Order Code RL33273

CRS Report for Congress
Received through the CRS Web

Data Security: Federal Legislative Approaches

February 9, 2006

Gina Marie Stevens
Legislative Attorney
American Law Division

Data Security: Federal Legislative Approaches

Summary

Numerous data security bills were introduced in the first session of the 109th Congress to address data security breaches; some of these bills preempt and sometimes limit recently enacted state laws. Three congressional hearings were held in 2005 to examine issues related to data breaches. Three bills were reported by Senate committees during the first session of the 109th Congress. The prospect for continued congressional attention is high during the second session of the 109th Congress, with eight congressional committees having jurisdiction over some aspect of data security, data breach notification, and data privacy. This report discusses the core areas addressed in federal legislation, including the scope of coverage (who is covered 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 on consumer reports; identity theft penalties; causes of action; and preemption. For related reports, see CRS Report RS22374, *Data Security: Federal and State Laws*, by Gina Marie Stevens; CRS Report RL33005, *Information Brokers: Federal and State Laws*, by Angie A. Welborn; CRS Report RS20185, *Privacy Protection for Customer Financial Information*, by M. Maureen Murphy; and CRS Report RL31408, *Internet Privacy: Overview and Pending Legislation*, by Marcia S. Smith. This report will be updated as warranted.

Contents

Data Security: Federal Legislative Approaches

Overview

Numerous data security bills were introduced in the first session of the 109th Congress to address data security breaches, some of which would preempt or limit recently enacted state laws. Three bills were reported by Senate committees during the first session of the 109th Congress (S. 1326, S. 1408, S. 1789), with a written report issued for S. 1408.[1] The prospect for continued congressional attention is high during the second session of the 109th Congress, with eight congressional committees having jurisdiction over some aspect of data security, data breach notification, and data privacy (House Energy and Commerce; House Financial Services; House Government Reform; House Judiciary; House Ways and Means; Senate Commerce, Science, and Transportation; Senate Banking, Housing, and Urban Affairs; and Senate Judiciary). Three congressional hearings were held in 2005 to examine issues related to data breaches.[2] Given the large number of bills introduced in the first session of the 109th Congress, similarities and differences will exist.[3] Although, as noted, the occurrence of data breaches has been commonplace, the solutions presented in federal legislation to address the problems vary. The following discussion highlights some of the approaches developed in selected bills. In general, core areas addressed in the bills include scope of coverage (who is covered and what information is covered); data privacy and security safeguards for sensitive personal information; security breach notification requirements (when, how, triggers, frequency, and exceptions); restrictions on social security numbers (collection, use, and sale); credit freezes on consumer reports; identity theft penalties; causes of action; and preemption.

Some of the bills amend the Gramm-Leach-Bliley Act to require a financial institution to notify customers, consumer reporting agencies, and law enforcement

---

[1] *Identity Theft Protection Act: Report of the Committee on Commerce, Science, and Transportation on S. 1408*, S. Rep. No. 109-203 (2005).

[2] *Securing Electronic Personal Data: Striking A Balance Between Privacy and Commercial and Governmental Use: Hearing Before the Senate Comm. on the Judiciary*, 109th Cong., 1st Sess. (2005); *Assessing Data Security: Preventing Breaches and Protecting Sensitive Information; Hearing Before the House Comm. on Financial Services*, 109th Cong., 1st Sess. (2005); *Securing Consumers' Data: Options Following Security Breaches; Hearing Before the Subcomm. On Commerce, Trade, and Consumer Protection of the Senate Comm. on Energy and Commerce*, 109th Cong., 1st Sess. (2005).

[3] See American Bankers Association, Data Breach Legislation (Dec. 2, 2005), available at [http://internetcouncil.nacha.org/docs/Data%20Breach%20Legislation%20Chart%20December%202%202005%20Data%20update.pdf].

agencies of a breach. Others would amend 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 are 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. The federal bills vary in their definitions 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 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 include provisions that define protected information, regulating either personal information, sensitive financial identity information, sensitive financial account information, or sensitive personally identifiable information. Some bills establish limitations on the sale or transfer of sensitive personal information.

Data Privacy and Security Safeguards. The federal bills require 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 require the Federal Trade Commission (FTC) to promulgate regulations governing the conduct of information brokers. Many of the federal bills include provisions that would impose mandatory security requirements for sensitive personal information, require implementation of technical security safeguards and best practices, and mandate the development of security policies governing the processing and storage of personal data. Regulations in some cases are to include requirements for financial institutions to dispose of sensitive personal financial information. An Online Information Security Working Group to develop best practices is created in one of the bills.

Another theme that exists in some of the bills is 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 incorporate fair information practices, such as access to and correction of personal information by the subject. Some bills adopt fair information practices and provide for individual access to information held by an information broker, accounting of disclosures, and amendment of errors.

Security Breach Notification Requirements. The federal bills establish breach notification requirements, delineate triggers for consumer notice, and specify 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 are generally included. Sometimes exceptions to notification requirements are 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 require 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 provide an exemption from the notice requirement when the information was encrypted. In some of the bills, covered entities are 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. Several of the bills specify prohibitions on the solicitation, display, sale, purchase, use of, and access to social security numbers.

Credit Freezes. Some bills permit a consumer to place a security freeze on his or her credit report in response to a security breach. Others require consumer reporting agencies to maintain fraud alerts for consumers who have received notice of a breach of their data.

Identity Theft. Other bills establish in the FTC an Office of Identity Theft to take civil enforcement actions. Some define identity theft as the unauthorized assumption of another person's identity for the purpose of engaging in commercial transactions under that person's name; or 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 provide for enforcement by state attorneys general. The bills also treat violations as unfair or deceptive acts or practices under the FTC Act. In some of the bills, states are authorized to bring civil actions on behalf of residents and a private right of action is created for individuals injured by violations. Others provide 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 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, is addressed in federal legislation.[4] A variety of approaches are 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 amend 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 amend Gramm-Leach-Bliley.

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

---

[4] For a discussion of the law regarding preemption, see CRS Report RL32197, *Preemption of State Law for National Banks and Their Subsidiaries by the Office of the Comptroller of the Currency*, by Maureen Murphy, March 4, 2004. ("The starting point for preemption analysis is the language of the federal legislation. If Congress enacts legislation under one of its delegated powers that includes an explicit statement that state law is preempted, the Supreme Court generally will give effect to that legislative intent. Where there is no language of preemption, the Court is likely to find preemption when it identifies a direct conflict between the federal law and the state law or when it concludes that the federal government has so occupied the field as to preclude enforcement of state law with respect to the subject at hand.")[Citations omitted.]

- 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 create 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.[5] Privacy advocates seek a uniform national notification standard without preempting stronger state laws.[6] 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 establish a federal notice requirement when there has been a breach that raises significant risks to consumers. Federal legislation has also been introduced to establish a federal floor for notification requirements that are not preemptive of state laws (this approach is supported by the majority of state attorney generals). 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. The preemption provisions in each of the selected bills is included in the following summaries at the end of each bill.

Summary of Selected Federal Data Security Legislation

S. 115, Notification of Risk to Personal Data Act (Feinstein). The bill requires any agency or person that owns or licenses electronic data containing personal information, following the discovery of a breach of security of the system containing such data, to notify any U.S. resident whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. It also requires any agency or person who possesses but does not own or license such data to notify the information owner or licensee about unauthorized acquisition. The bill

---

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

[6] "Panelists See Federal Preemption Of State Security, Breach Notice Laws as Key," 2220 *Daily Report for Executives*," A-5 (November 16, 2005).

allows delayed notification for authorized law enforcement purposes. It provides authorized methods of notification and alternative notification procedures. Civil penalties and rights and remedies are provided in connection with violations. Enforcement by state attorneys general is instituted.

The bill supersedes any inconsistent provisions of state or local law relating to the notification of any U.S. resident of any breach of security of an electronic database containing such resident's personal information, except as provided under sections 1798.82 (notification of breach of the security of the system) and 1798.29 (agencies owning, licensing, or maintaining computerized data, including personal information; disclosure of security breach; notice requirements) of the California Civil Code. (Sec. 5.)

S. 500/H.R. 1080, Information Protection and Security Act (Nelson), directs the FTC to promulgate regulations governing the conduct of information brokers and the protection of personally identifiable information held by such brokers. The bill requires regulations establishing procedures for data accuracy, confidentiality, user authentication and tracking, prevention and detection of illegal or unauthorized activity, and mitigation of potential harm to individuals. The bill also requires that the regulations issued by the FTC allow individuals to obtain disclosure of information pertaining to them held by an information broker, to be informed of each entity that procured such information, and to request and receive prompt correction of errors. The regulations also must prohibit brokers from engaging in activity that fails to comply with FTC regulations. The bill would treat violations of the regulations as unfair or deceptive acts or practices under the Federal Trade Commission Act. States are authorized, after providing notice to the FTC and the Attorney General, to bring civil actions on behalf of residents in federal district court or any other court of competent jurisdiction to enjoin such acts or practices; enforce compliance with FTC regulations; or obtain damages, restitution, compensation, or other appropriate relief. A private right of action is created for individuals injured by violations of the regulations issued pursuant to the bill.

The bill would not modify, limit, or supersede the operation of the Fair Credit Reporting Act. To the extent that there is any conflict, whichever law provides greater protection governs. Multiple requirements with respect to the same information, transaction, or individual would not be considered a conflict. (Sec. 5(a)).

The bill would not supersede, alter, or affect any state statute, regulation, order, or interpretation, except to the extent that such state law is inconsistent, and then only to the extent of the inconsistency. A state law would not be considered inconsistent if it affords greater protection. (Sec. 5(b).)

S. 751, Notification of Risk to Personal Data Act (Feinstein), requires any federal agency or person that owns, licenses, or collects personal information data following the discovery of a breach of its personal data security system, or upon receiving notice of a system breach, to notify (as specified) the individual whose information was obtained by an unauthorized person. Any agency or person possessing, but not owning or licensing such data, is required to notify the information owner or licensee of an unauthorized acquisition. Agencies are excepted from notification requirements for national security and law enforcement purposes,

with immediate notification to Congress of such exceptions. Enforcement provisions are included.

The bill supersedes any inconsistent provisions of state or local law with respect to the conduct required by S. 751. (Sec. 5.)

S. 768, Comprehensive Identity Theft Prevention Act (Schumer), establishes in the Federal Trade Commission (FTC) an Office of Identity Theft and authorizes the Office to take civil enforcement actions against persons who violate this bill. The bill sets limits on the sale or transfer of sensitive personal information. It requires data merchants to register. It establishes an international directorate to coordinate international responses to identify theft and develop best practices. The bill sets forth notification requirements regarding the unauthorized acquisition of, or the intention to share, an individual's sensitive personal information and penalties for violations. It specifies prohibitions on the solicitation, display, sale, purchase, or use of and access to social security numbers. The Chairman of the FTC is directed to establish an Online Information Security Working Group.

The bill would not supersede, alter, or affect any state statute, regulation, order, or interpretation, except to the extent that such state law is inconsistent with it, and then only to the extent of the inconsistency. A state statute, regulation, order, or interpretation is not inconsistent if it affords any U.S. resident greater protection than S. 768. (Sec. 16.)

S. 1216, Financial Privacy Breach Notification Act of 2005 (Corzine), amends the Gramm-Leach-Bliley Act to require a financial institution to promptly notify each customer affected by a breach, certain consumer reporting agencies, and appropriate law enforcement agencies whenever a breach of personal information has occurred. Any person who maintains personal information for or on behalf of a financial institution is required to promptly notify the institution of any case in which such customer information has been breached. The bill prescribes notification procedures. It authorizes a customer injured by a violation to institute a civil action to recover damages. The FTC is authorized to enforce compliance and to assess fines for violations.

S. 1326, Notification of Risk to Personal Data Act (Sessions) (reported by Senate Judiciary Committee), requires any agency or person that owns or licenses computerized data containing sensitive personal information to implement and maintain reasonable security and notification procedures and practices to protect sensitive personal information from unauthorized access, destruction, use, modification, or disclosure; and to notify any individual whose sensitive personal information was compromised. The bill permits a federal law enforcement agency to delay notification if it would impede a criminal or civil investigation. It also requires any agency or person in possession of computerized data containing sensitive personal information that it does not own or license to notify the entity from whom it received the information if the security of that information was compromised, resulting in a significant risk of identity theft. The bill sets forth provisions regarding the timeliness of notification, the methods and content of notice, and the duty to coordinate with consumer reporting agencies. It establishes civil

remedies for failure to provide notice of a security breach and authorizes enforcement by state attorneys general on behalf of state residents.

The bill supersedes any state or local law, rule, or regulation related to electronic information security standards or notification of any U.S. resident of a breach of security of personal information about such resident. (Sec. 5.)

S. 1332, Personal Data Privacy and Security Act of 2005 (Specter), amends 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. The bill amends the Racketeer Influenced and Corrupt Organizations Act to cover fraud in connection with such unauthorized access. It directs the U.S. Sentencing Commission to amend the sentencing guidelines regarding identity theft. Data brokers would be required to disclose to an individual, upon request, personal electronic records pertaining to such individual and to publish procedures for responding to inaccuracies. The bill establishes safeguards to protect the privacy and security of personal information, including notice of security breaches, and offers to cover specified costs. It requires the Department of Justice to contract with the National Research Council to study securing personal information; it requires the Comptroller General to study social security number uses and federal use of commercial databases; and the Administrator of the General Services Administration to evaluate contractor programs. The bill prohibits without consent the display of an individual's social security number to a third party and the sale or purchase of such number. It amends the Social Security Act to restrict social security number use by businesses and the government. It includes remedies for violations.

It provides that no state law requirement or prohibition may be imposed with respect to individual access to, and correction of, personal electronic records. Except as provided above, it would not annul, alter, affect, or exempt data brokers from complying with state laws with respect to access, use, compilation, distribution, processing, analysis, and evaluation of personally identifiable information by data brokers, except to the extent that those laws are inconsistent, and then only to the extent of such inconsistency. (Sec. 303.)

It provides that no requirement or prohibition may be imposed under state law with respect to financial institutions subject to the data security requirements and regulations of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) and to compliance examinations as required by S. 1332; nor with respect to "covered entities" subject to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.), including its data security requirements and regulations. Except as provided above, it would not annul, alter, affect, or exempt any person from complying with state law with respect to security programs for personally identifiable information, except to the extent that those laws are inconsistent, and then only to the extent of such inconsistency. (Sec. 404.)

It provides that no requirement or prohibition may be imposed under state law with respect to prerequisites for consent for the display, sale, or purchase of social security numbers; relating to harvesting of social security numbers; and relating to

treatment of social security numbers on government checks and prohibition of inmate access. Except as provided above, it would not annul, alter, affect, or exempt any person from complying with state law with respect to protecting and securing social security numbers, except to the extent that those laws are inconsistent, and then only to the extent of such inconsistency. (Sec. 507.)

S. 1408, Identity Theft Protection Act (Smith) (reported by the Senate Commerce, Science, and Transportation Committee (Senate Reports109-203), requires any commercial entity or charitable, educational, or nonprofit organization that acquires, maintains, or uses sensitive personal information 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, and it requires the FTC to promulgate regulations. The bill requires a covered entity, upon discovering a breach of security, to report the breach to the FTC or other appropriate federal regulator and to notify all consumer reporting agencies specified in the Fair Credit Reporting Act if it determines that the breach affects the sensitive personal information of 1,000 or more individuals; and to notify individuals if the breach has resulted in, or poses a reasonable risk of, identity theft. It authorizes the placement of a security freeze on a consumer credit report. It directs that violations be treated as unfair or deceptive acts or practices and sets civil penalties for violations. The bill places limits on the use of, and access to, social security numbers. It also directs the chairman of the FTC to establish an Information Security Working Group.

The bill preempts any state or local law, regulation, or rule that requires a covered entity to develop, implement, maintain, or enforce information security programs; or to notify individuals of breaches of security pertaining to them.

The bill preempts any state or local law, regulation, rule, administrative procedure, or judicial precedent under which liability is imposed on a covered entity for failure to implement and maintain an adequate information security program; or to notify an individual of any breach of security pertaining to any sensitive personal information about that individual.

The bill preempts any state or local law, regulation, or rule that requires consumer reporting agencies to comply with a consumer's request to place, remove, or temporarily suspend a prohibition on the release by a consumer reporting agency of information on that consumer.

The bill preempts any state or local law, regulation, or rule prohibiting or limiting the solicitation or display of Social Security account numbers.

Federal preemption would only apply to information security programs, notification requirements, liability, security freezes, and social security numbers, and would have no effect on other state or local jurisdiction over covered entities. (Sec. 7.)

S. 1594, Financial Privacy Protection Act of 2005 (Corzine), amends the Gramm-Leach-Bliley Act to require each financial institution to develop and maintain a security system designed to prevent any breach of its customer

information. The bill prescribes guidelines for federal regulations governing a customer information security system and for financial institutions to notify customers of unauthorized access to customer information. It provides for damages by a customer adversely affected by a violation of this Act, for injunctions against a financial institution in violation of this Act, and for civil enforcement actions by state attorneys general. It amends the Fair Credit Reporting Act to require a consumer reporting agency to trigger a fraud alert in a consumer file upon notification of a data security breach and to prohibit the user of a consumer report to take any adverse action with respect to a consumer based on the fraud alert (extended alert).

S. 1789, Personal Data Privacy and Security Act of 2005 (Specter) (reported by the Senate Judiciary Committee), amends the federal criminal code to prohibit intentionally accessing a computer without authorization and obtaining data broker information, concealing security breaches involving sensitive personally identifiable information, and unlawfully accessing another person's means of identification during a felony involving computers. The bill amends the Racketeer Influenced and Corrupt Organizations Act to cover fraud in connection with such unauthorized access. It directs the U.S. Sentencing Commission to amend the sentencing guidelines regarding identity theft. The bill requires data brokers to disclose to an individual personal electronic records pertaining to such individual and to publish procedures for responding to inaccuracies. It establishes safeguards to protect the privacy and security of personal information and requires notice of security breaches. It requires the Administrator of the General Services Administration (GSA), in considering contract awards totaling more than $500,000, to evaluate the data privacy and security program of a data broker, the extent to which its databases and systems have been compromised by security breaches, and data broker responses to such breaches. The bill directs the Secret Service to report to Congress on security breaches and directs the Comptroller General to report on federal agency use of data brokers or commercial databases containing personally identifiable information. It sets remedies for violations of this Act.

It prohibits states from imposing any requirements relating to individual access to, and correction of, personal electronic records held by data brokers. (Sec. 204 of title II — Data Brokers.)

It prohibits states from requiring any business entity to comply with any requirements relating to administrative, technical, and physical safeguards for the protection of sensitive personally identifying information. It would not modify, limit, or supersede the operation of the Gramm-Leach-Bliley Act or its regulations, including those adopted or enforced by states. (Sec. 304 of subtitle A of title III — Data Privacy and Security Programs.)

It supersedes federal law or state law relating to notification of a security breach, except that a state may require that a notice also include information regarding victim protection assistance provided by that state. It would not preclude any operation permitted under section 507 (relation to state laws) of the Gramm-Leach-Bliley Act (15 U.S.C. 6807). (Sec. 329 of subtitle B of title III — Security Breach Notification.)

H.R. 1069, Notification of Risk to Personal Data Act (Bean), prescribes notification procedures governing any agency, or person engaged in interstate commerce, that owns or licenses electronic data containing personal information, following the discovery of a breach of security of the system containing such data. The bill amends the Gramm-Leach-Bliley Act to require a financial institution at which a breach of personal information is reasonably believed to have occurred to promptly notify (1) each affected customer, (2) each pertinent consumer reporting agency, (3) the information clearinghouse established by the FTC under this Act, and (4) appropriate law enforcement agencies in any case in which the financial institution has reason to believe that the breach or suspected breach affects a large number of customers. It requires any person who maintains personal information for or on behalf of a financial institution to notify promptly the financial institution of any case in which such customer information has been, or is reasonably believed to have been, breached. It amends the Fair Credit Reporting Act to require a consumer reporting agency to maintain a fraud alert file with respect to any consumer upon receiving notice of a breach of personal information from (1) an agency or person engaged in interstate commerce pursuant to this Act or (2) a financial institution subject to the Gramm-Leach-Bliley Act. It also authorizes state attorneys general to bring civil actions in federal district court to enforce this Act on behalf of the residents of the state, and directs the FTC to establish and maintain a clearinghouse to collect and analyze information required under this Act.

The bill supersedes inconsistent provisions of state or local law relating to the notification of any U.S. resident of any breach of security of an electronic database containing such resident's personal information, except as provided under sections 1798.82 (notification of breach of the security of the system) and 1798.29 (agencies owning, licensing, or maintaining, computerized data including personal information; disclosure of security breach; notice requirements) of the California Civil Code. (Sec. 8.)

H.R. 1080, Information Protection and Security Act (Markey), see **S. 500.**

H.R. 3140, Consumer Data Security and Notification Act of 2005 (Bean), amends the Fair Credit Reporting Act (FCRA) to cover communication of personally identifiable information by unregulated information brokers who, for compensation, regularly assemble or evaluate personally identifiable information for the purpose of furnishing reports to third parties. The bill imposes an affirmative obligation upon each consumer reporting agency to respect the privacy of consumers and to protect the security and confidentiality of their nonpublic personal information. It instructs the FTC to promulgate safeguards for the protection of nonpublic consumer information and amends the Gramm-Leach-Bliley Act to direct federal oversight agencies to include notification requirements within the regulations governing financial institutions.

H.R. 3374, Consumer Notification and Financial Data Protection Act of 2005 (LaTourette), declares that each financial institution has an obligation to maintain reasonable policies and procedures to protect the security and confidentiality of a consumer's sensitive financial personal information against any unauthorized use reasonably likely to result in harm or substantial inconvenience. The bill prescribes procedural guidelines, including investigation and notice

procedures, mitigation procedures, and a safe harbor from liability for a financial institution in compliance. It directs the FTC to promulgate regulations requiring a financial institution that maintains or possesses sensitive financial personal information for a business purpose to dispose of it so that it cannot be read or reconstructed.

It provides that its provisions would supersede any state or local law, rule, or regulation that relates to information security standards of financial institutions; or the notification of consumers by financial institutions with respect to any breach of the confidentiality or security of information maintained or received by or on behalf of the financial institutions. (Sec. 7.)

H.R. 3375, Financial Data Security Act of 2005 (Pryce), amends the Fair Credit Reporting Act to establish for each consumer reporting agency, reporting broker, or reporting collector an obligation to maintain reasonable policies and procedures to protect the security and confidentiality of a consumer's sensitive financial account and identity information against any unauthorized use that is reasonably likely to result in substantial inconvenience or substantial harm. The bill prescribes data security safeguards that include investigations to protect against identity theft and fraud; notification alerts to law enforcement agencies, regulatory agencies, and affected consumers; investigation and notice requirements for third-party agreements; and financial fraud mitigation procedures. It requires the Secretary of the Treasury, the Board of Governors of the Federal Reserve System, and the Federal Trade Commission to jointly prescribe regulations shielding a consumer reporter from liability under state common law for loss or harm to the consumer subsequent to such reporter's offer of the free file monitoring service. It provides that persons in compliance with the Gramm-Leach Bliley Act shall be in compliance with this Act. It establishes guidelines for the joint promulgation of security regulations by the Secretary, the Board, and the FTC.

The bill amends the Fair Credit Reporting Act to prohibit states from imposing any requirement or prohibition with respect to the responsibilities of any person to protect the security or confidentiality of information on consumers maintained by or on behalf of the person; to safeguard such information from potential misuse; to investigate and provide notices to consumers of any unauthorized access to information concerning the consumer, or the potential misuse of such information, for fraudulent purposes; and to mitigate any loss or harm resulting from such unauthorized access or misuse. (Sec. 3.)

H.R. 3997, Financial Data Protection Act of 2005 (LaTourette), amends the Fair Credit Reporting Act to prescribe safeguards for data security. The bill requires consumer reporters to implement policies and procedures to protect the security and confidentiality of any consumer's sensitive financial personal information maintained, serviced, or communicated by or on the reporter's behalf against any unauthorized use reasonably likely to result in substantial harm or inconvenience to the consumer. It defines a "consumer reporter." It prescribes implementation guidelines that include investigation requirements, investigation notices and system restoration requirements, third-party duties, consumer notice, financial fraud mitigation, and free file monitoring. The Secretary of the Treasury, the Board of

Governors of the Federal Reserve System, and the Federal Trade Commission are to jointly develop implementing standards and guidelines.

The bill amends the Fair Credit Reporting Act to prohibit states from imposing any requirement or prohibition with respect to the responsibilities of any person to protect the security or confidentiality of information on consumers maintained by or on behalf of the person; to safeguard such information from potential misuse; to investigate or provide notices of any unauthorized access to information concerning the consumer, or the potential misuse of such information, for fraudulent purposes; or to mitigate any loss or harm resulting from such unauthorized access or misuse. (Sec. 2.)

H.R. 4127, Data Accountability and Trust Act (Stearns), instructs the FTC to promulgate regulations that require each person engaged in interstate commerce that owns or possesses data in electronic form containing personal information to establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information. The bill sets forth special requirements for information brokers and prescribes notification procedures for breaches of information security. It grants the FTC enforcement powers.

The bill supersedes any state or local statute, regulation, or rule that expressly requires similar information security practices and treatment of personal information and requires notification to individuals of a breach of security resulting in unauthorized acquisition of their personal information. It provides that it would not preempt the applicability of state trespass, contract, or tort laws or other state laws that relate to acts of fraud