Selected Federal Data Security Breach Legislation

Kathleen Ann Ruane
Legislative Attorney

April 9, 2012

Congressional Research Service
7-5700
www.crs.gov
R42474

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

The protection of data, particularly data that can be used to identify individuals, has become an issue of great concern to Congress. There is no comprehensive federal law governing the protection of data held by private actors. Only those entities covered by the Gramm-Leach-Bliley Act, 15 U.S.C. §§6801-6809, (certain financial institutions) and the Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. §1320d *et seq*., and amendments to HIPAA contained in the Health Information Technology for Economic and Clinical Health Act (HITECH Act), P.L. 111-5, (certain health care facilities) are required explicitly by federal law to report data breaches. If private companies have indicated in their privacy policies that they will notify individuals upon a suspected data breach, failure to provide such notification may be considered to be an unfair and deceptive trade practice under Section 5 of the Federal Trade Commission Act (FTC Act). However, the FTC does not explicitly require private actors in possession of data related to individuals to notify individuals or the federal government should a data breach occur.

Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted laws requiring notification upon a data security breach involving personal information. However, these laws may vary in their application. They may only apply to certain entities or to certain data. Furthermore, companies maintaining stores of personal data may find it difficult to comply with the potentially different requirements of various state laws.

A combination of a lack of a comprehensive federal law addressing security breaches involving personal data and the difficulty industry participants report in complying with various state laws has led Congress to propose a number of bills that would require private actors in possession of personal data to report breaches of that data. The Senate Judiciary Committee recently approved and reported three bills that would create federal standards for data breach notification: S. 1151, the Personal Data Privacy and Security Act of 2011 (Chairman Leahy); S. 1408, the Data Breach Notification Act of 2011 (Senator Feinstein); and S. 1535, the Personal Data Protection and Breach Accountability Act of 2011 (Senator Blumenthal). The bills have similar structures and elements. This report will analyze the bills, as reported out of the committee, discussing their similarities and differences.

For more information about current state and federal data security breach notification laws, see CRS Report R42475, *Data Security Breach Notification Laws*, by Gina Stevens.

Contents

Contacts

Introduction

The protection of data, particularly data that can be used to identify individuals, has become an issue of great concern to Congress. There is no comprehensive federal law governing the protection of data held by private actors. Only those private entities covered by the Gramm-Leach-Bliley Act, 15 U.S.C. §§6801-6809, (certain financial institutions) and the Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. §1320d *et seq*., and amendments to HIPAA contained in the Health Information Technology for Economic and Clinical Health Act (HITECH Act), P.L. 111-5, (certain health care facilities) are required explicitly by federal law to report data breaches. If private companies have indicated in their privacy policies that they will notify individuals upon a suspected data breach, failure to provide such notification may be considered to be an unfair and deceptive trade practice under Section 5 of the Federal Trade Commission Act (FTC Act). However, the FTC does not explicitly require private actors in possession of data related to individuals to notify individuals or the federal government should a data breach occur.

Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted laws requiring notification upon a data security breach involving personal information.[1] However, these laws may vary in their application. They may only apply to certain entities or to certain data. Furthermore, companies maintaining stores of personal data may find it difficult to comply with the potentially different requirements of various state laws.[2]

A combination of a lack of a comprehensive federal law addressing security breaches involving personal data and the difficulty industry participants report in complying with various state laws have led Congress to propose a number of bills that would require private actors and government agencies in possession of personal data to report breaches of that data. The Senate Judiciary Committee recently approved and reported three bills that would create federal standards for data breach notification: S. 1151, the Personal Data Privacy and Security Act of 2011 (Chairman Leahy); S. 1408, the Data Breach Notification Act of 2011 (Senator Feinstein); and S. 1535, the Personal Data Protection and Breach Accountability Act of 2011 (Senator Blumenthal). The bills have similar structures and elements. This report will analyze the bills, as reported out of the committee, discussing their similarities and differences.

There have been other data security bills introduced in this Congress, as well, but they have yet to be reported out of their respective committees.[3] In the interest of brevity and clarity, they will not be discussed in this report.

[1] The Commercial Law League of America, State Data Security / Breach Notification Laws (as of December 2011), at http://clla.org/. Click "Resources." Click "Data Breach Notification Laws By State." Download document.

[2] For more information about current state and federal data security breach notification laws, see CRS Report R42474, *Selected Federal Data Security Breach Legislation*, by Kathleen Ann Ruane.

[3] For example, S. 1207, the Data Security and Breach Notification Act of 2011 and H.R. 2577, the SAFE Data Act are both bills that would create new federal privacy and security regimes for data.

Selected Federal Data Security Legislation

The three bills reported out the Senate Judiciary Committee have common elements and structure. All three bills would require notice of data security breaches, with certain exemptions. Each bill would attach penalties to a failure to provide notice in violation of the proposals. Each bill would preempt certain other state laws insofar as they would overlap with the new federal law. Two of the bills would require the creation and maintenance of data security programs. The bills have important differences as well. For example, S. 1151 contains amendments and additions to the crimes of identity theft and other criminal violations. S. 1535 would create a clearinghouse for technical information related to system vulnerabilities that would be maintained by a new government office. These, and other important differences, will be highlighted below.

Application

Before discussing the requirements of the proposed legislation, it is important to understand what entities the proposals would apply to and what types of information they would seek to protect. All three of the bills would apply to business entities (both for-profit and not-for-profit) and government agencies that collect and store sensitive, personally identifiable information. The bills also carve out certain exceptions for businesses to the extent that they are acting as "service providers." Each of the bills has slightly different definitions for each of these terms of art, but the spirit of their application remains substantially similar.

Entities Covered by the Bills

Agencies are defined as federal agencies by all three bills. Business entities cover all forms of business including corporations, partnerships, and other types of ventures. Service providers are defined as a business entity that provides electronic data transmission routing intermediate and transient storage or connections to its system or network where the business entity providing such services does not select or modify the content; is not the sender or intended recipient of the information; and the business entity transmits, routes, stores, or provides connections for personal information in a manner that personal information is undifferentiated from other types of data that such business entity transmits. Service providers are only treated as service providers to the extent that they are engaged in transmission services. If service providers hold or transmit data in such a way as to otherwise be covered by the proposals, then they would be required to comply with the proposals' requirements.

S. 1408 and S. 1535 also contain specific definitions for data brokers (or information brokers in the case of S. 1408). Both bills define these as commercial entities engaged in the business of collecting and assembling personal information of individuals who are not current or former customers of that entity for the purposes of selling that information to third parties. S. 1535 requires the entities to have information pertaining to at least 5,000 individuals who aren't customers or employees of that particular business entity to be covered by the definition of data broker, as well.

Data Covered by the Bills

All three bills would protect sensitive, personally identifiable information. They would define sensitive, personally identifiable information as the first and last name of an individual (or first

initial and last name) plus some other piece of identifying information, such as a birth date, Social Security number, bank or credit card number, driver's license number, or other government indentifying number. S. 1408 seems to have the most restrictive definition of sensitive, personally identifiable information, because it would require an individual's first and last name (or first initial and last name) to be part of the information covered, plus another identifying piece of information. However, S. 1408 also grants the Federal Trade Commission (FTC) the authority to modify the types of information considered to be sensitive, personally identifiable information if such modification would not unreasonably impede interstate commerce, which may allow the agency to expand the types of data that would be covered by the bill.

S. 1151 and S. 1535 define sensitive, personally identifiable information more expansively, with S. 1535 having the most expansive definition of all three bills. Both S. 1151 and S. 1535 would define sensitive, personally identifiable information to include the information above as well as an individual's first and last name plus his or her home address, phone number, mother's maiden name, or birth date. The definition would also include a nontruncated Social Security number, driver's license number, passport number, alien registration number, or other government-issued unique identifier on its own; cellphone GPS location; fingerprints, voice prints, retina scans, or other "biometric data"; or other unique account identifiers, such as financial account numbers, credit card numbers, etc.

S. 1535 would also include in the definition of sensitive, personally identifiable information not less than two of the following: first and last name, unique account identifier, security code access code or password, and information regarding medical history. Most expansively, S. 1535 would include in the definition of sensitive, personally identifiable information any combination of data elements that could allow unauthorized access to or acquisition of the information described above.

Notice Requirement

Each of the bills would require business entities and agencies to notify individuals and the government, under certain circumstances, when there is a security breach involving sensitive, personally identifiable information, unless an exception or an exemption would apply. The bills would define security breach as the compromise of the security, confidentiality, or integrity of, or the loss of, computerized data that results in the unauthorized acquisition of, or unauthorized access to, sensitive, personally identifiable information.

Notice to Individuals Whose Information Was Subject to a Security Breach

The bills would require the notification of individuals whose sensitive, personally identifiable information was breached to occur in a timely fashion. If the business entity or agency is not the owner of the information that has been breached, the business or agency must notify the owner or licensee of the information of the breach. The business entity or agency will not be required to notify the individuals whose information has been breached if the owner or licensee provides the notification.

The notification requirement is also different for companies that are service providers. Service providers that become aware of a security breach that has occurred over their systems must notify the business entity or agency that originated the communication or transfer of sensitive, personally identifiable information that was breached. At which point, the business entity or

agency that initiated the communication would then be required to comply with the notification requirements described above.

As noted, notification must occur in a timely fashion. Timeliness is defined as "without unreasonable delay." Businesses and agencies may take the time necessary, following a security breach, to determine the scope of the breach and take steps to prevent further or ongoing security breaches. They may also conduct risk assessments, discussed in more detail below, and take the time to restore the integrity of their data protection systems. A delay of longer than 60 days would be considered unreasonable, unless the FTC, or other agency with authority to do so, grants an extension, or an exception applies.

All of the bills allow notification to be delayed for law enforcement purposes. They also allow companies to avoid the notification requirement entirely if the company conducts an internal investigation and determines that there is no significant risk of harm resulting from the breach. Each of the bills has slightly different formations of these exceptions to the notice requirement, however.

Law Enforcement Exception

S. 1151 and S. 1408 allow notification to be delayed when either the Secret Service or the FBI determines that providing notification would impede a law enforcement investigation or national security. Notice would be required once law enforcement lifted its security delay.

S. 1535 allows for a similar delay by law enforcement, but this bill would be broader because any federal law enforcement agency or member of the intelligence community may require the delay. The delay in this case may only be accomplished upon written notice from the agency and must specify in writing the period of the delay. This delay may be extended by the law enforcement agency in writing as well. If the delay is not extended, 30 days after the first law enforcement delay order, the entity that experienced the breach would be required to provide notification to individuals whose information was affected.

Risk Assessment Safe Harbor

Businesses and agencies would be exempt from providing notice under all of the bills if they conduct a risk assessment that determines there is no significant risk that the breach will result in certain harms to the individuals affected. The harms the bills are concerned about are similar, but slightly different. S. 1151 and S. 1408 allow for notification to be avoided if no significant risk of identity theft, or physical or economic harm to the individual is found. S. 1535 would allow for avoidance of notification if there is no significant risk of identity theft or physical, economic, or significant emotional harm to the individuals found during the risk assessment.

Under all three bills, the business entity or agency would be required to submit the results of a risk assessment to the FTC and declare its intention to avail itself of the risk assessment safe harbor. The bills would differ slightly on the ways in which the FTC would proceed in granting the exemption, however. Under S. 1151, the FTC, upon receiving the results of a risk assessment, would then indicate in writing that the company or agency may use the safe harbor in order for the exemption from notification to apply. S. 1408, on the other hand, would allow the companies to use the risk assessment safe harbor unless, after notifying the FTC, the FTC indicated in writing that they could not. This would appear to be a broader risk assessment exemption. S. 1535

would require that the agency or business entity consult with the FTC in conducting the risk assessment and that the notification of the entity's intention to use the risk assessment safe harbor be delivered to both the FTC and the designated entity in charge of receiving reports to law enforcement of security breaches. The S. 1535 safe harbor may be used if no significant risk of harm is found and the FTC, or the designated entity, does not indicate that the safe harbor cannot be used, similar to S. 1408.

Each of the bills then would provide for a rebuttable presumption that no significant risk of harm exists if the data subject to the breach were encrypted or rendered otherwise unreadable or indecipherable, which would make it easier for agencies and business entities to avail themselves of the risk assessment safe harbor if they encrypt or otherwise render indecipherable the sensitive, personally identifiable information in their possession. S. 1535 would also create a presumption that there was significant risk of harm due to the breach if the information subject to the breach was not encrypted or otherwise rendered unreadable.

Notice to the Government Regarding a Security Breach

Under all three of the bills, under certain circumstances, entities and agencies experiencing a security breach would be required to notify the federal government of the breach. The bills would require the Secretary of the Department of Homeland Security to designate a central office to receive all notifications regarding security breaches. The bills call that office the "designated entity." That designated entity would then provide notification to the Secret Service, FBI, FTC, and other agencies, as appropriate.

Those experiencing breaches are not always required to notify the government, however. Under S. 1151 and S. 1535, they are only required to notify the government of a breach when the number of individuals affected is greater than 5,000; the database network that was breached contains information regarding 500,000 people, or more, nationwide; or the security breach involved federal government owned databases or involved the sensitive, personally identifiable information of individuals known to be employees or contractors of the government in certain positions. S. 1408 has the same requirements, except companies are not required to notify the government unless the breach pertains to more than 10,000 people, or the breach occurred in a database that held records of more than 1,000,000 people nationwide. Therefore, S. 1408 has a slightly higher threshold for when companies would have to report security breaches to the government. All three bills would require the FTC to conduct a rulemaking regarding what information the reports of security breaches should contain.

Exemptions From the Notice Requirement

All three bills provide for circumstances in which business entities and agencies would be exempt from providing notice of a security breach entirely. One of the primary reasons for exemptions from the notice requirement is if the entity is already required to provide notification by another federal data security law. All of the bills provide exemptions from the notice requirement for entities to the extent they are financial institutions covered by the security breach notification requirements in the Gramm-Leach-Bliley Act, 15 U.S.C. §§6801 – 6809. The bills would also exempt entities subject to the HIPAA data security provisions, P.L. 104-191 (1996), codified in part at 42 U.S.C. §1320 *et seq*.

All of the bills provide an exemption from the notice requirement for national security reasons. S. 1151 and S. 1535 would provide that if the Secret Service or the FBI determines that providing notification of a breach would reveal methods or sources that would impede law enforcement, notification would not be required. S. 1408 has a similar provision, but it is worded differently. Under that bill, notification would not be required where the Secret Service determined that it could be expected to reveal sensitive sources, law enforcement methods, or otherwise impede law enforcement. The FBI could also prevent notification if the FBI believed such notification would damage national security. In order for the FBI or the Secret Service to prevent disclosure, under S. 1408, the agencies would have to justify the prevention in writing to the Attorney General and the Secretary of DHS, respectively.

The bills also contain an exemption for business entities that participate in a financial fraud security program. If the business entity participates in a security program that effectively blocks the use of sensitive, personally identifiable information to initiate unauthorized financial transactions before the individual's account is charged, and provides notice to the affected person after a breach has resulted in fraud, the notice requirement under these bills would not apply. The notice requirement will apply, however, if the information subject to the breach is more than the individual's credit card number or security code.

Content and Methods of Notice

The bills lay out requirements for providing notification in written, telephone, and public notification formats. However, each bill combines these requirements slightly differently.

Methods of Notification

S. 1151 and S. 1408 would require business entities or agencies to provide individual notice through written notification, telephone notification, or e-mail notification if the individual has consented to receiving notice in that manner. The business entity or agency would also be required to provide notice to state media outlets if the number of residents in that state affected by the breach exceeds 5,000. S. 1408 would include a requirement that when a business entity or agency experiences a breach that affects more than 5,000 people, the agency or entity must notify nationwide consumer reporting as well.

S. 1535 requires more of agencies and businesses that have experienced a breach, however. S. 1535 would require written notice via the physical mail or e-mail, unless the individual has opted out of receiving e-mail. In addition to the written notice, telephone notification would be required as well. If the number of individuals affected by the breach would exceed 5,000, the company or agency must provide notice on its website, and other electronic interfaces, that the breach occurred in addition to the written and telephone notices. Furthermore, like S. 1151 and S. 1408, if an entity or agency experiences a breach that affects more than 5,000 people in a state, then the agency or company must provide notice through major media outlets in the state.

Content of Notification

S. 1151 and S. 1408 would require that notices contain a description of the categories of sensitive information that was or is believed to have been accessed or acquired; a toll free number where affected persons can contact the entity and find out what types of information the entity or agency possessed about that person; as well as contact information for major credit reporting agencies.

States may also require information about that state's victim protection assistance to be included in the notice if the state provides such assistance. The agency or business entity experiencing the breach must also coordinate notification with credit reporting agencies.

S. 1535 is more detailed than the other two bills in its requirements for the content of notifications. The written notice would be required to include a description of the information that had been breached; a toll free number where the individual could obtain information regarding the types of information the entity possesses related to that person; the contact information for credit reporting agencies; phone numbers for federal agencies that provide information about identity theft; and a notification that the person experiencing a breach of their sensitive, personally identifiable information can receive credit reports for two years and credit monitoring that enables the detection of misuse of sensitive, personally identifiable information. The notice must also inform the individual that he or she is entitled to a security freeze. A security freeze would be defined as a notice that prohibits consumer reporting agencies from releasing all or part of an individual's credit report without the consent of the individual, with certain limitations.

Perhaps most importantly, and providing the starkest contrast to the other two bills, the notice required by S. 1535 would also be required to inform the individual that the company or agency providing the notification will be responsible for all costs or damages incurred as a result of the breach. The telephone notification that would be necessary in addition to the written notification would be required to contain notice of the breach and a description of the categories of information that may have been acquired or accessed without authorization. It would also be required to inform individuals of the toll free number where they can obtain further information; the website that may be used to contact the agency or business; a description of the remedies that are available; and a notice that there will be a written notification forthcoming. The public notice that must appear on the company or agency's website will be required to contain notification of the breach, categories of information that were breached, and the toll free number and the website where people can obtain further information. The media notice, if required, must contain everything that must be in the public notice plus the contact numbers for credit reporting agencies; numbers for federal agencies that deal with identity theft; notice that individuals can get free credit reports and monitoring; notice that they are entitled to security freezes; and that the agency or business entity is liable for damages resulting from the breach.

Penalties and Enforcement for Violations of the Notice Requirement

All of the bills would allow the Attorney General and the FTC to enforce violations of the notice requirement with civil penalties resulting from the violations. Their enforcement powers generally and under each of the bills would be slightly different, however.

S. 1151and S. 1408 would allow the Attorney General to bring enforcement actions in federal court against agencies and businesses suspected of violating the notice requirement. Upon proof by a preponderance of the evidence that a violation occurred, the agency or business may be subject to civil penalties of up to $11,000 per day per security breach, with a total fine not to exceed $1,000,000, unless the violation was willful or intentional. If it is shown that the violation was willful or intentional, double penalties up to an additional $1,000,000 may be assessed. The Attorney General may also institute injunctive actions to prevent future violations if it appears that there was an ongoing practice of violation. Similarly, S. 1535 would allow the Attorney General to seek civil penalties of not more than $500 per day per violation, with total penalties

not to exceed $20,000, unless the violation was willful. Willful violations would be eligible for higher civil penalties, and certain types of violations would be presumed to be willful. The lower dollar amount for civil penalties under S. 1535 may be due to the fact that S. 1535 makes businesses and agencies financially responsible to individuals for damages done by security breaches. Like S. 1151 and S. 1408, the Attorney General would also be able to obtain injunctions under S. 1535.

S. 1151 and S. 1535 would allow the FTC to enforce violations of the notice requirement as though it were a violation of Section 5 of the FTC Act, 15 U.S.C. §45, because the bills would define violations of the notice requirement as unfair and deceptive trade practices that are prohibited by Section 5. The FTC would also have its various enforcement tools at its disposal, including civil penalties up to $1,000,000, unless the violation were willful in which case double penalties may be awarded.[4] Furthermore the FTC and Attorney General would be required to coordinate their enforcement

All three of the bills would allow states attorneys general to enforce violations of the notice requirement, under certain circumstances.

Neither S. 1151 nor S. 1408 contain private rights of action. S. 1535 does contain a private right of action, however. Under S. 1535, individuals would be able to sue and obtain damages incurred as a result of violations of the act. They may obtain damages of not more than $500 per individual per day while the violation persists, up to a maximum of $20,000,000 per violation. Punitive damages would also be able to be assessed if the violation were willful. This right of action could not be waived by any agreement or contract between individuals and companies or agencies, and it could not be subject to predispute arbitration agreements. Such requirements would make this a relatively strong private right of action.

Remedies for Security Breach

As noted above, S. 1535 would create the most extensive requirements for the content of the notices to be provided to individuals affected by a security breach. Included in the notice would be the fact that companies and agencies would be liable for any damages or costs to individuals that result from security breaches. Companies and agencies would therefore be liable to individuals for the costs of security breaches under S. 1535. The companies or agencies could comply by providing insurance to the individual against the damages for at least $25,000, or to pay the actual damages and costs. If entities or agencies fail to provide these remedies, they could be subject to private suit by individuals. Damages available would be $500 per day per individual whose information was breached, up to a maximum of $20,000,000 per violation, with punitive damages available for willful violations.

Agencies or business entities would also be required to provide, upon request, consumer credit reports on a quarterly basis for up to two years and credit monitoring, which would help those whose information has been disclosed without authorization detect whether that information is being misused. Individuals may also request a security freeze on their credit reports, which would

[4] Beyond seeking civil penalties, the FTC could also seeking injunctive relief, issue cease and desist orders, or institute an administrative procedure against violators of the act. See FTC, A Brief Overview of the FTC's Investigative and Law Enforcement Authority (last revised July, 2008), available at http://www.ftc.gov/ogc/brfovrvw.shtm.

prevent the release of their credit reports without their express authorization.[5] There would be certain limitations on the prevention of disclosure without consent, as well. The business or agency that experienced the security breach would be responsible for the costs of placing or removing a security freeze.

Data Security Program

S. 1151 and S. 1535 would both require business entities that are involved in collecting, accessing, transmitting, using, storing, or disposing of sensitive, personally identifiable information on 10,000 or more U.S. persons to put a data and privacy security program into place. Business entities would not be required to institute the program if and to the extent that they are in compliance with the requirements of Gramm-Leach-Bliley or HIPAA data security provisions. They would also be exempt from instituting the security program for data they encounter solely in their role as service providers, as defined above.

The data security program would be required to be comprehensive, expanding to the size appropriate for the complexity of each individual business entity and the complexity of the data it is required to protect. The program would have to be designed to ensure privacy, security, and confidentiality, protect against anticipated vulnerabilities, and protect against unauthorized access to the data.

The FTC would be required to conduct a rulemaking to create the administrative, technical, or physical safeguards that would comprise the data security program with which business entities must comply.

Periodic risk assessments would also be required, along with the risk assessments described above that would occur in the event of a security breach. In conducting the assessments, business entities would be required to identify reasonably foreseeable internal and external vulnerabilities that could result in a security breach; assess the likelihood of damage that would result from a breach; assess the sufficiency of its policies to prevent breaches; and assess the vulnerability of sensitive, personally identifiable information during the process of destroying or disposing of such information. The business entity would then be required to design its privacy and security program to control for the risks that it has identified and adopt measures "commensurate with the sensitivity of the data as well as the size, complexity, and scope of the activities of the business entity." This would include program elements that control access to systems and facilities containing protected data; features for detection, recording, and preserving information relevant to actual or attempted unlawful or unauthorized access and disclosure of the protected data; features that protect the data during use, transmission, storage, and disposal that includes encryption; and other protective and preventative measures. Lastly, the business entity would be required to establish a plan and procedure for minimizing the amount of protected data it maintains, by reducing its stores to only that data which is reasonably needed for the business purposes of the entity or to comply with legal obligations.

Each business entity would have to train its employees to comply with these precepts. They would also be required to ensure regular testing of these controls, the frequency of which would be determined by each business entity's risk assessment. In these periodic assessments, the

[5] Credit reporting agencies would be entitled to refuse to place or to remove a security freeze from an individual's credit report if the agency determines, in good faith, that the request to place or remove the freeze was part of a fraud.

business entity would be required to monitor, evaluate, and adjust its security program as appropriate and in light of relevant changes.

Business entities would also be required to exercise a certain amount of control over third parties when transferring data to them. If the third party would not be covered by the act, the business entity transferring the information would be required to secure the data's security via contractual obligations.

The bills would also create a safe harbor for businesses that comply with or provide protection equal to industry standards or standards widely accepted as an effective industry practice as identified by the FTC.

Penalties and Enforcement

S. 1151 and S. 1535 would create slightly different schemes of penalties and enforcement for violations of the data security program provisions. Under S. 1151, business entities that violate the requirements of the data security program provisions would be subject to civil penalties of not more than $5,000 per violation with a maximum penalty of $500,000, unless the violation is willful or intentional, in which case double penalties may be assessed. Injunctions may also be issued to prevent further violations. The FTC would be given the power to enforce these provisions. States attorneys general would also be given the authority to enforce violations of the data security program requirements in certain circumstances. There is no private cause of action for violations, however.

Under S. 1535, penalties may be slightly more harsh. While singular violations could face civil fines of $5,000 per violation per day, as under S. 1151, the maximum penalty would be raised to $20,000,000, under S. 1535, unless the conduct was willful or intentional. If the violation was willful or intentional, an extra $5,000 per violation per day may be assessed while the violation exists. S. 1535 is also more specific about the considerations to be undertaken when assessing penalties for violations. Like S. 1151, the Attorney General may seek injunctions to prevent future or continuing violations, and states attorneys general may enforce the title as well, under certain circumstances.

Unlike S. 1151, S. 1535 would create a robust private right of action in which any person aggrieved by a violation of the data security program requirements could bring a civil action to recover for the personal injuries the individual sustained as a result of the violation. Remedies could include actual damages of not more than $10,000 per violation per day, up to $20,000,000. Punitive damages could also be assessed if the business entity intentionally and willfully committed the violations. Equitable relief in the form of an injunction would also be available to private litigants. This private right of action would not be able to be waived by the individual via contract with the business entity, nor would predispute arbitration agreements be valid if it would require arbitration of disputes raised by this section.

Preemption

All three bills would preempt all other provisions of federal or state law that relate to notification of security breaches by a business entity engaged in interstate commerce or agencies, with certain exceptions. None of the bills would supersede the data security requirements of the Gramm-Leach-Bliley Act or any of its implementing regulations. Furthermore, none of the bills would

supersede the provisions of Health Information Technology for Economic Clinical Health Act (HITECH Act) which require certain entities to provide breach notifications. S. 1535 also makes clear that it would not preempt state common law, which would mean that businesses would remain liable for state trespasses, contract violations, tort law, and damages caused by a failure to notify an individual following a security breach. S. 1151 would make clear that the bill would not supersede HIPAA privacy provisions, as well.

Reporting on the Use of Exemptions

The bills would also require various reports to Congress. S. 1151 and S. 1535 would require the FTC to report to Congress on the number and nature of the security breaches described in the notices filed by business entities invoking the risk assessment exemption. S. 1535 would require the FBI and the Secret Service to report to Congress on the use of the risk assessment exemption and the response of those agencies to such notices. All three of the bills would require the Secret Service and the FBI to report to Congress on the number and nature of security breaches subject to the national security exemption.

Clearinghouse

S. 1535, unlike the other two bills, would also require the entity designated by the federal government to receive reports of security breaches to create and maintain a clearinghouse of technical information concerning system vulnerabilities identified after security breaches. Whenever a business entity or agency is required to notify the government of a security breach under the bill, the agency or business entity would also be required to include information about the nature of the breach and vulnerabilities that may have been exposed as a result.

Agencies and business entities may review the information maintained by the clearinghouse for the purposes of preventing security breaches in the future, so long as they obtain certification to access the information. Certification would be obtained from the designated entity, and it would be conditioned on those receiving certification only using the data to improve security, and reduce the vulnerability of networks that use sensitive, personally identifiable information. The information in the clearinghouse could not be used for competitive commercial purposes and could not be shared with third parties. Furthermore, the data in the clearinghouse would be anonymous to protect those providing data as a result of a breach.

New Crimes and Penalty Enhancements

All three bills would create new crimes for willful concealment of security breaches. Any person who, having knowledge of a security breach that was subject to the notice requirement and that knew the breach was subject to the notice requirement, conceals the security breach, and economic harm results from the breach to any individual in the amount of $1,000 or more, would be guilty of a crime and may be fined, or imprisoned for up to five years, or both.

S. 1151 would add new offenses to the Computer Fraud and Abuse Act (CFAA). It would expand offenses for trafficking in passwords (18 U.S.C. §1030(a)(6)) to cover passwords for access to protected computers, not just government computers. It would create a new offense for causing or attempting to cause damage to a critical infrastructure computer that results in substantial impairment of the operation of critical infrastructure associated with that computer. Violations

could result in fines or imprisonment for between 3 and 20 years, or both. Other amendments to the CFAA would be implemented as well.

Government Contracting Requirements

S. 1535 would also restrict the General Services Administration (GSA) in granting government contracts. Whenever considering a contract award totaling more than $500,000 with data brokers, the GSA would be required to evaluate the data privacy and security program of the data broker, its record of compliance with the program, and its response to security breaches of sensitive, personally identifiable information. When entering into contracts with data brokers that would involve the use of sensitive, personally identifiable information, the GSA would be required when awarding the contract to attach penalties for failure to comply with the data security and breach notification requirements contained in the bill. GSA would also have to require data brokers that engage service providers, which are not subject to the data security and notification requirements of the bill, to exercise due diligence in selecting service providers for responsibilities related to sensitive, personally identifiable information; take reasonable steps to select service providers that are capable of maintaining appropriate safeguards; and require the service providers, by contract, to implement and maintain programs designed to meet the objectives of the data security and notification requirements of the bill.

S. 1535 would also amend the Federal Information Security Management Act (44 U.S.C. §3541, *et seq.*) to require agencies implementing information security programs to include procedures for evaluating and auditing the information security practices of contractors and third parties with which the agencies must share sensitive, personally identifiable information.[6] The agencies would also be required to ensure that remedies will be available should significant deficiencies be discovered in security.

Federal agencies would be prohibited from entering into contracts with data brokers to access for a fee any database containing, primarily, the sensitive, personally identifiable information of U.S. persons, unless the agency has conducted a privacy impact assessment under Section 208 of the E-Government Act of 2002 (44 U.S.C. §3501 note). Agencies would also have to adopt regulations for fair information practices for databases to be accessed in this manner, and incorporates into contracts with data brokers that are worth more than $500,000 provisions for penalties for failure to comply with the notification requirements of the bill, and penalties for knowingly providing inaccurate sensitive, personally identifiable information to the federal government.

Author Contact Information

Kathleen Ann Ruane
Legislative Attorney
kruane@crs.loc.gov, 7-9135

[6] The bill would specifically amend 44 U.S.C. §3544(b).