Summary Comparison of Current Data Security and Breach Notification Bills

Topic	S. 117 (Nelson)	S. 961 (Carper/Blunt)	H.R. 1770 (Energy & Commerce)	S. _____ (Warner) Draft	S. _____ (Leahy) Introduced	H.R. 2205 (Neugebauer)	Comments
Data Security Standards	The FTC shall promulgate regulations requiring information security practices that are appropriate to the size, scope and complexity of the organization.	Develop, implement, and maintain a comprehensive information security program that is appropriate to the size, scope, and sensitivity of the enterprise.	Implement and maintain reasonable security measures and practices appropriate for the size and complexity of such covered entity and the nature and scope of its activities.	Implement, maintain, and enforce reasonable policies and procedures to protect sensitive account and personal information that are appropriate to the size, complexity, scope, and sensitivity of the data.	Implement a comprehensive information security program appropriate to the size and complexity of the entity.	Develop, implement, and maintain a comprehensive information security program that ensures security and confidentiality of sensitive information that is appropriate to the size, scope, and sensitivity of the information.	Leahy allows the FTC to develop data security requirements through rulemaking.
Specific Data Security Requirements	These policies would require a security policy, identification of a security officer, an assessment of vulnerabilities, mitigation of vulnerabilities, data retention,	The bill contains specific guidelines for creating such a program, including specific recommendations for security controls (e.g. access, restrictions,	None	None	The bill contains specific elements including risk assessment; access controls; data minimization; training; and vulnerability testing.	The bill contains specific guidelines for creating such a program, including specific recommendations for security controls (e.g. access, restrictions,	N/A

As of: May 7, 2015

	and data destruction policies.	encryption, and training) as well as administration requirements (e.g. board oversight).				encryption, and training) as well as administration requirements (e.g. board oversight).	
Personal Information Definition	(i) non-truncated social security number; (ii) a financial account number or credit or debit card number in combination with access code; (iii) an individual's first and last name or first initial and last name in combination with: (a) a driver's license number, passport	(i) Social security number; (ii) An individual's first name and last name, in combination with: (a) Driver's license, passport or other government identification number; (b) information that could access a consumer's account, such as user name and password or email and password; or (c) biometric data to access a financial account.	(i) An individual's first and last name or first initial and last name in combination with <u>all</u> of the following: (a) home address or telephone number; (b) mother's maiden name if identified as such; (c) or birthdate. (ii) A financial account number or credit or debit card number or other identified in combination with an access code that allows	Sensitive Personal Information: means the first and last name, address, or telephone number of an individual in combination with any of the following: (i) social security number; (ii) driver's license number or equivalent state identification, passport, military identification, or other unique identification number; (iii)	Sensitive personally identifiable information means: (i) a non-truncated social security, driver's license or other government identification number; (ii) a financial account number or credit or debit card number in combination with any security code or password required to obtain funds; (iii) unique	Sensitive personal information includes: (i) Social Security number; and (ii) first and last name in combination with: (a) consumers driver's license number, passport number, or other similar government identification number; (b) information to access an account, such as email and password; (c) biometric data use to gain access	S. 117 allows the FTC to amend the definition if it is determined that the definition is not sufficient to protect consumers from identity theft. H.R. 1770 and Warner exclude encrypted information the definition of personal information.

	number, or other government identification number; (b) unique biometric data; (c) a unique account identifier, user name, or routing code with any associated security code or password that is required to obtain money, goods, services, or any other thing of value; or 2 of any of the following: (aa) home address or telephone number; (bb) mother's maiden name, if identified as such; birthdate.	Sensitive Account Information means financial account numbers relating to a consumer, including credit or debit card number alone, or in combination with any security code required to access a financial account.	an individual to obtain credit or other financial transactions. (iii) A unique account identifier, biometric data, username, or routing code in combination with an access code that allows an individual to obtain money or other things of value. (iv) A non-truncated social security number. (v) The location of, number from which and to which a call is placed, and the time and duration of a call.	tax identification number. Sensitive Account Information means the first and last name, address, or telephone number of an individual in combination with a financial account number relating to an individual, including (i) a bank account number, (ii) credit card number, (iii) or debit card number and any security code, access code, password, or other personal identification	account identifier, including username or email address in combination with a security code or password; (iv) unique biometric data; (v) an individual's first and last name in combination with information about past present or future physical or mental health or condition, as well as health insurance information; (vi) in formation about an individual's geographic location that is	to a financial account. Sensitive account financial information means financial account number, routing number, or debit card number, in combination with any security code or password.	

			(vi) A user name or email address, in combination with a password or security question and answer that would permit access to an online account. (vii) Driver's license number, passport number, or other government-issued identification number.	information necessary to access the financial account or to conduct a transaction.	sufficient to identify the street and name of city; (vii) password-protected digital photos or videos.		
What Constitutes a Security Breach	A compromise of a system that leads to unauthorized access to or acquisition of personal information.	Unauthorized acquisition of sensitive account or sensitive personal information. Does not include unauthorized acquisition of encrypted, redacted, or	A compromise of a system where there is a reasonable basis to conclude there is unauthorized access to and acquisition of personal information.	Unauthorized acquisition electronic sensitive account or personal information	Compromise of privacy or security of data that results in, or there is a reasonable basis to conclude has resulted in, unauthorized access to or	The unauthorized acquisition of sensitive financial account or sensitive personal information. Does not include unauthorized acquisition of encrypted,	N/A

Summary Comparison of Current Data Security and Breach Notification Bills

		otherwise protected data if the key is not also obtained.			acquisition of sensitive personally identifiable information.	redacted, or otherwise protected data if the key is not also obtained.	
Individual Notification Requirement	Notify each individual whose personal information was or is reasonably believed to have been acquired or accessed.	Notify all consumers to whom the sensitive information relates.	Notify any consumer that has been affected, or is reasonably believed to be affected, by the breach of security.	Notify each individual citizen or resident whose data in electronic for was, or is reasonably believed to have been, acquired.	Notify any resident of the U.S. whose personally identifiable information has been, or is reasonably believed to have been, accessed or acquired.	Notify all consumers to whom the sensitive information relates.	HIPAA and GLBA covered entities are all exempt or deemed in compliance with these requirements. Leahy allows entities to be exempted from notification if national security or law enforcement agency determines that notification could reveal sensitive sources and damage

Summary Comparison of Current Data Security and Breach Notification Bills

							national security.
Exemptions to Notification Requirement (Risk Trigger)	If the covered entity reasonably concludes that there is no reasonable risk of identity theft, fraud or unlawful conduct. Rebuttable presumption that encrypted data does not create a reasonable risk of harm.	Only notify if there is a reasonable likelihood of substantial harm of identity theft or fraudulent transactions to the consumers to whom information relates.	If the covered entity determines there is no reasonable risk of identity theft, economic loss or harm, or financial fraud.	If the covered entity reasonably believes that the data has or will cause financial harm.	If data is encrypted or otherwise unusable such that misuse will not occur.	Only notify if there is a reasonable likelihood of substantial harm of identity theft or fraudulent transactions to the consumers to whom information relates.	N/A
Timing of Notification	Within 30 days, or as promptly as possible if the covered entity requires it to identify affected consumers, prevent further breach, or reasonably restore the	Without unreasonable delay.	As expeditiously as possible and without unreasonable delay, but no later than 30 days after the scope of the breach is determined and the system is	As expeditiously as practicable and without unreasonable delay. A reasonable delay may include time to determine the scope of the breach,	As expediently as possible and without unreasonable delay. Reasonable delay includes determining the scope of the breach, provide notice to law	Without unreasonable delay.	N/A

	integrity of the system.		reasonably restored.	identify individuals affected by the breach, and restore the reasonable integrity of the data system.	enforcement, or prevent further disclosures, but shall not exceed 30 days after discovery.		
Method of Notification	Writing, email or other electronic means if the covered entity's primary method of communication is email or the individual has consented to receive notification by email.	Written, telephonic, email or electronic form.	Written, email or electronic means if that is the primary method of communication.	Written, telephone, email or other electronic means.	Written, telephone, or email notice.	Written, telephonic, or email.	N/A
Substitute Notice	Lack of sufficient contact information or the covered entity owns or possess data for fewer than 10,000 individuals and	Notice in print and broadcast media where there is a lack of sufficient contact information, excessive costs to the covered entity, or exigent circumstances.	If after attempting to provide direct notification, there remain 500 or more individuals with insufficient contact information	If direct notification is not feasible due to (i) excessive cost or (ii) lack of sufficient contact information for the individual.	If notice is required to more than 5,000 individuals in 1 state and individual notice is not feasible due to insufficient	Notice in print and broadcast media where there is a lack of sufficient contact information, excessive costs to the covered entity, or exigent circumstances.	S. 117 allows the FTC to issue rules to govern when substitute notice may be provided.

	direct notification would be an excessive cost. Email if possible; conspicuous posting on the entity's website, and notification to print and broadcast media in both urban and rural areas. Must contain the same information as direct notice.		notification shall be made in a way that is reasonably calculated to reach them. Including email or other electronic notification to the extent that the covered entity has contact information and a conspicuous notice on the covered entity's Internet website for at least 90 days. Contain the same information as direct notification.	Notice shall be in either (i) a conspicuous notice on the website of the covered entity; or (ii) notification in print and broadcast media, including metropolitan and rural areas.	contact information. Notice shall be provided in major statewide media outlets and in a clear and conspicuous positing in the website of the entity.		
Content of Notification	(i) estimated date or date range of the breach of security; (ii)	(i) Description of the sensitive information involved; (ii) general	(i) Identity of the covered entity, if that entity is subject to the breach;	(i) the date, estimated date, or estimated date range; (ii) a description	(i) a general description of the incident and the date of the breach; (ii)	(i) Description of the sensitive information involved; (ii) general	N/A

	description of personal information affected; (iii) toll-free number to learn about the breach; (iv) notice that consumer may be eligible for free credit report and instructions to obtain it; (v) toll-free numbers for credit reporting agencies; (vi) toll-free number and website where the consumer can learn about identity theft from the FTC.	description of actions taken to secure the breach; (iii) summary of the rights under the FCRA if the breach is of personal information.	(ii) description of the personal information involved; (iii) date, or date range, of the breach; (iv) telephone number for any covered entities that are not non-profits or small businesses, where consumers can learn about the breach; (v) toll-free number for consumer reporting agencies; (vi) toll-free number and website for the FTC's identity theft information.	of the type of sensitive account or personal information that was accessed and acquired; (iii) information that the individual can use to contact the covered entity to inquire about the breach of security or the information.	a description of the sensitive information that was, or is reasonably believed to have been, accessed or acquired; (iii) the acts taken to protect from further breaches; (iv) toll free number to contact the entity and where individuals can learn what information is maintained about them; and (v) toll free contact number for the consumer reporting agencies.	description of actions taken to secure the breach; (iii) summary of the rights under the FCRA if the breach is of personal information.	
Notice to Credit Agencies	Notify the consumer reporting agencies if the	Notify the consumer reporting agencies if the	Notify the consumer reporting agencies	None	If notification is required to be made to more than	Notify the consumer reporting agencies if the	N/A

	breach affected 5,000 or more consumers.	breach affected 5,000 or more consumers. Notice to relevant payment card networks, if breach involves payment card numbers	without unreasonable delay if the breach affected 10,000 or more consumers.		5,000 individuals and the information could be used to commit financial fraud, notify the consumer reporting agencies without unreasonable delay, and if possible before notice to individuals.	breach affected 5,000 or more consumers. Notice to relevant payment card networks, if breach involves payment card numbers	
Notice to Government/ Law Enforcement	Department of Homeland Security shall designate an agency to receive notice if more than 10,000 individuals are affected. Notice to be delivered within 3 business days before individual	Must notify an appropriate federal regulator and federal law enforcement.	Must notify FTC and Secret Service or FBI if the number of affected individuals is, or is reasonably believed to have been over 10,000. Notice should be provided no less than 10 days before consumer notification.	Must notify the Secret Service or the FBI if the number of individuals whose personal information the covered entity reasonably believes to have been accessed and acquired	Notify the FTC not later than the date on which notice is provided to individuals. Notify the designated federal government entity if more than 5,000 individuals are impacted, the	Must notify an appropriate federal regulator and federal law enforcement.	Leahy allows the Attorney General to issue rules to adjust the thresholds for notice to law enforcement and national security authorities.

	notification, and no later than 10 days after the date of discovery.			excessed 10,000.	breach involves a networked database with more than 500,000 individual's information, the breach involved a federal database, or the breach involves those known to be federal law enforcement or national security employees. Notice to be provide as promptly as possible, but not less than 72 hours before individual notification or not later than 10 days after discovery.		

Summary Comparison of Current Data Security and Breach Notification Bills

Delay Provisions	At the request of the FBI or Secret Service upon written request.	N/A	At written request of federal, state, or local law enforcement if notification would interfere with an investigation or harm national security.	At written notification from federal law enforcement that notification would interfere with a criminal investigation. At the written request of a national security agency or homeland security agency that the notification would threaten national or homeland security.	Written request of a Federal law enforcement or intelligence agency if it determines that notification would impede a criminal investigation or national security. Notice would be given 15 days after invocation unless a written request is made not to notify.	If delay is requested by a law enforcement agency.	S. 117 grants exemption for entities that participate in a security program that effectively blocks the use of personal information for unauthorized financial transaction and provides notice to affected individuals of attempted transactions. This exemption does not apply if the breach contains information other than credit card or credit card security code or if it consists of an

Summary Comparison of Current Data Security and Breach Notification Bills

							individual's credit card number and first and name
Criminal Penalties for Concealment of a Security Breach	Intentional and willful concealment of a breach, can result in 5 years in prison if $1,000 or more in economic harm is caused.	None	None	None	Intentional and willful concealment of a breach, can result in 5 years in prison, a fine, or both if $1,000 or more in economic harm is caused.	None	N/A
Civil Enforcement	FTC shall enforce as unfair or deceptive acts. State attorney generals may enforce and obtain injunctive relief and civil penalties of not $11,000 per day for violating data	The appropriate regulator would be required to enforce the Bill. The regulators under the Bill are: (i) the FDIC, Federal Reserve Board, (ii) National Credit Union Administration	FTC shall enforce as unfair or deceptive acts, and may seek civil penalties. Violations of breach requirements capped at not greater than $1,000 per violation. Civil penalties are capped at	FTC shall enforce as unfair or deceptive acts against entities that are not subject to regulation a functional regulator, as well as common carriers.	Enforceable by the Attorney General, state attorney general, and the FTC. Civil penalties based on the number of persons impacted multiplied by $16,500, capped at $5,000,000 for both FTC and	The appropriate regulator would be required to enforce the Bill. The regulators under the Bill are: (i) the FDIC, Federal Reserve Board, (ii) National Credit Union Administration	Leahy allows for FTC rulemaking to carry out enforcement practices.

	security provisions, and $11,000 for each violation of breach notification. Total cap of $5,000,000 for data security and notification separately. U.S. Attorney General may bring an action against an entity for failing to notify law enforcement.	Board, (iii) SEC, (iv) CFTC, (v) Federal Housing Enterprise Oversight, (vi) the appropriate State insurance authority, and (vii) the FTC. The FTC would also have enforcement authority over common carriers, air carriers, and entities subject to the Packers and Stockyards Act. Limited private right of action for entities or consumers that suffer financial harms to recover actual financial damages, court costs, and reasonable attorney fees in the case of negligent	$8,760,000 for violations of data security provisions and $17,520,000 for breach provision. State attorney generals may enforce and obtain injunctive relief and civil penalties of not $11,000 per day for violating data security provisions, and $1,000 for each violation of breach notification. Total cap of $2,500,000 for data security and notification separately.	The functional regulators are: (i) the FDIC, Federal Reserve Board, (ii) National Credit Union Administration Board, (iii) SEC, (iv) CFTC, (v) the appropriate State insurance authority, (vi) the FTC, (vii) Department of Transportation, (viii) Department of Agriculture. Penalty caps for a violation of either section is capped at $5,000,000 per section.	AG actions. Violations are treated as unfair and deceptive practice by the FTC. No private right of action.	Board, (iii) SEC, (iv) CFTC, (v) Federal Housing Enterprise Oversight, (vi) the appropriate State insurance authority, and (vii) the FTC. The FTC would also have enforcement authority over common carriers, air carriers, and entities subject to the Packers and Stockyards Act.	

		violation. May also recover damages, costs and attorney's fees, as well as punitive damages for knowing violations.					
Preemption	Any rule or law that requires information security practices similar to those required or requires notification for a security breach as defined in the law. Does not preempt state common law or enforcement of state consumer protection laws.	Any state law relating to protection of security of information, safeguarding information from unauthorized access and acquisition, investigate or provide notice of unauthorized acquisition, or access to, information, mitigate any potential or actual loss or harm resulting from access or harm.	Any state law with respect to data security or breach notification. Would not exempt entities from liability under common law.	Expressly preempts state laws related to data security and breach notification.	Preempts federal and state law requiring data security practice or notification of security breaches that are less stringent. Protects state consumer protection laws and state common law.	Any state law relating to protection of security of information, safeguarding information from unauthorized access and acquisition, investigate or provide notice of unauthorized acquisition, or access to, information, mitigate any potential or actual loss or harm resulting from access or harm.	N/A

Summary Comparison of Current Data Security and Breach Notification Bills

Credit Monitoring or Reports	Free credit reports quarterly for 2 years after a consumer requests a credit report. Not required if the only information is a consumer's name address, or phone number in combination with a credit or debit card number and security code.	None	None	None	None	None	S. 117 allows the FTC to issue rules to determine the circumstances where a free credit report is required.