA's privacy requirements published by the federal banking regulators govern the treatment of nonpublic personal information about consumers by financial institutions, require a financial institution in specified circumstances to provide notice to customers about its privacy policies and practices, describe the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties, and provide a method for consumers to prevent a financial

---

[79] 12 U.S.C. § 1843(k).

[80] (4) Nonpublic personal information
(A) The term "nonpublic personal information" means personally identifiable financial information —
(i) provided by a consumer to a financial institution;
(ii) resulting from any transaction with the consumer or any service performed for the consumer; or
(iii) otherwise obtained by the financial institution.
(B) Such term does not include publicly available information, as such term is defined by the regulations prescribed under section 6804 of this title.
(C) Notwithstanding subparagraph (B), such term —
(i) shall include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but
(ii) shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information. 15 U.S.C. § 6809(4).

institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure, subject to exceptions.[81]

FTC Safeguards Rule. This rule implements GLBA's requirements for entities under FTC jurisdiction. The Safeguards Rule applies to all businesses, regardless of size, that are "significantly engaged" in providing financial products or services. These include, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, real estate appraisers, and professional tax preparers. The Safeguards Rule also applies to companies like credit reporting agencies and ATM operators that receive information about the customers of other financial institutions. The rule requires financial institutions to have an information security plan that "contains administrative, technical, and physical safeguards" to "insure the security and confidentiality of customer information: protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer."[82] Using its authority under the Safeguards Rule, the Commission has brought a number of enforcement actions to address the failure to provide reasonable and appropriate security to protect consumer information.[83]

Information Security Standards. Section 501(b) of GLBA requires the banking agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards to ensure the security, confidentiality, and integrity of customer information, protect against any anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Similar to the Safeguards Rule issued by the FTC, Interagency Guidance issued by the federal banking regulators applies to customer information which is defined as "any record containing nonpublic personal information ... about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of" a financial institution."[84] The security guidelines direct each financial institution to assess the risks of reasonably foreseeable threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information and customer information systems, the likelihood and potential damage of threats, and the sufficiency of policies, procedures, customer information systems, and other controls. Following the assessment of risks, the security guidelines require a financial

---

[81] See generally, 12 C.F.R. 225.28, 225.86

[82] Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information, 16 C.F.R. Part 314.

[83] For information on enforcement actions the Commission has brought involving the privacy of consumer information under Section 5 of the FTC Act, see [http://www.ftc.gov/privacy/privacyinitiatives/safeguards_enf.html].

[84] See Board of Governors Federal Reserve System, The Commercial Bank Examination Manual, Supp. 27, 984-1034(May 2007)at [http://www.federalreserve.gov/boarddocs/SupManual/cbem/200705/0705cbem.pdf].

institution to manage and control the risk through the design of a program to address the identified risks, train staff to implement the program, regularly test the key controls, systems, and procedures of the information security program, and develop and maintain appropriate measures to dispose of customer information. The security guidelines also direct every financial institution to require its service providers by contract to implement appropriate measures designed to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Each financial institution is required to monitor, evaluate, and adjust its information security program as necessary. Finally, each financial institution is required to report to its board at least annually on its information security program, compliance with the security guidelines, and issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security breaches or violations and management's responses, and recommendations for changes in the information security program.[85]

Response Programs for Unauthorized Access to Customer Information and Customer Notice. The security guidelines recommend implementation of a risk-based response program, including customer notification procedures, to address unauthorized access to or use of customer information maintained by a financial institution or its service provider that could result in substantial harm or inconvenience to any customer, and require disclosure of a data security breach if the covered entity concludes that "misuse of its information about a customer has occurred or is reasonably possible."[86] Pursuant to the guidance, substantial harm or inconvenience is most likely to result from improper access to "sensitive customer information."[87]

At a minimum, an institution's response program should contain procedures 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; notifying its primary federal regulator when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer

---

[85] The Office of the Comptroller of the Currency assessed a $180,000 civil penalty by consent against a bank's subsidiary for allegedly failing to dispose of confidential customer information in a secure fashion, in violation of OCC regulations governing the security of customer information *In the Matter of First Horizon Home Loan Corporation (operating subsidiary of First Tennesseee Bank N.A., Memphis, Tenn.),* Doc. No. 2005-78 (June 30, 2005).

[86] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, Part III of Supplement A to Appendix, at 12 C.F.R. Part 30 (OCC), Supplement A to Appendix D-2, at 12 C.F.R. Part 208 (Federal Reserve System), 12 C.F.R. Part 364 (FDIC), and 12 C.F.R. Part 568 (Office of Thrift Supervision), 70 Fed. Reg. 15736 - 15754 (March 29, 2005).

[87] "Sensitive customer information means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number." 70 Fed. Reg. 15736-15754 (Mar. 29, 2005).

information; consistent with the Agency's Suspicious Activity Report ("SAR") regulations, notifying appropriate law enforcement authorities; taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information (e.g., by monitoring, freezing, or closing affected accounts and preserving records and other evidence); and notifying customers when warranted.

The security guidelines note that financial institutions have an affirmative duty to protect their customers' information against unauthorized access or use, and that customer notification of a security breach involving the customer's's information is a key part of that duty. The guidelines prohibit institutions from forgoing or delaying customer notification because of embarrassment or inconvenience.

The guidelines provide that when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. The institution should notify its customers as soon as notification will no longer interfere with the investigation.

If a financial institution can determine which customers' information has been improperly accessed, it may limit notification to those customers whose information it determines has been misused or is reasonably likely to be misused. In situations where the institution determines that a group of files has been accessed improperly, but is unable to identify which specific customers' information has been accessed, and the institution determines that misuse of the information is reasonably possible, it should notify all customers in the group. The guidelines also address what information should be included in the notice sent to the financial institution's customers.

Conclusion

As Congress considers legislation to impose additional information security requirements and breach notification obligations on entities that collect, maintain, or process personal information — whether sensitive or individually identifiable — it will do so against an existing patchwork of relatively recent federal and state laws and regulations that impose obligations on many information owners, and that require notice to persons affected by the breach of their personal information. An important issue to be addressed is harmonization of these various laws in order to provide uniform protections for personal information not dependent on the owner of the information or the category of information involved. crsphpgw