Federal Information Security and Data Breach Notification Laws

Gina Stevens
Legislative Attorney

January 28, 2010

Congressional Research Service
7-5700
www.crs.gov
RL34120

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

The following report describes information security and data breach notification requirements included in 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, the Health Information Technology for Economic and Clinical Health Act, the Gramm-Leach-Bliley Act, the Federal Trade Commission Act, and the Fair Credit Reporting Act. Also included in this report is a brief summary of the Payment Card Industry Data Security Standard (PCI DSS), an industry regulation developed by VISA, MasterCard, and other bank card distributors.

Information security laws 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 such information for unauthorized purposes. Data breach notification laws typically require covered entities to implement a breach notification policy, and include requirements for incident reporting and handling and external breach notification.

Expectations of many are that efforts to enact data security legislation will continue in 2010. In the first session of the 111th Congress the House passed H.R. 2221 (Rush and Stearns), the Data Accountability and Trust Act, which would apply only to businesses engaged in interstate commerce, and require data security programs and notification of breaches to affected consumers. The Senate Judiciary Committee approved S. 139 (Feinstein), the Data Breach Notification Act, which would apply to any agency, or business engaged in interstate commerce; and S. 1490 (Leahy), the Personal Data Privacy and Security Act of 2009, which would apply to business entities engaged in interstate commerce and require data security programs and notification to individuals affected by a security breach. S. 1490 also includes data accuracy requirements for data brokers, and requirements concerning government acccess to and use of commercial data.

For related reports, see the Current Legislative Issues Web page for "Privacy and Data Security" available at http://www.crs.gov/Pages/subissue.aspx?cliid=2105&parentid=14. This report will be updated.

Contents

Contacts

Background

Because of questions about the security of sensitive personal information, this report provides an overview of federal information security and data breach notification laws that are applicable to certain entities that collect, maintain, own, possess, or license sensitive personal information.[1]

Information security laws are designed to protect personally identifiable information or sensitive personal information from compromise, and from unauthorized disclosure, acquisition, access, or other situations where unauthorized persons have access or potential access to personally identifiable information for unauthorized purposes. Data breach notification laws typically require covered entities to implement a breach notification policy, and include requirements for incident reporting and handling and external breach notification. A data breach occurs when there is a loss or theft of, or other unauthorized access to, data containing sensitive personal information that results in the potential compromise of the confidentiality or integrity of data. Data breach notification laws typically cover "personally identifiable information" or "individually identifiable information."

No single federal law or regulation governs the security of all types of sensitive personal information. Determining which federal law, regulation, and guidance is applicable depends in part on the entity or sector that collected the information, and the type of information collected and regulated. Under federal law certain sectors are legally obligated to protect certain types of 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 breach notice to affected persons.[2]

For example, there are federal information security requirements applicable to all federal government agencies (FISMA) and a federal information security law applicable to a sole federal department (Veterans Affairs). In the private sector, different laws apply to private sector entities engaged in different businesses. This is what is commonly referred to as a sectoral approach to the protection of personal information.

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.[3] 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. Others advocate a national standard

[1] For 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), see CRS Report RL34409, *Selected Laws Governing the Disclosure of Customer Phone Records by Telecommunications Carriers*, by Kathleen Ann Ruane. For 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, see 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.

[2] Smedinghoff, Thomas J. , The State of Information Security Law: A Focus on the Key Legal Trends (May 2008). Available at SSRN: http://ssrn.com/abstract=1114246.

[3] Tom Zeller, Jr., *"Breach Points Up Flaws in Privacy Laws,"* N.Y. Times, Feb. 24, 2005 at A1.

for entities that maintain personal information in order to harmonize legal obligations.[4] Others distinguish between private data held by the government and private data held by others, and advocate a higher duty of care for governments with respect to sensitive personal information in the U.S. public sector and to data breaches.[5]

In the absence of a comprehensive federal data breach notification law, the majority of states have passed bills or introduced legislation to require businesses and/or government agencies to notify persons affected by breaches involving their sensitive personal information, and in some cases to implement information security programs to protect the security, confidentiality, and integrity of data.[6] As of December 9, 2009, 45 states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.[7] Several states have reportedly considered legislation to hold retailers liable for third party companies' costs arising from data breaches (California, Connecticut, Illinois, Massachusetts, Minnesota, New Jersey, Texas, and Wisconsin).[8] Many states provide a safe harbor for an entity that is regulated by state or federal law and maintains procedures pursuant to such laws, rules, regulations, or guidelines. Reportedly 29 states impose similar duties for the public and private sectors, 14 states do not, and Oklahoma's law applies only to the public sector.[9]

Numerous data breaches and computer intrusions have been disclosed by the nation's largest data brokers, retailers, educational institutions, government agencies, health care entities, financial institutions, and Internet businesses. The Privacy Rights Clearinghouse chronicles and reports that over 345 million records containing sensitive personal information[10] were involved in security breaches in the U.S. since January 2005.[11] From February 2005 to December 2006, 100 million personal records were reportedly lost or exposed.[12] In 2006 the personal data of 26.5 million veterans was breached when a VA employee's hard drive was stolen from his home. In 2007 the retailer TJX Companies revealed that 46.2 million credit and debit cards may have been compromised during the breach of its computer network by unauthorized individuals.[13] In 2008 the Hannaford supermarket chain revealed that approximately 4 million debit and credit card numbers were compromised when Hannaford's computer systems were illegally accessed while

---

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

[5] A. Michael Froomkin, "Government Data Breaches," *University of Miami Legal Studies Research Paper No. 2009-20.* Available at SSRN: http://ssrn.com/abstract=1427964.

[6] See *Security Breach Legislation 2009*, National Conference of State Legislatures at http://www.ncsl.org/default.aspx?tabid=18325

[7] See *State Security Breach Notification Laws 2009*, National Conference of State Legislatures at http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.

[8] 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.

[9] See Froomkin, *supra* text accompnying notes 53-56

[10] Sensitive personal information generally includes an individual's name, address, or telephone number, in conjunction with the individual's Social Security number, driver's license number, account number, credit or debit card number, or a personal identification number or password.

[11] Privacy Rights Clearinghouse, A Chronology of Data Breaches, at http://www.privacyrights.org/ar/ChronDataBreaches.htm.

[12] Tom Zeller, *An Ominous Milestone: 100 Million Data Leaks*, N. Y. Times, Dec. 18, 2006, at C3.

[13] U.S. Securities and Exchange Commission, *Form 10-K Annual Report: The TJX Cos., Inc.*, http://www.sec.gov/Archives/edgar/data/109198/000095013507001906/b64407tje10vk.htm.

the cards were being authorized for purchase. There were 1,800 reported cases of fraud connected to the computer intrusion. In 2009, personal information from Health Net on almost half a million Connecticut residents, and 1.5 million patients nationally (including patients in Arizona, New Jersey, and New York) was breached.[14] The information had been compressed, but not encrypted.

Data breaches involving sensitive personal information may result in identity theft and financial crimes (e.g., credit card fraud, phone or utilities fraud, bank fraud, mortgage fraud, employment-related fraud, government documents or benefits fraud, loan fraud, and health-care fraud). Identity theft involves the misuse of any identifying information, which could include name, SSN, account number, password, or other information linked to an individual, to commit a violation of federal or state law.[15] According to the Federal Trade Commission, identity theft is the most common complaint from consumers in all 50 states, and accounts for over 35% of the total number of complaints the Identity Theft Data Clearinghouse received for calendar years 2004, 2005, and 2006. In calendar year 2006,[16] of the 674,354 complaints received, 246,035 or 36% were identity theft complaints.[17] With continued media reports of data security breaches,[18] concerns about new cases of identity theft are widespread.[19]

These public disclosures have heightened interest in the security of sensitive personal information;[20] security of computer systems; applicability of federal laws to the protection of sensitive personal information; adequacy of enforcement tools available to law enforcement officials and federal regulators; business and regulation of data brokers;[21] liability of retailers, credit card issuers, payment processors, banks, and furnishers of credit reports for costs arising from data breaches; remedies available to individuals whose personal information was accessed without authorization;[22] prosecution of identity theft crimes related to data breaches; and criminal liability of persons responsible for unauthorized access to computer systems.[23]

---

[14] According to the Privacy Rights Clearinghouse, Connecticut Attorney General Richard Blumenthal is suing Health Net of Connecticut for failing to secure private patient medical records and financial information involving 446,000 Connecticut enrollees and promptly notify consumers exposed by the security breach. The AG is seeking a court order blocking Health Net from continued violations of HIPAA by requiring that any protected health information contained on a portable electronic device be encrypted. This case marks the first action by a state attorney general involving violations of HIPAA since the Health Information Technology for Economic and Clinical Health (HITECH) Act, which authorized state attorneys general to enforce HIPAA.

[15] P.L. 105-318, Identity Theft Assumption and Deterrence Act; 18 U.S.C. § 1028.

[16] The last year for which Identity Theft Victim Complaint Data is available.

[17] Federal Trade Commission, *Identity Theft Victim Complaint Data*, Feb. 7, 2007, at http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse_2006.pdf.

[18] See Nancy Trejos, "Identity Theft Gets Personal: When a Debit Card Number Is Stolen, America's New Crime Wave Hits Home," Washington Post at F01 (Jan. 13, 2008).

[19] CRS Report R40599, *Identity Theft: Trends and Issues*, by Kristin M. Finklea

[20] BNA E-Commerce Law Daily, Data Privacy Expected To Be High Priority for House Commerce Panel, Jan. 15, 2010.

[21] See 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.

[22] See CRS Report RL31919, *Federal Laws Related to Identity Theft*, by Gina Stevens.

[23] See CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle.

Federal Information Security and Data Breach Notification Laws

The following report describes information security and data breach notification requirements included in 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, the Health Information Technology for Economic and Clinical Health Act, the Gramm-Leach-Bliley Act, the Federal Trade Commission Act, and the Fair Credit Reporting Act.

Federal Sector

In August 2009, the Department of Health and Human Services (HHS) issued interim final breach notification regulations to implement Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act (P.L. 111-5), that apply to breaches of protected health information occurring on or after September 23, 2009.[24] Also in 2009, the Federal Trade Commission issued a final rule pursuant to Section 13407 of the HITECH Act requiring certain Web-based businesses to notify consumers when the security of their electronic health information is breached. [25] The FTC rule applies to both vendors of personal health records—which provide online repositories that people can use to keep track of their health information—and entities that offer third-party applications for personal health records.

Privacy Act

The Privacy Act is the principal law governing the federal government's information privacy program. Other relevant federal laws include the Computer Matching and Privacy Protection Act of 1988,[26] and Section 208 of the E-Government Act of 2002 which requires agencies to conduct privacy impact assessments on new information technology systems and electronic information collections.[27] The Privacy Act of 1974[28] governs the collection, use, and dissemination of a "record"[29] about an "individual"[30] maintained by federal agencies in a "system of records."[31] 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. In order for an agency record to be protected by the Privacy Act, it must be retrieved by individual name

[24] Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information, 45 C.F.R. Part 164.400 *et seq.*

[25] Health Breach Notification Rule, 16 C.F.R. 318.

[26] 5 U.S.C. § 552a note.

[27] 44 U.S.C. § 3501 note.

[28] 5 U.S.C. § 552a.

[29] 5 U.S.C. § 552a(a)(4).

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

[31] 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).

or individual identifier. The Privacy Act also applies to systems of records created by government contractors.[32] The Privacy Act does not apply to private databases.

The Privacy Act 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.[33] 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.[34]

Each agency that maintains a system of records is 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 result in substantial harm, embarrassment, inconvenience, or unfairness to any individual ... "[35]

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 whenever an agency fails to compy with the act "in such a way as to have an adverse effect on an individual."[36] 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.[37] 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.[38]

Federal Information Security Management Act

FISMA is the principal law governing the federal government's information security program. Title III of the E-Government Act of 2002, the Federal Information Security Management Act of 2002 (FISMA),[39] requires federal government agencies to provide information security

[32] 5 U.S.C. § 552(m).

[33] 5 U.S.C. § 552a(e)(5).

[34] 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. 5 U.S.C. § 552e(4).

[35] 5 U.S.C. § 552a(e)(10).

[36] 5 U.S.C. § 552a(g)(1)(D).

[37] 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 alleging violations of the Administrative Procedure Act and the Privacy Act. *Vietnam Veterans of America, Inc. et al. V. Nicholson,* No. 1:06-cv-01038-JR (D. D.C. filed June 6, 2006).

[38] 5 U.S.C. § 552a(v). 40 Fed. Reg. 28976 (July 9, 1975).

[39] 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 D. Moteff.

protections for agency information and information systems.[40] Agencies are required to develop, document, and implement an agency wide 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."[41]

The agency's information security plan also must include procedures for detecting, reporting, and responding to security incidents; notifying and consulting with the Federal information security incident center and with law enforcement agencies and relevant Offices of Inspector General.[42] 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. Agencies are required to comply with the information security standards developed by NIST.[43] Agencies must also conduct, annually, an independent evaluation of their security programs. The evaluations are forwarded to the Director of the Office of Management and Budget, for an annual report to Congress.[44] The Director's authorities do not include national security systems.[45]

Agency heads are responsible for compliance with FISMA's requirements and related information security policies, procedures, standards, and guidelines, and for ensuring that senior agency officials provide information security. The authority to ensure compliance is delegated to the agency Chief Information Officer (CIO). FISMA also assigns specific policy and oversight responsibilities to the Office of Management and Budget (OMB).

---

[40] Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability. 44 U.S.C. § 3542.

[41] 44 U.S.C. § 3544(a)(1)(A).

[42] 44 U.S.C. § 3544(b)(7).

[43] 44 U.S.C. § 3544(a)(1)(B); 40 U.S.C. § 11331.

[44] 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), available at http://www.gao.gov/new.items/d07935t.pdf.

[45] FISMA defines a national security system, in statute, as:

Any computer system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(i) the function of which—

(I) involves intelligence activities;

(II) involves cryptologic activities related to national security;

(III) involves command and control of military forces;

(IV) involves equipment that is an integral part of a weapon or weapons system;

(V) ...is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

The definition explicitly excludes systems that are used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). P.L. 107-347,§ 301(b)(1).

Office of Management and Budget "Breach Notification Policy"

In response to recommendations from the President's Identity Theft Task Force,[46] the Office of Management and Budget issued guidance in May 2007 for federal agencies on "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."[47] The OMB Memorandum M-07-16 requires all federal agencies to implement a breach notification policy to safeguard "personally identifiable information" by August 22, 2007 to apply to both electronic systems and paper documents.[48] To formulate their policy, agencies are 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.

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. Two new privacy requirements and five new security requirements are established. 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.[49]

Attachment 2 of the OMB Memorandum, Incident Reporting and Handling Requirements, applies to the breach of personally identifiable information in electronic or paper format. Agencies are required to report all incidents involving personally identifiable information within one hour of discovery/detection; and publish a "routine use"[50] under the Privacy Act applying to the disclosure of information to appropriate persons in the event of a data breach.[51]

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. Each agency is

[46] Exec. Order No. 13,402, 71 FR 27945 (2006).

[47] http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

[48] The memo defines the term "personally identifiable information" as "information which 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." *Id.*

[49] The first four information security requirements were adopted in an earlier memorandum, See OMB Memo 06-16, "Protection of Sensitive Agency Information" at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf.

[50] 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).

[51] OMB Memorandum M-07-16, p.11.

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 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. 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 rules of behavior and identifying consequences and corrective actions available for failure to follow these rules. 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. 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,[52] 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)[53] 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.[54]

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.[55] 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 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

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

[53] "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.

[54] See CRS Report RL33612, *Department of Veterans Affairs: Information Security and Information Technology Management Reorganization*, by Sidath Viranga Panangala.

[55] 38 U.S.C. § 5722.

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"[56] 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.[57] 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.[58]

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.[59] If the breach involved the sensitive data of DOD civilian or enlisted personnel the Secretary must also report to the Armed Services Committees.[60] 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.[61] 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.[62]

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 personal information.[63] 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.

[56] "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).

[57] 38 U.S. C. § 5724(a)(1).

[58] 38 U.S. C. § 5724(a)(2).

[59] 38 U.S.C. § 5724(c)(1).

[60] 38 U.S.C. § 5724(c)(2).

[61] 38 U.S.C. § 5726.

[62] 38 U.S.C. § 5724(b).

[63] 38 U.S.C. § 5725.

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.[64] 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.[65] The final regulations, issued April 2008, adopted the interim rule without change.[66] 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.

Private Sector

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.

Health Insurance Portability and Accountability Act

Part C of the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[67] requires "the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[68] 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; and to adopt procedures for the use of electronic signatures.[69]

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.[70] 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.[71] The maximum civil money penalty (i.e., the

[64] 38 U.S. C. § 5724(b).

[65] 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. 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. *Id.*

[66] 73 Fed. Reg. 19747 (Apr. 11, 2008).

[67] 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 and Security Rules*, by Gina Stevens.

[68] 42 U.S.C. §§ 1320d—1320d-8.

[69] 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.

[70] 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.

[71] 42 U.S.C. § 1320d-5(a).

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.[72] HIPAA also establishes criminal penalties for any person who knowingly and in violation of the Administrative Simplification provisions of HIPAA uses a unique health identifier, or obtains or discloses individually identifiable health information.[73] 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.[74] These penalties do not affect other penalties imposed by other federal programs.

Privacy Standard

HIPAA also addressed the privacy of individually identifiable health information and required adoption of a national privacy standard.[75] HHS issued final Standards for Privacy of Individually Identifiable Health Information, known as the Privacy Rule, on April 14, 2003.[76] The HIPAA Privacy Rule is applicable to health plans, health care clearinghouses, and health care providers who transmit financial and administrative transactions electronically. The rule regulates protected health information that is "individually identifiable health information"[77] transmitted by or maintained in electronic, paper, or any other medium.[78] The definition of PHI excludes individually identifiable health information contained in certain education records and employment records held by a covered entity in its role as employer.

The HIPAA Privacy Rule limits the circumstances under which an individual's protected health information may be used or disclosed by covered entities. A covered entity is permitted to use or disclose protected health information without patient authorization for treatment, payment, or health care operations.[79] For other purposes, a covered entity may only use or disclose PHI with patient authorization subject to certain exceptions.[80] Exceptions permit the use or disclosure of PHI without patient authorization or prior agreement for public health, judicial, law enforcement, and other specialized purposes.[81] In certain situations that would otherwise require authorization,

[72] 42 U.S.C. § 1320d-5(a)(1).

[73] 42 U.S.C. § 1320d-6.

[74] 42 U.S.C. § 1320d-6(b).

[75] HIPAA required a privacy standard that would address the rights of the subject of individually identifiable health information, the procedures established for the exercise of such rights, and authorized or required uses and disclosures of such information. P.L. 104-191, Title II, § 264, Aug. 21, 1996, 110 Stat. 2033, 42 U.S.C. § 1320d-2 (note).

[76] 45 C. F.R. Part 164 Subpart E—Privacy of Individually Identifiable Health Information.

[77] 45 C.F.R. § 160.103.

[78] See *South Carolina Medical Assoc. v. Thompson*, 327 F.3d 346 (4th Cir. 2003)(HIPAA could be interpreted to include non-electronic medical records).

[79] 45 C.F.R. § 164.506.

[80] 45 C.F.R. § 164.508.

[81] 45 C.F.R. § 164.512(a)-(l).

a covered entity may use or disclose PHI without authorization provided that the individual is given the opportunity to object or agree prior to the use or disclosure.[82]

The HIPAA Privacy Rule also provides for accounting of certain disclosures;[83] requires covered entities to make reasonable efforts to disclose only the minimum information necessary; requires most covered entities to provide a notice of their privacy practices;[84] establishes individual rights to review and obtain copies of protected health information;[85] requires covered entities to safeguard protected health information from inappropriate use or disclosure; and gives individuals the right to request changes to inaccurate or incomplete protected health information.[86]

The HIPAA Privacy Rule requires a covered entity to maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent use or disclosure of protected health information in violation of the Privacy Rule.[87] The Office of Civil Rights (OCR) in HHS enforces the Privacy Rule.[88]

Security Standard

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"[89]; 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 information.[90] The Centers for Medicare and Medicaid Services (CMS) has been delegated authority to enforce the HIPAA Security Standard.[91]

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

[82] 45 C.F.R. § 164.510.

[83] 45 C.F.R. § 164.528.

[84] 45 C.F.R. § 164.520.

[85] 45 C.F.R. § 164.524.

[86] 45 C. F.R. § 164.526.

[87] 45 C.F.R. § 164.530(c).

[88] 65 Fed. Reg. 82381.

[89] "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).

[90] HIPAA Security Standards for the Protection of Electronic Personal Health Information, 45 C.F.R. Part 164 (February 20, 2003).

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

reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule; and ensure compliance by its workforce.[92]

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.

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.

Subtitle D (Privacy) of Title XIII of the ARRA

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) was enacted as Title XIII of Division A (§§ 13001-13424) and Title IV of Division B (§§ 4001-4302) of the American Recovery and Reinvestment Act of 2009 (ARRA) and signed into law on February 17, 2009, by President Obama.[93]

As part of this new law, sweeping changes to the health information privacy regime were enacted. Most of the provisions in Subtitle D (Privacy) of Title XIII of ARRA are additional requirements supplementing the HIPAA Privacy and Security Rules, but a few provisions deal specifically with EHRs.[94] Subtitle D (Privacy) of Title XIII of ARRA extended application of certain provisions of the HIPAA Privacy and Security Rules to the business associates of HIPAA-covered entities making those business associates subject to civil and criminal liability for violations; established new limits on the use of protected health information for marketing and fundraising purposes; provided new enforcement authority for state attorneys general to bring suit in federal district court to enforce HIPAA violations; increased civil and criminal penalties for HIPAA violations; required covered entities and business associates to notify the public or HHS of data breaches (regardless of whether actual harm has occurred); changed certain use and disclosure rules for protected health information; and created additional individual rights.

[92] 45 C.F.R. § 164.306(a).

[93] P.L. 111-5.

[94] An electronic health record is defined as "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff." P.L. 111-5, § 13400(5).

Application of the HIPAA Security Provisions and Penalties to Business Associates

The HITECH Act extended the application of the HIPAA Security Rule's provisions on administrative, physical, and technical safeguards and documentation requirements to business associates of covered entities, making those business associates subject to civil and criminal liability for violations of the HIPAA Security Rule.[95]

Under the HIPAA Security Rule, only covered entities can be held civilly or criminally liable for violations. While business associates are still not technically considered covered entities under HIPAA, they will be subject to the same civil and criminal penalties as a covered entity for Security Rule violations after February 17, 2010.[96] The HITECH Act also requires existing business associate agreements to incorporate the new security requirements added by the HITECH Act.[97] The Secretary is also directed to issue annual guidance on the most effective and appropriate technical safeguards.[98] The guidance issued by HHS specifies encryption and destruction as the technologies and methodologies for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals.[99] Covered entities and business associates, as well as entities covered by the FTC regulations, that secure information as specified by the guidance are relieved from providing notifications following the breach of such information.

Breach Notification

Prior to the enactment of the HITECH Act, neither the HIPAA Privacy nor Security Rule required covered entities or business associates to notify individuals when the security or privacy of their PHI had been compromised. Furthermore, vendors of personal health records (PHRs) were also under no obligation to notify affected individuals or the public after a breach of privacy or security.[100] The HITECH Act imposed such notification requirements on covered entities and business associates. A similar requirement was also imposed on vendors of PHR's.

The HITECH Act requires covered entities, business associates, and vendors of PHR's to notify affected individuals in the event of a "breach" of "unsecured protected health information."[101] A "breach" is defined as the "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."[102] A vendor of PHR is defined as "an entity, other than a covered

[95] P.L. 111-5, § 13401. The HITECH Act adopts the same definition of business associates as the HIPAA Privacy and Security Rules. 45 C.F.R. § 160.103.

[96] P.L. 111-5, §§ 13401(b), 13404(c).

[97] P.L. 111-5, § 13404(a).

[98] P.L. 111-5, § 13401(c).

[99] 74 Fed. Reg. 19006 (Apr. 27, 2009).

[100] A PHR is defined as "an electronic record of identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." P.L. 111-5, § 13400(11). A vendor of PHR is defined as "an entity, other than a covered entity ... that offers or maintains a personal health record." P.L. 111-5, § 13400(18).

[101] P.L. 111-5, §§ 13402, 13407.

[102] P.L. 111-5, § 13400(1). Not included in the definition of breach are any unintentional acquisition, use, or access of (continued...)

entity ... that offers or maintains a personal health record."[103] The term "unsecured protected health information" means "protected health information that is not secured through the use of a technology or methodology specified by the Secretary in guidance."[104] The HITECH Act required the HHS Secretary to issue guidance by April 17, 2009, and annually thereafter specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.[105] The HITECH Act also provides a default definition if such guidance is not issued. Under the default definition, PHI is unsecured if

> it is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and that is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

On April 17, 2009, guidance on the meaning of "unsecured protected health information " was issued by HHS.[106] The guidance became effective upon issuance; however, the comment period remained open until May 17, 2009. It identified two methods for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals: encryption and destruction (paper and electronic form). Pursuant to this guidance, "if PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals by one or more of the methods identified in this guidance, then such information is not 'unsecured' PHI. Thus, because the breach notification requirements apply only to breaches of unsecured PHI, this guidance provides the means by which covered entities and their business associates are to determine whether a breach has occurred [and the extent] to which the notification obligations under the Act and its implementing regulations apply."[107]

Notice of Unauthorized Disclosure of Protected Health Information

Section 13402 of the HITECH Act requires a covered entity to notify affected individuals when it discovers that their unsecured PHI has been, or is reasonably believed to have been, breached.[108] This requirement applies to covered entities that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information. The scope of notification is dependant upon the number of individuals whose unsecured PHI was compromised. Generally, only written notice need be provided if less than 500 individuals are

(...continued)

PHI by an employee or other authorized individual of a covered entity or a business associate done in good faith and within the scope of employment or the relationship where such information is not breached any further; or inadvertent disclosures by authorized persons of PHI within the same facility; and information received as a result of such disclosure is not further disclosed without authorization.

[103] P.L. 111-5, § 13400(18).

[104] P.L. 111-5, § 13402(h).

[105] P.L. 111-5, § 13402(h).

[106] HHS, *Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009*, at 2, available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf.

[107] *Id.* at 15-16.

[108] P.L. 111-5, § 13402(a).

involved.[109] For larger breaches, notice through prominent media outlets may be required. In all cases, the Secretary of HHS must be notified, although breaches involving less than 500 people may be reported on an annual basis. The Secretary of HHS is directed to display on the department's website a list of covered entities with breaches involving more than 500 individuals.

Generally, notice must be given without unreasonable delay, but no later than 60 days after the breach is discovered. If a delay is not reasonable, a covered entity may still have violated this provision even if notice was given within 60 days. In an enforcement action of this provision, the covered entity has the burden of proving that any delay was reasonable. Delayed notification is permitted for law enforcement purposes if a law enforcement official determines that notice would impede a criminal investigation or cause damage to national security.

To the extent possible, notification of a breach must include a description of what occurred; the types of information involved in the breach; steps individuals should take in response to the breach; what the covered entity is doing to investigate, mitigate, and protect against further harm; and contact information to obtain additional information.

No later than February 17, 2010, and annually thereafter, the Secretary is required to submit a report to Congress containing information on the number and nature of breaches for which notice was provided, and actions taken in response to such breaches.[110] The Secretary is also directed to issue interim final regulations, no later than 180 days after enactment, to implement the breach notification requirement.[111] This breach notification requirement will apply to breaches that are discovered 30 days after these regulations are promulgated.[112] The Breach Notification Interim Final Regulation was issued August 24, 2009, addressing notification to individuals, the media, and the Secretary, by a business associate; law enforcement delay; and administrative requirements and burdens of proof.[113]

Notice of Unauthorized Disclosure of Personal Health Records

Section 13407 of the HITECH Act includes a breach notification requirement for PHR vendors (such as Google Health or Microsoft Vault), service providers to PHR vendors, and PHR servicers that are not covered entities or business associates that sunsets "if Congress enacts new legislation."[114] Under this breach notification requirement, these entities are required to notify citizens and residents of the United States whose unsecured "PHR identifiable health information" has been, or is believed to have been, breached. PHR vendors, service providers to PHR vendors, and PHR servicers are also required to notify the federal government, although in this case the governing agency is the Federal Trade Commission (FTC) and not HHS.[115]

---

[109] If recent contact information for these individuals cannot be obtained, more public notice via the covered entity's website or through media publications may be required. P.L. 111-5, § 13402(e)(1)(B).

[110] P.L. 111-5, § 13402(i).

[111] P.L. 111-5, § 13402(j).

[112] *Id.*

[113] 45 C.F.R. 164.400 *et seq.*, available at http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf.

[114] P.L. 111-5, § 13407(g)(2). For further information on electronic personal health records, *see* CRS Report RS22760, *Electronic Personal Health Records*, by Gina Stevens.

[115] The FTC is directed to also notify the Secretary of HHS in the event of a breach.

The HITECH Act defines several terms specific to the PHR breach notification requirement. A "breach of security" is defined as the unauthorized acquisition of an individual's PHR identifiable health information.[116] PHR identifiable health information is defined as individually identifiable health information, and includes information provided by or on behalf of the individual, and information that can reasonably be used to identify the individual.[117]

The requirements regarding the scope, timing, and content of these notifications are identical to the requirements applicable to breaches of PHI under § 13402 of the HITECH Act. Violations of these requirements shall be considered unfair and deceptive trade practices in violation of the Federal Trade Commission Act.[118]

The HITECH Act also directed the FTC to issue regulations implementing these requirements by August 18, 2009. A Health Breach Notification Rule was promulgated by the FTC on August 25, 2009.[119] It would apply to breaches that are discovered after September 18, 2009, by vendors of PHRs, PHR-related entities, and third party service providers—irrespective of any jurisdictional tests in the FTC Act—that maintain information on U.S. citizens or residents.[120] The rule contains provisions discussing timeliness, methods of notification, content, and enforcement of the breach notification requirements.

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.[121] 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.[122] Such activities include traditional banking, lending, and insurance functions, along with other financial activities. Financial institutions are prohibited from disclosing "nonpublic personal information"[123] to non-affiliated third parties without providing

[116] P.L. 111-5, § 13407(f)(1).

[117] P.L. 111-5, § 13407(f)(2).

[118] *See* CRS Report RL34120, *Federal Information Security and Data Breach Notification Laws*, by Gina Stevens, at 20-21.

[119]16 C.F.R. 318 *et seq.* (Aug. 25, 2009).

[120] *Id.*.

[121] 15 U.S.C. § 6801 - 6809. *See* CRS Report RS20185, *Privacy Protection for Customer Financial Information*, by M. Maureen Murphy.

[122] 12 U.S.C. § 1843(k).

[123] (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—
(continued...)

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.

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,[124] 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 institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure, subject to exceptions.[125]

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."[126] 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.[127]

Information Security Guidelines

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,

---

(...continued)

(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).

[124] 16 C.F.R. Part 13 (FTC); 12 C.F.R. Parts 40 (OCC), 216 (FRB), 332 (FDIC), 573 (OTS), and 716 (NCUA).

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

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

[127] 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.

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.

Interagency Guidance issued by the federal banking regulators[128] 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."[129] 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 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.

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."[130] Pursuant to the guidance, substantial harm or inconvenience is most likely to result from improper access to "sensitive customer information."[131]

---

[128] *See* 12 C.F.R. Part 30, App. B (national banks); 12 C.F.R. Part 208App. D-2 and Part 255, App. F (state member banks and holding companies); 12 C.F.R. Part 364, App. B (state non-member banks); 12 C.F.R. Part 570, App. B (savings associations; 12 C.F.R. Part 748, App. A (credit unions).

[129] 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.

[130] 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).

[131] "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 (continued...)

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 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.

Federal Trade Commission Act

The Federal Trade Commission (FTC), an independent agency of the U.S. government, was established by the Federal Trade Commission Act of 1914 (FTCA).[132] Its principal mission is the promotion of consumer protection and the elimination and prevention of anticompetitive business practices. The Commission's jurisdiction extends to a variety of entities and individuals operating in commerce. The FTC has taken a multi-faceted approach to protecting the privacy and security of consumers' personal information. Its enforcement tools include laws and regulations such as the Safeguards Rule issued under the Gramm-Leach-Bliley Act, which requires financial

(...continued)

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 (March 29, 2005).

[132] 15 U.S.C. §§ 41-58.

institutions to take reasonable measures to protect customer data, and the Disposal Rule under the FACT Act which requires companies to dispose of credit report data in accord with a set of practices designed to prevent others from using that data without authorization.[133]

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[134] Unfair practices are practices that cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers not offset any countervailing benefit to consumers or competition.[135] A representation, omission, or practice is deceptive if (1) it is likely to mislead consumers acting reasonably under the circumstances; and (2) it is material—likely to affect consumers' conduct or decisions with respect to the product at issue.[136]

The Commission has used Section 5 to challenge deceptive claims companies have made about the privacy and security of their customers' personal information. In deceptive security claims cases the FTC alleged that the companies had made promises to take reasonable steps to protect sensitive consumer information, and that they did not implement reasonable and appropriate measures to protect the sensitive personal information obtained from customers against unauthorized access.[137] In unfair practices cases, the FTC has alleged that a company's failure to employ reasonable and appropriate security measures to protect consumers' personal information caused or was likely to cause substantial injury to consumers that was not offset by countervailing benefits to consumers or competition and was not reasonably avoidable by consumers.

In cases where the FTC did not have authority to assess civil money penalties, the FTC entered into consent orders requiring the defendants to implement information security programs (e.g., B.J.'s Wholesale Club, DSW, Inc., and Card Systems). In a recent case where violations of the Federal Trade Commission Act and the Fair Credit Reporting Act were alleged, the largest civil money penalty ever by the FTC ($10 million) was assessed.

Fair Credit Reporting Act, as amended by the Fair and Accurate Transactions Act

The Fair Credit Reporting Act of 1970 (FCRA) regulates credit bureaus, entities or individuals who uses credit reports, and businesses that furnish information to credit bureaus.[138] "[A] major purpose of the Act is the privacy of a consumer's credit-related data."[139] Consumer reporting agencies, also known as credit bureaus, have particular responsibilities with respect to ensuring that a consumer's information is used only for purposes that are permissible under the act,[140] for ensuring that "reasonable procedures" are employed (including making reasonable efforts to verify the identity of each new prospective user of consumer report information and the uses

[133] See CRS Report RL32535, *Implementation of the Fair and Accurate Credit Transactions (FACT) Act of 2003*, by Angie A. Welborn and Grace Chu.

[134] 15 U.S.C. §§ 45(a).

[135] 15 U.S.C. § 45(n).

[136] Cliffdale Associates Inc., 103 F.T.C. 110(1984).

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

[138] 15 U.S.C. §§ 1681 - 1681x, as amended.

[139] *Trans Union Corp. v. FTC*, 81 F.3d 228, 234 (D.C. Cir. 1996).

[140] 15 U.S.C. § 1681e(a).

certified by each prospective user prior to furnishing such user a consumer report) to ensure that consumer reports are supplied only to those with a permissible purpose,[141] and for correcting information in a consumer's report that may be incorrect or the result of fraud.[142] Permissible purposes include decisions involving credit, insurance, or employment.[143] A consumer reporting agency is also permitted to provide reports to persons having "a legitimate business need" for the information in connection with a consumer-oriented transaction. The Act and its requirements only apply to entities that fall within the definition of a "consumer reporting agency,"[144] and only to products that fall within the definition of a "consumer report."[145]

The Fair and Accurate Transactions Act ("FACT Act") amended FCRA, adding requirements designed to prevent identity theft and assist identity theft victims. The FACT Act also included a provision requiring financial regulatory[146] agencies and the FTC to promulgate a coordinated rule designed to prevent unauthorized access to consumer report information by requiring reasonable procedures for the proper disposal of such information.

The Federal Trade Commission enforces the FCRA. A violation under the FCRA is deemed to be an unfair or deceptive act or practice in violation of section 5(a) of the FTC Act. There are various penalties for violating the FCRA, the applicability of a particular provision depends on such factors as who brings the action and the degree of the violator's noncompliance. For example, the Act imposes liability for both willful noncompliance and negligent noncompliance.[147] The monetary penalties include actual damages sustained by a consumer, plus costs and attorneys fees. In the case of willful violations, the court may also award punitive damages to a consumer. Any person who procures a consumer report under false pretenses, or knowingly without a permissible purpose, is liable for $1000 or actual damages (whichever is greater) to both the consumer and to the consumer reporting agency.[148] Also, the Act governs enforcement actions brought by the Commission, other agencies, and the states, and provides for various monetary and injunctive penalties.[149] For those who knowingly violate the FCRA, the monetary penalties include up to $2500 per violation in a civil action brought by the Commission.[150]

---

[141] 15 U.S.C. § 1681e.

[142] For a detailed discussion of the Fair Credit Reporting Act, see CRS Report RL31666, *Fair Credit Reporting Act: Rights and Responsibilities*, by Margaret Mikyung Lee.

[143] 15 U.S.C. § 1681b.

[144] The FCRA defines "consumer reporting agency" as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f).

[145] A "consumer report" is "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes; or any other purpose authorized under section 604 [of the FCRA]." 15 U.S.C. § 1681a(d).

[146] P.L. 108-159, 117 Stat. 1952.

[147] 15 U.S.C. § 1681n(a).

[148] 15 U.S.C. § 1681n(b).

[149] 15 U.S.C. § 1681s.

[150] 15 U.S.C. § 1681s(2)(A).

Payment Card Industry Data Security Standard

The payment card industry has also issued security standards and reporting requirements for organizations that handle bank cards.[151] The Payment Card Industry Data Security Standard (PCI 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. PCI DSS went into effect December 31, 2006. On October 1, 2008, the PCI Security Standards Council (PCI SSC) announced general availability of version 1.2 of the PCI DSS that does not introduce any new major requirements to the existing standard, but does change some practices. Entities that fail to comply with PCI DSS face fines and increases in the rates that the credit card companies charge for transactions, and potentially can have their authorization to process payment cards revoked. Legislation has been passed in the Texas House mandating compliance with the PCI DSS standard.[152]

Author Contact Information

Gina Stevens
Legislative Attorney
gstevens@crs.loc.gov, 7-2581

[151] Available at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

[152] *See*, 2007 Tex. H. B. No. 3222 which mandates PCI DSS compliance, and provides a safe harbor under the statute if the business that suffered the data breach was in compliance with PCI DSS 90 days before the date of the security breach.