Order Code RL33273

CRS Report for Congress

Data Security: Federal Legislative Approaches

Updated June 6, 2008

Gina Marie Stevens
Legislative Attorney
American Law Division

Prepared for Members and
Committees of Congress

Data Security: Federal Legislative Approaches

Summary

During the First Session of the 110th Congress, three data security bills were reported favorably out of Senate committees — S. 239 (Feinstein), a bill to require federal agencies, and persons engaged in interstate commerce, in possession of data containing sensitive personally identifiable information, to disclose any breach of such information; S. 495 (Leahy), a bill to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information; and S. 1178 (Inouye), a bill to strengthen data protection and safeguards, require data breach notification, and further prevent identity theft. On June 3, 2008, H.R. 4791 (Clay), a bill to strengthen requirements for ensuring the effectiveness of information security controls over information resources that support federal operations and assets and to protect personally identifiable information of individuals that is maintained in or transmitted by federal agency information systems, was passed by the House by voice vote under suspension of the rules.

Other data security bills were also introduced including S. 1202 (Sessions), S. 1260 (Carper), S. 1558 (Coleman), H.R. 516 (Davis), H.R. 836 (Smith), H.R. 958 (Rush), H.R. 1685 (Price), H.R. 2124 (Davis), and H.R. 4175 (Conyers).

This report discusses the core areas addressed in federal legislation. For related reports, see CRS Report RL34120, *Information Security and Data Breach Notification Safeguards*, by Gina Marie Stevens. Also see the Current Legislative Issues web page for "Privacy and Data Security" available at [http://apps.crs.gov/cli/cli.aspx?PRDS_CLI_ITEM_ID=2105]. This report will be updated as warranted.

Contents

Overview 1
Background 2
Data Security Legislation 4
- Laws Affected 4
- Scope of Coverage 4
- Data Privacy and Security Safeguards 5
- Data Breach Notification Requirements 6
- Restrictions on Social Security Numbers 6
- Credit Freezes 6
- Identity Theft 7
- Cause of Action 7
- Study and Evaluation 7
- Preemption 7
- Legislation 9

Data Security: Federal Legislative Approaches

Overview

Because concerns about possible identity theft resulting from data breaches are widespread,[1] Congress spent a considerable amount of time in the 109th Congress assessing data security practices and working on data breach legislation that would require companies to safeguard sensitive personal data and notify consumers about data security breaches.[2] According to the Federal Trade Commission (FTC), identity theft is the most common complaint from consumers in all 50 states.[3] In the FTC-sponsored ID-theft survey of U.S. adults, victims reported misuse of credit card and non-credit card accounts, and misuse of personal information to open new accounts or engage in other types of fraud. Victims of identity theft may incur damaged credit

---

[1] Federal Trade Commission, "2006 Identity Theft Survey Report," November 2007, at [http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf], "Consumer Fraud and Identity Theft Protection: January — December 2006," February 2007, at [http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf]; and 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].

[2] The 109th Congress passed The Veterans Benefits, Health Care, and Information Technology Act of 2006 (P.L. 109-461) to require the Department of Veterans Affairs (VA) to provide notice to veterans in case of breach of veterans' personal data, to perform a risk analysis if unauthorized access to sensitive personal information occurs, and for free credit monitoring services if a "reasonable risk" for misuses of personal information exists. In addition, the 109th Congress reported six other data security bills, none were enacted into law: S. 1326, S. 1408, and S. 1789 were reported either by the Senate Commerce or Judiciary committees; and H.R. 4127, H.R. 3997, and H.R. 5318 were reported either by the House Energy and Commerce, Financial Services, or Judiciary committees. The passage of such comprehensive data breach legislation in the 109th Congress was precluded by jurisdictional conflicts, along with unreconcilable approaches on credit freezes, exceptions for law enforcement and intelligence agencies, exemptions for financial institutions, notice requirements, notification triggers, enforcement authorities, and preemption. Congressional hearings were also held by the Commerce , Veterans' Affairs, Finance, Ways and Means, Judiciary, and House Government Reform committees on Securing Electronic Personal Data, Assessing Data Security, Securing Consumers' Data, the Veterans' Affairs Security Breach, Social Security Numbers; Security of Federal Computers, Identity Theft, and Privacy Laws and Data Brokerage Services.

[3] According to the FTC, for the seventh year in a row, identity theft tops the list of complaints consumers have filed with the agency, accounting for 36% of the 674,354 complaints received between January 1 and December 31, 2006. See note 1.

records, unauthorized charges on credit cards, and unauthorized withdrawals from bank accounts.

In the remainder of the 110th Congress, "The data-security legislative outlook is murky, with several conflicting bills pending in Congress, several committees involved, and little sign of imminent consensus."[4] Although, as noted, the occurrence of data breaches has been commonplace,[5] the solutions presented in the federal legislation to address the problems have varied. Common themes included the scope of coverage (who and what is covered); imposition of information security safeguards; breach notification requirements (when, how, triggers, frequency, and exceptions); customer access to and amendment of records; restrictions on the use of social security numbers; credit freezes on consumer reports; identity theft penalties; enforcement authorities and causes of action; and preemption.

Congress will continue to grapple with the problem of establishing a legal framework to prevent and respond to improper disclosures of personally identifiable information, including how to notify the public about such security breaches. For the 110th Congress, several high-tech companies have formed the Consumer Privacy Legislative Forum to promote a comprehensive data privacy bill to create a simplified, uniform legal framework that would set standards for what notice must be given to consumers about personal information collected on them and how it will be used, and preempt any existing state laws.[6]

Background

Federal legislative data security proposals were modeled after, in large part, state breach notification and data security laws. The imposition of data security breach notification obligations on entities that own, possess, or license sensitive personal information is a relatively new phenomenon. California was the first jurisdiction to enact a data breach notification law in 2002. There followed the emergence of numerous federal and state bills to impose notification requirements on entities that collect sensitive personal information.

S.B. 1386, the California Security Breach Notification Act, requires a state agency, or any person or business that owns or licenses computerized data that include personal information, to disclose any breach of security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. A "breach of the security of the system" is the "unauthorized acquisition of computerized data that

---

[4] "Murky Outlook Seen for Federal Data Breach Notification Legislation in 2008," 7 *BNA Privacy & Security Law* (Jan. 21, 2008). See also BNA chart that summarizes the status of key privacy and security legislation (e.g., data breach notification, credit freezes) pending in Congress, "Hill Watch," 6 *BNA Privacy & Security Law* 1879 (December 10, 2007).

[5] NACHA Internet Council, "*Chronological Data Breach List,"* (updated July 12, 2007), at [http://internetcouncil.nacha.org/docs/Chronological%20Data%20Breach%20List%20070712.pdf].

[6] "Technology Companies Form Coalition To Promote 'Robust' Federal Privacy Bill," 5 *BNA Privacy & Security Law* 893 (June 26, 2006).

compromises the security, confidentiality, or integrity of personal information maintained by the person or business." "Personal information" is defined as the first name or initial and last name of an individual, with one or more of the following: Social Security Number, driver's license number, credit card or debit card number, or a financial account number with information such as PIN numbers, passwords, or authorization codes that could gain access to the account. Exemptions are provided for encrypted information, for criminal investigations by law enforcement, and for breaches that are either immaterial or not "reasonably likely to subject the customers to unauthorized disclosure of personal information." California requires notice be given in the "most expedient time possible and without unreasonable delay," either in writing or by e-mail. If a company can show that the cost of notification will exceed $250,000, that more than 500,000 people are affected, or that the individual's contact information is unknown, then notice may be given through the media.

Numerous data security breaches were subsequently disclosed in response to California's law. In the absence of a comprehensive federal data breach notification law, many states enacted laws requiring consumer notice of security breaches of personal data.[7] The majority of states have introduced or passed bills to require companies to notify persons affected by breaches involving their personal information, and in some cases to implement information security programs to protect the security, confidentiality, and integrity of data.

Many states have enacted laws requiring notice of security breaches of personal data and consumer redress.[8] As of January 2008, 39 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.[9] The two predominant themes are consumer notification requirements in the event of a data breach and consumer redress. Most of the statutes cover both private entities and government agencies. Some statutes also impose obligations on third-party service providers to notify the owner or licensor of the data when a breach occurs. Many of the state laws follow the basic framework of the California breach notification law. The majority of state laws apply to electronic or

---

[7] See CRS Report RL34120, *Federal Information Security and Data Breach Notification Laws*, by Gina Marie Stevens; Julie Brill, Vermont Assistant Attorney General, *Chart on Comparison of State Security Breach Laws* (July 12, 2007).

[8] Since enactment of the state data breach notification laws, major data security breaches have been disclosed by several of the nation's largest information brokerage firms, retailers, universities, and federal and state government agencies. See generally CRS Report RL33199, *Data Security Breaches: Context and Incident Summaries*, by Rita Tehan (Table 1 summarizes selected data security breaches since 2000).

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

computerized data only. Notice provisions addressed by the states include description of triggering events, consideration of the level of harm or the risk of misuse that triggers notification, recipients of notification, timing of notice, method of notification, and content of notice. In addition, state laws may include exemptions for entities that are regulated under federal privacy laws (e.g., the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act); expanded definitions of "personal information"; notice requirements to consumer reporting agencies of customers affected by security breaches; civil penalties for failure to promptly notify customers of a security breach; requirements for the implementation of information security programs; creation of a private right of action to recover actual damages from businesses for failure to notify customers of a security breach in a timely manner; the right to place a credit freeze on a consumer credit report; restrictions on the sale and use of social security numbers; and enhanced criminal penalties for identity fraud.

Data Security Legislation

The following discussion highlights some of the various legislative approaches proposed in the 110th Congress, including existing laws affected by the bills; the scope of coverage (who and what information is covered); data privacy and security safeguards for sensitive personal information; requirements for security breach notification (when, how, triggers, frequency, and exceptions); restrictions on social security numbers (collection, use, and sale); credit freezes and fraud alerts on consumer reports; identity theft penalties; causes of action; and preemption (some of these bills preempt and sometimes limit recently enacted state laws).

Laws Affected. Some of the bills attempted to amend the Gramm-Leach-Bliley Act to require a financial institution to notify customers, consumer reporting agencies, and law enforcement agencies of a breach. Others would have amended the Fair Credit Reporting Act to prescribe data security standards, and others would amend the federal criminal code to prohibit intentionally accessing a computer without authorization, concealing security breaches involving personally identifiable information, and unlawfully accessing another's means of identification during a felony involving computers. Amendments to the Racketeer Influenced and Corrupt Organizations Act to cover fraud in connection with unauthorized access were also recommended, along with amendments by the U.S. Sentencing Commission to the sentencing guidelines regarding identity theft. Some of the bills are free-standing.

Scope of Coverage. Data brokers sell a wide array of personal information (real property, motor vehicle, health, employment, and demographic information), and are in many respects unregulated.[10] Generally, they are not subject to the requirements imposed on credit reporting agencies under the Fair Credit Reporting Act. The federal bills varied in their scope of covered entities: agencies or persons that own, license, or possess electronic personal data; any commercial entity or charitable, educational, or nonprofit organization that acquires, maintains, or uses

---

[10] See CRS Report RS22137, *Data Brokers: Background and Industry Overview*, by Gina Marie Stevens.

sensitive personal information; individual reference services providers, marketing list brokers, governmental entities, consumer reporting agencies, businesses sharing information with affiliates, entities with established business relationships with the data subject, news organizations, private investigators, and labor unions; any agency or person engaged in interstate commerce that owns or licenses electronic data containing personal information; a financial institution; or a consumer reporting agency, reporting broker, or reporting collector.

The federal bills included provisions that define protected information, regulating either personal information, sensitive financial identity information, sensitive financial account information, or sensitive personally identifiable information. Some bills established limitations on the sale or transfer of sensitive personal information.

Data Privacy and Security Safeguards. The federal bills required covered entities to take reasonable steps to protect against security breaches and to prevent unauthorized access to sensitive personal information that the entity sells, maintains, collects, or transfers. Some bills prescribe data security safeguards and guidelines for joint promulgation of security regulations. Others required the Federal Trade Commission (FTC) to promulgate regulations governing the conduct of information brokers. Many of the federal bills included provisions that would have imposed mandatory security requirements for sensitive personal information, required implementation of technical security safeguards and best practices, and mandated the development of security policies governing the processing and storage of personal data. Regulations in some cases were to include requirements for financial institutions to dispose of sensitive personal financial information. An Online Information Security Working Group to develop best practices was created in one of the bills.

Another theme that existed within some of the bills was application of fair information practices, similar to the Privacy Act (5 U.S.C. § 552a) and other privacy laws, such the Health Insurance Portability and Accountability Act (HIPAA), to information brokers not currently subject to similar protection to give individuals more control over the sharing of their personal information. Fair Information Practices typically include notice of information practices; informed consent/choice as to how personal information is used beyond the use for which the information was provided (e.g., giving the individual the opportunity to either opt-in or opt-out before personal data is sold); access to one's personal information, including a reasonable opportunity to review information and to correct inaccuracies or delete information; requirements for companies to take reasonable steps to protect the security of the information they collect from consumers; and the establishment of enforcement mechanisms to ensure compliance, including independent recourse mechanisms, systems to verify the privacy practices of businesses, and obligations to remedy implementation problems. Some of the federal bills incorporated fair information practices, such as access to and correction of personal information by the subject. Some bills adopted fair information practices and provided for individual access to information held by an information broker, accounting of disclosures, and amendment of errors.

Data Breach Notification Requirements. The federal bills established breach notification requirements, delineated triggers for consumer notice, and specified the level of risk of harm or injury that triggers notification. Provisions regarding the timeliness of notification, the methods and content of notice, and the duty to coordinate with consumer reporting agencies were generally included. Sometimes exceptions to notification requirements were permitted for national security and law enforcement purposes, with notice to Congress when exceptions are made. The purpose of a law enforcement exception to request a hold on notification is to gather additional information pending investigation. Some bills required notice to individuals if it is determined that the breach has resulted in or poses a reasonable risk of identity theft, or if the breach is reasonably likely to result in harm or substantial inconvenience to the consumer. Some amend Gramm-Leach-Bliley to require financial institutions to provide notice when a breach occurs to the consumer, to consumer reporting agencies, to a newly created FTC information clearinghouse, and to law enforcement agencies. In some cases, entities that maintain personal information for financial institutions are required to notify the institution when a breach has occurred. Some of the proposals provided an exemption from the notice requirement when the information was encrypted. In some of the bills, covered entities were required upon discovering a breach of security to report the breach to the FTC or other appropriate federal regulator and to notify consumer reporting agencies if the breach is determined to affect the sensitive personal information of 1,000 or more individuals.

Restrictions on Social Security Numbers. Recently, Congress has sought to further limit uses of the social security number, and is likely to continue to consider such measures in the 110th Congress, including proposals to remove social security numbers from Medicare cards, and limiting or prohibiting solicitation, display, sale, purchase, use, or access to social security numbers in the private sector.[11]

Credit Freezes. Thirty-eight states now have credit freeze laws.[12] Some bills would have permitted a consumer to place a credit or security freeze on his or her credit report in response to a security breach.[13] Others required consumer reporting agencies to maintain fraud alerts for consumers who have received notice of a breach of their data. A security freeze law allows a customer to block unauthorized third parties from obtaining his or her credit report or score. A consumer who places a security freeze on his or her credit report or score receives a personal identification number to gain access to credit information or to authorize the dissemination of credit information. Benefits of security freeze laws include increased consumer control over access to personal information and corresponding decreased

---

[11] See CRS Report RL30318, *The Social Security Number: Legal Developments Affecting Its Collection, Disclosure, and Confidentiality*, by Kathleen S. Swendiman.

[12] "New Credit Freeze, Breach Notice Laws Take Effect; Others May Join Ranks in 2008," *BNA Daily Report for Executives* (January 7, 2008);National Conference of State Legislators, "*Consumer Report Security Freeze Legislation 2007 Session,"* at [http://www.ncsl.org/programs/banking/SecurityFreeze_2007.htm].

[13] See CRS Report RS22484, *Identity Theft Laws: State Penalties and Remedies and Pending Federal Bills*, available upon request.

opportunities for imposters to obtain access to credit. Critics of security freeze laws argue that security freezes may cause consumers unwanted delays when they must provide third-party institutions access to credit histories for purposes such as qualifying for loans, applying for rental property leases, and obtaining mortgage rate approval.

Identity Theft.[14] Some bills established in the FTC an Office of Identity Theft to take civil enforcement actions. Some defined identity theft as the unauthorized assumption of another person's identity for the purpose of engaging in commercial transactions under that person's name; others defined it as the unauthorized acquisition, purchase, sale, or use by any person of a person's sensitive personal information that violates section 1028 of title 18 of the U.S. Code (fraud and related activity in connection with identification documents and information) or any provision of state law on the same subject or matter, or results in economic loss to the individual.

Cause of Action. Some of the bills expressly provided for enforcement by state attorneys general. The bills also treated violations as unfair or deceptive acts or practices under the FTC Act. In some of the bills, states were authorized to bring civil actions on behalf of residents and a private right of action was created for individuals injured by violations. Others provided a safe harbor for financial institutions that comply with the legislation. Some would require joint promulgation of regulations to shield consumer reporters from liability under state common law.

Study and Evaluation. The National Research Council would study securing personal information. The Comptroller General would study either social security number uses or federal agency use of data brokers or commercial databases containing personally identifiable information. The Administrator of the General Services Administration (GSA) would be required to evaluate contractor programs. For example, in considering contract awards totaling more than $500,000, GSA would be required to evaluate the data privacy and security program of a data broker, program compliance, the extent to which databases and systems have been compromised by security breaches, and data broker responses to such breaches. In some bills, the Secret Service would report to Congress on security breaches.

Preemption. The relationship of federal law to state data security laws, the question of federal preemption, was addressed in federal legislation. A variety of approaches was incorporated in the bills. With respect to other federal laws, such as the Fair Credit Reporting Act or the Gramm-Leach-Bliley Act, some would not preempt them. Others would have amended the Fair Credit Reporting Act to prevent states from imposing laws relating to the protection of consumer information, safeguarding of information, notification of data breaches, to misuse of information, and mitigation. Others would have amended Gramm-Leach-Bliley.

Some of the bills would have preempted state laws, some would preempt only inconsistent state laws, and some would have preempted state law except to the

---

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

extent that the state law provides greater protection for consumers. Others would preempt state laws relating to

- notification of data breaches;
- notification of data breaches (with the exception of California's law);
- information security programs and notifications of financial institutions;
- individual access to and correction of electronic records;
- liability for failure to notify an individual of a data breach or failure to maintain an information security program;
- requirements for consumer reporting agencies to comply with a consumer's request to prohibit release of the consumer's information;
- prohibitions on the solicitation or display of social security account numbers; and
- compliance with administrative, technical, and physical safeguards for sensitive personally identifying information.

Other bills would have created a national notification standard without preempting stronger state laws, and still others would not preempt state trespass, contract, or tort law or other state laws that relate to fraud.

Compliance concerns have been raised with the prospect that multiple laws requiring potentially different notification requirements will make compliance an overly complex and expensive task. Business groups and privacy advocates differ in their views of whether a federal data security law should allow stronger state laws. Industry groups and affected companies advocate a narrow notification standard that would preempt differing state laws.[15] Privacy advocates seek a uniform national notification standard without preempting stronger state laws.[16] The question of over-notification has been raised by industry participants. Business groups argue that the California breach notification law has prompted over-notification (companies notifying consumers of data security breaches when there is no risk of economic harm or fraud). A related question is whether breach notification should occur for all security breaches, or whether it should be limited to significant breaches. Some of the federal bills would have established a federal notice requirement when there has been a breach that raises significant risks to consumers. Federal legislation was also introduced to establish a federal floor for notification requirements that are not preemptive of state laws (an approach supported by the majority of state attorneys general). Business interests have pointed out that a federal floor approach will mean that, in practice, the law of the strictest state will become the de facto standard, and thus prefer clear federal preemption of state laws.

---

[15] "Industry Seeks One Law On Data Breach Alerts," *CQ Weekly* (February 6, 2006), at [http://www.cq.com/displayalertresult.do?matchId=18639833].

[16] "Panelists See Federal Preemption Of State Security, Breach Notice Laws as Key," 22 *Daily Report for Executives*," A-5 (November 16, 2005).

Legislation. Several bills have been introduced in the 110th Congress to combat identity theft, address security breaches, and protect personal information. During the First Session of the 110th Congress, three data security bills were reported favorably out of Senate committees — S. 239 (Feinstein), a bill to require federal agencies, and persons engaged in interstate commerce, in possession of data containing sensitive personally identifiable information, to disclose any breach of such information; S. 495 (Leahy), a bill to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information; and S. 1178 (Inouye), a bill to strengthen data protection and safeguards, require data breach notification, and further prevent identity theft. On June 3, H.R. 4791 (Clay), a bill to strengthen requirements for ensuring the effectiveness of information security controls over information resources that support federal operations and assets, was passed by the House by voice vote under suspension of the rules. Summaries of the bills provided below are from the Legislative Information System [http://www.congress.gov].

H.R. 516 (Davis)

Federal Agency Data Privacy Protection Act. This bill would establish requirements for the use of encryption for sensitive data maintained by the federal government; relating to access by agency personnel to sensitive data; and relating to government contractors and their employees involving sensitive data.

H.R. 836 (L. Smith)

Cyber-Security Enhancement and Consumer Data Protection Act of 2007. This bill would amend the federal criminal code to (1) prohibit accessing or remotely controlling a protected computer to obtain identification information; (2) revise the definition of "protected computer" to include computers affecting interstate or foreign commerce or communication; (3) expand the definition of racketeering to include computer fraud; (4) redefine the crime of computer-related extortion to include threats to access without authorization (or to exceed authorized access of) a protected computer; (5) impose criminal penalties for conspiracy to commit computer fraud; (6) impose a fine and/or five year prison term for failure to notify the U.S. Secret Service or Federal Bureau of Investigation (FBI) of a major security breach (involving a significant risk of identity theft) in a computer system, with the intent to thwart an investigation of such breach; (7) increase to 30 years the maximum term of imprisonment for computer fraud and require forfeiture of property used to commit computer fraud; and (8) impose criminal penalties for damaging 10 or more protected computers during any one-year period. The bill also directs the U.S. Sentencing Commission to review and amend its guidelines and policy statements to reflect congressional intent to increase criminal penalties for computer fraud and authorizes additional appropriations in FY2007-FY2011 to the U.S. Secret Service, the Department of Justice, and the FBI to investigate and prosecute criminal activity involving computers.

H.R. 958 (Rush)

Data Accountability and Trust Act. This bill would require the Federal Trade Commission (FTC) to promulgate regulations requiring each person engaged in interstate commerce that owns or possesses electronic data containing personal

information to establish security policies and procedures. The bill also authorizes the FTC to require a standard method or methods for destroying obsolete nonelectronic data. The bill also requires information brokers to submit their security policies to the FTC in conjunction with a security breach notification or on FTC request, requires the FTC to conduct or require an audit of security practices when information brokers are required to provide notification of such a breach, and authorizes additional audits after a breach. Additionally, the bill requires information brokers to (1) establish procedures to verify the accuracy of information that identifies individuals; (2) provide to individuals whose personal information they maintain a means to review it; (3) place notice on the Internet instructing individuals how to request access to such information; and (4) correct inaccurate information. Furthermore, the bill directs the FTC to require information brokers to establish measures which facilitate the auditing or retracing of access to, or transmissions of, electronic data containing personal information and prohibits information brokers from obtaining or disclosing personal information by false pretenses (pretexting). Additionally, the bill prescribes procedures for notification to the FTC and affected individuals of information security breaches. The bill also sets forth special notification requirements for breaches (1) by contractors who maintain or process electronic data containing personal information; (2) involving telecommunications and computer services; and (3) of health information. H.R. 958 preempts state information security laws.

H.R. 1685 (T. Price)

Data Security Act of 2007. This bill would prescribe security procedures which an entity that maintains or communicates sensitive account or personal information must implement and enforce in order to protect the information from an unauthorized use likely to result in substantial harm or inconvenience to the consumer. The bill also grants exclusive enforcement powers to specified federal regulatory agencies with oversight of financial institutions. The bill also denies a private right of action, including a class action, regarding any act or practice regulated under this act. The bill also prohibits any civil or criminal action in state court or under state law relating to any act or practice governed under this act. The bill prescribes data security standards to be implemented by federal agencies. The bill also expresses the sense of the Congress that federal regulators shall make every effort to reconcile differences between this act and specified requirements of the Gramm-Leach-Bliley Act. The bill provides that a notice provided to any consumer under this act may be the basis for a request by the consumer for an initial fraud alert under the Fair Credit Reporting Act. H.R. 1685 preempts state law with respect to the responsibilities of any person to protect against and investigate such data security breaches and mitigate any losses or harm resulting from them.

H.R. 2124 (T. Davis)

Federal Agency Data Breach Protection Act. The bill would amend federal law governing public printing and documents to instruct the Director of the Office of Management and Budget (OMB) to establish policies, procedures, and standards for agencies to follow in the event of a breach of data security involving disclosure of sensitive personal information for which harm to an individual could reasonably be expected to result. The bill would also require such policies and procedures to include (1) timely notification to individuals whose sensitive personal information could be compromised as a result of a breach; (2) guidance on determining how to

provide timely notice; and (3) guidance regarding whether additional special actions are necessary and appropriate, including data breach analysis, fraud resolution services, identity theft insurance, and credit protection or monitoring services. The bill would also authorizes each agency Chief Information Officer to: (1) enforce data breach policies; and (2) develop an inventory of all personal computers, laptops, or any other hardware containing sensitive personal information. The bill would require federal agency information security programs to include data breach notification procedures to alert individuals whose sensitive personal information is compromised. H.R. 2124 would make it the duty of each agency Chief Human Capital Officer to prescribe policies and procedures for employee exit interviews, including a full accounting of all federal personal property assigned to the employee during the course of employment.

H.R. 4175 (Conyers)

Privacy and Cybercrime Enforcement Act of 2007. This bill would amend the federal criminal code provisions relating to computer fraud and unauthorized access to computers to (1) include computer fraud within the definition of racketeering activity; (2) provide criminal penalties for intentional failures to provide required notices of a security breach involving sensitive personally identifiable information; (3) expand penalties for conspiracies to commit computer fraud and extortion attempts involving threats to access computers without authorization; (4) provide for forfeiture of property used to commit computer fraud; and (5) require restitution for victims of identity theft and computer fraud. The bill would also authorize additional appropriations for investigating and prosecuting criminal activity involving computers. H.R. 4175 would require the U.S. Sentencing Commission to review and amend, if appropriate, its sentencing guidelines and policies related to identity theft and computer fraud offenses. The bill authorizes the Attorney General and state attorneys general to bring civil actions and obtain injunctive relief for violations of federal laws relating to data security. H.R. 4175 would require federal agencies as part of their rulemaking process to prepare and make available to the public privacy impact assessments that describe the impact of proposed agency rules on the privacy of individuals. The bill would also authorize the Office of Justice Programs of the Department of Justice (DOJ) to award grants to states for programs to increase enforcement efforts involving fraudulent, unauthorized, or other criminal use of personally identifiable information. In addition, the bill would also authorize the Director of the Bureau of Justice Assistance to make grants to improve the identification, investigation, and prosecution of criminal or terrorist conspiracies or activities that span jurisdictional boundaries, including terrorism, economic crime, and high-tech crime.

H.R. 4791 (Clay)

Federal Agency Data Protection Act. Defines "personally identifiable information" as any information about an individual maintained by a federal agency, including information about the individual's education, finances, medical, criminal, or employment history, that can be used to distinguish or trace such individual's identity or that is linked or linkable to the individual. Defines "mobile digital device" as any device that can store or process information electronically and is designed to be used in a manner not limited to a fixed location. Includes the following within the information security duties of the Director of the Office of Management and Budget (OMB): (1) the establishment of minimum requirements

for the protection of personally identifiable information maintained in or transmitted by mobile digital devices, including requirements for the use of technologies that render information unusable by unauthorized persons; (2) the establishment of minimum requirements for agency actions following a breach of information security; (3) notification of individuals whose personally identifiable information may have been compromised or accessed during a security breach; (4) reporting of information security breaches involving personally identifiable information that may have been compromised or accessed during a security breach to the Federal Information Security Incident Center; (5) requiring agencies to comply with minimally acceptable system configuration requirements; (6) requiring agency contractors to meet minimally acceptable system configuration requirements; and (7) ensuring compliance with information security requirements for information and information systems used or operated by a contractor of an agency or subcontractor.

Requires federal agencies to (1) adopt plans and procedures for ensuring the adequacy of information security protections for systems maintaining or transmitting personally identifiable information; (2) follow policies, procedures, and standards in the event of a data security breach involving the disclosure of personally identifiable information; (3) maintain an inventory of all personal computers, laptops, or other hardware containing personally identifiable information; (4) implement policies for employee exit interview to account for all federal personal property assigned to the employee; (5) develop and implement a plan to protect the security and privacy of federal government information collected or maintained by or on behalf of the agency from the risks posed by peer-to-peer file sharing; and (6) undergo annual independent audits (currently, evaluations are required) in conformity with generally accepted government accounting standards of their information programs and practices (such audits would also include the information systems used, operated, or supported on behalf of the agency by a contractor of the agency, any subcontractor, or any other entity).

Amends the E-Government Act of 2002 to require the development of best practices for agencies to follow in conducting privacy impact assessments. The House Committee on Oversight and Government reported the bill, as amended, with H.Rept. 110-664 on May 21, 2008. On June 3, 2008, H.R. 4791 was passed by the House by voice vote under suspension of the rules.

S. 239 (Feinstein)

Notification of Risk to Personal Data Act of 2007. This bill would require any federal agency or business entity engaged in interstate commerce that uses, accesses, transmits, stores, disposes of, or collects sensitive, personally identifiable information, following the discovery of a security breach, to notify (as specified): (1) any U.S. resident whose information may have been accessed or acquired; and (2) the owner or licensee of any such information the agency or business does not own or license. Additionally, the bill exempts (1) agencies from notification requirements for national security and law enforcement purposes and for security breaches that do not have a significant risk of resulting in harm, provided specified certification or notice is given to the U.S. Secret Service; and (2) business entities from notification requirements if the entity utilizes a security program that blocks unauthorized financial transactions and provides notice of a breach to affected individuals. The bill also requires notifications regarding security breaches under specified

circumstances to the Secret Service, the Federal Bureau of Investigation, the United States Postal Inspection Service, and state attorneys general. Furthermore, the bill sets forth enforcement provisions and authorizes appropriations for costs incurred by the Secret Service to investigate and conduct risk assessments of security breaches. The Senate Committee on the Judiciary reported the bill without a written report on May 31, 2007.

S. 495 (Leahy)

Personal Data Privacy and Security Act of 2007. This bill would amend the federal criminal code to (1) make fraud in connection with the unauthorized access of sensitive personally identifiable information (in electronic or digital form) a predicate for racketeering charges; and (2) prohibit concealment of security breaches involving such information. The bill also directs the U.S. Sentencing Commission to review and amend its guidelines relating to fraudulent access to, or misuse of, digitized or electronic personally identifiable information (including identify theft). Additionally, the bill requires a data broker to (1) disclose to an individual, upon request, personal electronic records pertaining to such individual maintained for disclosure to third parties; and (2) maintain procedures for correcting the accuracy of such records. The bill also establishes standards for developing and implementing safeguards to protect the security of sensitive personally identifiable information. Additionally, the bill imposes upon business entities civil penalties for violations of such standards and requires such business entities to notify (1) any individual whose information has been accessed or acquired; and (2) the U.S. Secret Service if the number of individuals involved exceeds 10,000. Furthermore, the bill authorizes the Attorney General and state attorneys general to bring civil actions against business entities for violations of this act. The bill requires the Administrator of the General Services Administration in considering contract awards totaling more than $500,000, to evaluate (1) the data privacy and security program of a data broker; (2) program compliance; (3) the extent to which databases and systems have been compromised by security breaches; and (4) data broker responses to such breaches. The bill also requires federal agencies to conduct a privacy impact assessment before purchasing personally identifiable information from a data broker. The Senate Committee on the Judiciary reported the bill with written report 110-70 on May 23, 3007.

S. 1178 (Inouye)

Identity Theft Prevention Act. This bill would require any commercial entity or charitable, educational, or nonprofit organization that acquires, maintains, or uses sensitive personal information (covered entity) to develop, implement, maintain, and enforce a written program, containing administrative, technical, and physical safeguards, for the security of sensitive personal information it collects, maintains, sells, transfers, or disposes of. The bill defines "sensitive personal information" as an individual's name, address, or telephone number combined with at least one of the following relating to that individual: (1) the social security number or numbers derived from that number; (2) financial account or credit or debit card numbers combined with codes or passwords that permit account access, subject to exception; or (3) a state driver's license or resident identification number. The proposed act requires a covered entity (1) to report a security breach to the Federal Trade Commission (FTC); (2) if the entity determines that the breach creates a reasonable risk of identity theft, to notify each affected individual; and (3) if the breach involves at least 1,000 individuals, to notify all consumer reporting agencies specified in the

Fair Credit Reporting Act. The bill also authorizes a consumer to place a security freeze on his or her credit report by making a request to a consumer credit reporting agency, and prohibits a reporting agency, when a freeze is in effect, from releasing the consumer's report for credit review purposes without the consumer's prior express authorization. Additionally, this legislation requires (1) the establishment of the Information Security and Consumer Privacy Advisory Committee; and (2) a related crime study, including the correlation between methamphetamine use and identity theft crimes. Also, this bill treats any violation of this act as an unfair or deceptive act or practice under the Federal Trade Commission Act, requires enforcement under other specified laws, allows enforcement by state attorneys general, and preempts state laws requiring notification of affected individuals of security breaches. The Senate Committee on Commerce, Science and Transportation reported the bill with written report 110-235 on December 5, 2007.

S. 1202 (Sessions)

Personal Data Protection Act of 2007. This bill would require agencies and individuals who possess computerized data containing sensitive personal information to disclose security breaches that pose a significant risk of identity theft.

S. 1260 (Carper)

Data Security Act of 2007. The bill would prescribe security procedures which an entity that maintains or communicates sensitive account or personal information must implement and enforce in order to protect the information from an unauthorized use likely to result in substantial harm or inconvenience to the consumer. The bill would also grant exclusive enforcement powers to specified federal regulatory agencies with oversight of financial institutions. The bill also denies a private right of action, including a class action, regarding any act or practice regulated under this act. The bill would also prohibit any civil or criminal action in state court or under state law relating to any act or practice governed under this act.

The bill would prescribe data security standards to be implemented by federal agencies. S. 1260 preempts state law with respect to the responsibilities of any person to protect against and investigate such data security breaches and mitigate any losses or harm resulting from them.

S. 1558 (Coleman)

Federal Agency Data Breach Protection Act. The bill would amend federal law governing public printing and documents to instruct the Director of the Office of Management and Budget (OMB) to establish policies, procedures, and standards for agencies to follow in the event of a breach of data security involving disclosure of sensitive personal information for which harm to an individual could reasonably be expected to result. The bill would require such policies and procedures to include (1) timely notification to individuals whose sensitive personal information could be compromised as a result of a breach; (2) guidance on determining how to provide timely notice; and (3) guidance regarding whether additional special actions are necessary and appropriate, including data breach analysis, fraud resolution services, identity theft insurance, and credit protection or monitoring services. The bill also authorizes each agency Chief Information Officer to: (1) enforce data breach policies; and (2) develop an inventory of all personal computers, laptops, or any other hardware containing sensitive personal information. The bill would also require

federal agency information security programs to include data breach notification procedures to alert individuals whose sensitive personal information is compromised. S. 1558 makes it the duty of each agency Chief Human Capital Officer to prescribe policies and procedures for employee exit interviews, including a full accounting of all federal personal property assigned to the employee during the course of employment.