Order Code RL33273

CRS Report for Congress

Data Security: Federal Legislative Approaches

Updated January 25, 2007

Gina Marie Stevens
Legislative Attorney
American Law Division

Prepared for Members and
Committees of Congress

Data Security: Federal Legislative Approaches

Summary

Several data breach notification and data security bills were considered in the 109th Congress to respond to increasing incidences of data breaches involving personal information. Congressional hearings were held 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.

On December 22, 2006, S. 3421, The Veterans Benefits, Health Care, and Information Technology Act of 2006 was signed into law and became P.L. 109-461. Title IX of P.L. 109-46, the Department of Veterans Affairs Information Security Act of 2006, requires the Department of Veterans Affairs (VA) to issue interim regulations providing for notice to veterans in case of breach of veterans' personal data, to notify law enforcement and certain congressional committees when a data breach occurs, to perform a risk analysis if unauthorized access to sensitive personal information occurs, and to notify those affected and provide free credit monitoring services if this reveals a "reasonable risk" for misuses of the information.

During the 109th Congress, three bills were reported by the Senate Commerce and Judiciary committees: S. 1326, S. 1408, and S. 1789. Three other bills were reported by the House Energy and Commerce, Financial Services, and Judiciary committees: H.R. 4127, H.R. 3997, and H.R. 5318. However, none of these bills were enacted into law. The passage of such comprehensive data breach legislation in the 109th Congress was precluded by jurisdictional concerns, along with unreconcilable approaches on credit freezes, exceptions for law enforcement and intelligence agencies, exemptions for financial institutions, data breach notification requirements, notification triggers, enforcement authorities, and preemption. The prospect for continued congressional attention is high during the110th Congress, with the Chairs of some of the jurisdictional committees identifying data security and privacy as a top legislative priorities, and with widespread media reports of data security breaches continuing.

This report discusses the core areas addressed in federal legislation, including the scope of coverage (who and what 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. (Some of these bills preempt and sometimes limit recently enacted state laws.) For related reports, see the Current Legislative Issues web page for "Personal Privacy Protection and Data Security" available at [http://www.crs.gov]. This report will be updated as warranted.

Contents

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] Victims of identity theft may incur damaged credit records, unauthorized charges on credit cards, and unauthorized withdrawals from bank accounts. With reports of information security breaches increasing, concerns about new cases of identity theft will likely continue to receive significant attention in Congress. The prospect for continued congressional attention is high during the110th Congress, with the Chairs of some of the jurisdictional committees identifying data security and privacy as top legislative priorities.

On December 22, 2006, S. 3421, The Veterans Benefits, Health Care, and Information Technology Act of 2006, was signed into law and became P.L. 109-461. Title IX of P.L. 109-46, the Department of Veterans Affairs Information Security Act of 2006, requires the Department of Veterans Affairs (VA) to issue interim regulations providing for notice to veterans in case of breach of veterans' personal data, to notify law enforcement and certain congressional committees when a data breach occurs, to perform a risk analysis if unauthorized access to sensitive personal information occurs, and to notify those affected and provide free credit monitoring services if this reveals a "reasonable risk" for misuses of the information.

---

[1] Graeme R. Newman and Megan M. McNally, Identity Theft Literature Review (July 2005) available at [http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf]. This report, funded by the U.S. Department of Justice, presents a review of the available scientific literature and other sources pertaining to the problem of identity theft and its prevention.

[2] Congressional hearings were held in the 109th Congress by the Commerce committees, Veterans' Affairs committees, Finance and Ways and Means committees, Judiciary committees, and the House Government Reform committee 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] Federal Trade Commission, ID Theft Clearinghouse Data, Jan. 25, 2006, [http://www.consumer.gov/idtheft/pdf/clearinghouse_2005.pdf]. CY 2005 is the last year for which data are currently available.

In the 109th Congress, three broader data breach bills were reported by the Senate Commerce and Judiciary committees: S. 1326, S. 1408, and S. 1789. Three other data breach bills were reported by the House Energy and Commerce, Financial Services, and Judiciary committees: H.R. 4127, H.R. 3997, and H.R. 5318. Although, as noted, the occurrence of data breaches has been commonplace, 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.

The passage of such comprehensive data breach legislation in the 109th Congress was precluded by jurisdictional concerns, along with unreconcilable approaches on credit freezes, exceptions for law enforcement and intelligence agencies, exemptions for financial institutions, data breach notification requirements, notification triggers, enforcement authorities, and preemption.

The House Financial Services and Energy and Commerce Committees passed competing bills (H.R. 3997, H.R. 4127), but efforts to reconcile the bills failed. One issue of contention was whether financial institutions would be exempted because of existing information security obligations imposed by the Gramm-Leach-Bliley Act (GLBA).[4] The Commerce bill eliminated the regulation of financial institutions with respect to information security by their functional regulators, and instead gave enforcement authority to the Federal Trade Commission and state attorneys general. Another major issue of contention was preemption, with the financial services bill preempting state data breach laws, and the commerce bill providing for limited preemption. In the Senate, jurisdictional issues also arose with the Commerce and Judiciary Committees passing bills (S. 1408, S, 1789), and the Banking Committee not acting on another bill (S. 3568). Another contentious issue that arose during consideration concerned notification requirements: should notice of breach occur for all security breaches or should notification instead be limited to significant breaches. Another obstacle to passage was the permissibility of credit freezes. The House Commerce bill would have let the states regulate credit freezes but allowed consumer access to and correction of personal information in data broker files, but the Financial Services bill would have set a national standard allowing victims of identity theft to freeze their credit files. The question of the relationship of federal legislation to state data breach notification, data security, and credit freeze laws was paramount. Concerns were expressed that multiple state laws make compliance an overly complex task.[5]

The prospect for continued congressional attention to data security legislation is high during the 110th Congress. Congress will continue to grapple with the

---

[4] See CRS Report RS20185, *Privacy Protection for Customer Financial Information*, by M. Maureen Murphy.

[5] "State Breach Notice Laws Have Similarities, But Significant Differences Require Attention," 89 *BNA Analysis & Perspective* 176 (Aug. 12, 2005).

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.

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 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.[6] 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.

---

[6] See CRS Report RS22374, *Data Security: Federal and State Laws*, by Gina Marie Stevens.

As of December 2006, 45 states had enacted data security breach notification laws.[7] 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 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 109th Congress.[8]

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

---

[7] 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. Generally, the reported data breaches have involved either the creation of fraudulent accounts, stolen laptops or computers, hacking, compromised passwords, insider or employee theft, or lost or misplaced discs or back-up tapes. See generally CRS Report RL33199, *Personal Data Security Breaches: Context and Incident Summaries*, by Rita Tehan (Table 1 summarizes selected data security breaches since 2000).

[8] See CRS Report RL33005, *Information Brokers: Federal and State Laws*, by Angie Welborn, for summaries of data breach legislation introduced in the 109th Congress. See also American Bankers Association, Data Breach Legislation (June 30, 2006), available at [http://www.aba.com/NR/rdonlyres/EBCFA68E-ED93-11D4-AB70-00508B95258D/43686/DataBreachLegislationChartSummary063006.pdf].

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.[9] 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 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 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

---

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

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 the sale or purchase of social security numbers in the private sector.[10] Several of the bills introduced in the 109th Congress prohibited the solicitation, display, sale, purchase, use, or access to social security numbers.

---

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

Credit Freezes.[11] 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. 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 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.[12] 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.

---

[11] See CRS Report RS22484, *Identity Theft Laws: State Penalties and Remedies and Pending Federal Bills*, updated by Tara Alexandra Rainson.

[12] See CRS Report RL31919, *Remedies Available to Victims of Identity Theft*, updated by Gina Marie Stevens.

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 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.[13] Privacy advocates seek a uniform national notification standard without preempting stronger state laws.[14] 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

---

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

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

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.