Summary Comparison of Current Senate Data Security and Breach Notification Bills **2/25/2014**

Topic	S. 1193; (Toomey)	S. 1897 (Leahy)	S. 1927 (Carper/Blunt)	S. 1976 (Rockefeller)	S. 1995 (Blumenthal)	Comments
Data Security Standards	"reasonable measures"	Any business dealing with information of 10,000 or more citizens would be subject to the security program requirements.	Reasonable policies to protect and secure sensitive account and personal information that are reasonably likely to result in substantial harm if it were subject to a data breach.	The FTC would promulgate regulations within a year of the Bill's enactment that would require covered entities to create information security programs.	Any business dealing with information of 10,000 or more citizens would be subject to the security program requirements.	S. 1193 has a companion bill in the House, H.R. 1468, which contains additional cybersecurity information sharing provisions. S. 1897 has a companion bill in the House, H.R. 3990.
Specific Data Security Requirements	None	(i) Risk Assessment; (ii) Risk Management; (iii) Data Minimization; (iv) Training; (v) Encryption	These policies should be in line with the size of the covered entity, the use of the data, and the type of data in question.	(i) Risk assessment; (ii) Data Management Policies; (iii) Risk Management; (iv) Disposal	(i) Risk Management; (ii) Training & Testing; (iii) Supervision of Third Parties; (iv) Assessment and Modernization	S. 1897, S. 1976, and S. 1995 allow the FTC to establish security program requirements. None of these bills will change GLBA or HIPAA security requirements.
Personal Information Definition	(a) First name or (b) first initial and last name, in	(a) First and last name, or (b) first initial and last	(a) An individual's first name and last name, (b) Address,	(i) Non-truncated social security numbers; (ii)	Any the following data elements in electronic form:	N/A

Summary Comparison of Current Senate Data Security and Breach Notification Bills **2/25/2014**

Topic	S. 1193; (Toomey)	S. 1897 (Leahy)	S. 1927 (Carper/Blunt)	S. 1976 (Rockefeller)	S. 1995 (Blumenthal)	Comments
	combination with **one** of the following data elements: (i) Social security number; (ii) Government ID number; (iii) Financial account, credit, or debit card number, along with required security codes. Does not include encrypted, redacted, or secured data.	name, in combination with **any two** of the following data elements: (i) Home address or telephone number; (ii) Mother's maiden name; (iii) Date of birth. The definition would also include: (i) Social security, or other government ID number; (ii) Unique biometric data; (iii) Unique account identifiers, including credit and debit card numbers. Any combination of first and last	or (c) Telephone number, in combination with any **one** of the following data elements: (i) Social security number; (ii) Driver's license or other government ID number; (iii) taxpayer identification number.	Financial account, credit or debit card numbers with any security code; or (a) First and last name, or (b) first initial and last name in combination with: (i) Driver's license or state identification document; (ii) Unique biometric data; (iii) Unique account identifier, user name, or routing code with a password that would allow access to anything of value; or Any **two** of: (a) Home address or phone number, (b) Mother's maiden name, or (c) Date of birth.	(a) First and last name, or (b) first initial and last name in combination with any **two** of the following: (i) Home address; (ii) Telephone number; (iii)Mother's maiden name; (iv) Date of birth; or Non-truncated government ID number; Location data that is derived from an individual's electronic device, excluding device ID numbers and/or Internet Protocol addresses; Unique biometric data;	

Summary Comparison of Current Senate Data Security and Breach Notification Bills **2/25/2014**

Topic	S. 1193; (Toomey)	S. 1897 (Leahy)	S. 1927 (Carper/Blunt)	S. 1976 (Rockefeller)	S. 1995 (Blumenthal)	Comments
		name, or first initial and last name in combination with: (i) Unique account identifiers, credit or debit card numbers, or any security codes or source code to generate such codes.			Unique account identifiers, e.g. financial account, credit or debit card numbers, user name, health insurance policy numbers; or Not less than **two** of the following: (i) First and last name or first initial and last name; (ii) Unique account identifiers; (iii) Security code or source code that could be used to generate such codes; or (iv) Individual medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or Any combination of data elements that could allow	

Summary Comparison of Current Senate Data Security and Breach Notification Bills **2/25/2014**

Topic	S. 1193; (Toomey)	S. 1897 (Leahy)	S. 1927 (Carper/Blunt)	S. 1976 (Rockefeller)	S. 1995 (Blumenthal)	Comments
					unauthorized access or acquisition of the above information, including: (i) A unique identifier; (ii) An electronic identification number; (iii) A username or routing code; or (iv) Any associated security code or source code that could be used to generate such codes	
What Constitutes a Security Breach	Unauthorized access and acquisition of electronic data containing personal information.	The acquisition and access to sensitive personally identifiable information for an unauthorized purpose or in excess of authorization.	Unauthorized acquisition of sensitive account or personal information.	The unauthorized access or acquisition of personal information from a covered entity.	The unauthorized acquisition or access to sensitive personally identifiable information that is for an unauthorized purpose or in excess of authorization.	N/A
Individual Notification Requirement	Notify if personal information was reasonably	Notify if personally identifiable information has	Notify all consumers to whom the sensitive information relates.	Notify the individuals whose information was or is reasonably	Notify any resident of the United States whose sensitive personally	HIPAA and GLBA covered entities are all exempt or

Summary Comparison of Current Senate Data Security and Breach Notification Bills **2/25/2014**

Topic	S. 1193; (Toomey)	S. 1897 (Leahy)	S. 1927 (Carper/Blunt)	S. 1976 (Rockefeller)	S. 1995 (Blumenthal)	Comments
	believed to have been accessed and acquired by an unauthorized person.	been, or is likely to have been, accessed or acquired.		believed to have been acquired or accessed	identifiable information has been, or is reasonably believed to have been, accessed or acquired.	deemed in compliance with these requirements.
Exemptions to Notification Requirement (Risk Trigger)	Only notify if breach caused, or is likely to cause, identity theft.	Only notify if breach resulted in, or will result, in identity theft, economic loss or harm, or physical harm to affected individuals.	Only notify if there is a likelihood of substantial harm arising from the breach.	(i) No notice if there is no reasonable risk to identity theft, fraud, or other unlawful conduct; (ii) Law enforcement may stop notification if sensitive sources or national security may be harmed; (iii) Do not notify if a breach only includes an individual's credit card number or security code, and there is a security system that blocks fraud on accounts.	(i) No notice if there is no significant risk that a security breach has or will result in harm to affected individuals; (ii) Law enforcement may stop notification if sensitive sources or national security may be harmed; (iii) No notice if a security system effectively blocks fraud from accounts and if notice is given if fraud does occur on an account.	N/A
Timing of Notification	As expeditiously as practicable and without unreasonable delay following	Notice is to be sent without unreasonable delay following the discovery of	Requires that regulations be issued by appropriate agencies regarding	No later than 30 days after the discovery of the breach, or as promptly as	Notice is required to be made without unreasonable delay following the discovery of a	The regulators under the S. 1897 are: (i) the FDIC,

Summary Comparison of Current Senate Data Security and Breach Notification Bills **2/25/2014**

Topic	S. 1193; (Toomey)	S. 1897 (Leahy)	S. 1927 (Carper/Blunt)	S. 1976 (Rockefeller)	S. 1995 (Blumenthal)	Comments
	discovery of a breach.	a security breach.	timing.	possible if the covered entity must delay past 30 days.	breach. No later than 48 hours after the FBI or Secret Service receives notice of a breach from a business entity.	Federal Reserve Board, (ii) National Credit Union Administration Board, (iii) SEC, (iv) CFTC, (v) Federal Housing Enterprise Oversight, (vi) the appropriate State insurance authority, and (vii) the FTC.
Method of Notification	Mail, telephone, or email or other electronic means.	Mail, telephone, or email if the individual consented to receive notice this way and the notice is consistent with E-SIGN.	Requires that the regulations issued by appropriate agencies to allow for written, telephone, or email notification.	Mail or email if the individual consented to receive notice this way and the notice is consistent with E-SIGN. Any method must be reasonably expected to reach the individual.	Mail, telephone, or by email unless the individual has expressly opted out or the notice is inconsistent with ESIGN.	The regulators under S. 1987 are: (i) the FDIC, Federal Reserve Board, (ii) National Credit Union Administration Board, (iii) SEC, (iv) CFTC, (v) Federal Housing Enterprise Oversight, (vi)

Summary Comparison of Current Senate Data Security and Breach Notification Bills **2/25/2014**

Topic	S. 1193; (Toomey)	S. 1897 (Leahy)	S. 1927 (Carper/Blunt)	S. 1976 (Rockefeller)	S. 1995 (Blumenthal)	Comments
						the appropriate State insurance authority, and (vii) the FTC.
Substitute Notice	"Excessive cost" or lack of sufficient contact information. Substitute notice would consist of conspicuous notice on a website or in print and major broadcast media in the geographic region of affected individuals.	Notice to the major media outlets if breach exceeds 5,000 residents of a state.	The regulations must also allow for substitute notification if there is a lack of contact information or providing other means of notice would be too costly.	Lack of sufficient contact information, or if data on less than 10,000 people is held by the breached entity and the cost of direct notice would be excessive. Conspicuous emails; Conspicuous posting on the entities website; and Notification to major media outlets.	If the breach was, or is reasonably believed to, include the more than 5,000 individuals. Prominent notice via all reasonable means of electronic contact. Notice to the major media in a state where more than 5,000 affected individuals reside.	The regulators under S. 1987 are: (i) the FDIC, Federal Reserve Board, (ii) National Credit Union Administration Board, (iii) SEC, (iv) CFTC, (v) Federal Housing Enterprise Oversight, (vi) the appropriate State insurance authority, and (vii) the FTC.
Content of Notification	(i) The date of the breach; (ii) A description of the information affected; and (iii) contact information for	(i) What information was affected; (ii) Toll-free numbers for from which an individual may	Requires regulations be issued by appropriate agencies regarding content.	(i) The date or date range of the breach; (ii) The type of information believed to be affected; (iii) Toll-free numbers to	**Written notice**: (i) The type of information affected, and how the entity came into possession of it; (ii) A toll-free	N/A

Topic	S. 1193; (Toomey)	S. 1897 (Leahy)	S. 1927 (Carper/Blunt)	S. 1976 (Rockefeller)	S. 1995 (Blumenthal)	Comments
	the covered entity	learn about the breach and what information was maintained; and (iii) Contact information for the major credit reporting agencies.		contact the entity; (iv) Notice of free credit reports and how to request them; (v) Toll-free number for the major credit agencies; and Contact information for the FTC.	phone number to contact the entity; (iii) Toll-free number, website, and address for the major credit agencies; (iv) Telephone numbers and websites for federal agencies that provide information regarding identity theft; (v) Notice about free credit reports, credit monitoring, and credit freeze and how to request such services; (vi) Notice that any damages resulting from the breach will be paid by the entity that was breached. **Telephone and public electronic notice** would not require as much information as the written notice.	
Notice to Credit	None	If notification is	Notify the	If notification is	If notification is	N/A

Summary Comparison of Current Senate Data Security and Breach Notification Bills **2/25/2014**

Topic	S. 1193; (Toomey)	S. 1897 (Leahy)	S. 1927 (Carper/Blunt)	S. 1976 (Rockefeller)	S. 1995 (Blumenthal)	Comments
Agencies		made to more than 5,000 individuals, consumer reporting agencies would be notified without unreasonable delay of the timing and distribution of the public notices.	consumer reporting agencies if the breach affected 5,000 or more consumers.	made to more than 5,000 individuals, consumer reporting agencies would be notified without unreasonable delay of the timing and distribution of the public notices.	made to more than 5,000 individuals, consumer reporting agencies would be notified without unreasonable delay of the timing and distribution of the public notices.	
Notice to Government/Law Enforcement	Notify the Secret Service FBI if a breach includes, or is reasonably believed to include more than 10,000 individuals.	Must notify a designated government entity of any breach of: (i) More than 5,000 individuals; (ii) Where the data is known to, or reasonably believed to have been accessed or acquired, from a database of more than 500,000	Must notify appropriate regulator. The regulators under the Bill are: (i) the FDIC, Federal Reserve Board, (ii) National Credit Union Administration Board, (iii) SEC, (iv) CFTC, (v) Federal Housing Enterprise Oversight, (vi) the	Notify a designated government entity of a breach that involves, or is reasonably believed to involve: (i) More than 5,000 individuals; (ii) Where the data is known to, or reasonably believed to have been accessed or acquired, from a database of more than 500,000	Notify a designated government entity of a breach that involves, or is reasonably believed to involve: (i) More than 5,000 individuals; (ii) Where the data is known to, or reasonably believed to have been accessed or acquired, from a database of more than 500,000	N/A

Summary Comparison of Current Senate Data Security and Breach Notification Bills **2/25/2014**

Topic	S. 1193; (Toomey)	S. 1897 (Leahy)	S. 1927 (Carper/Blunt)	S. 1976 (Rockefeller)	S. 1995 (Blumenthal)	Comments
		individuals; (iii) A database owned by the federal government; or (iv) That involves the information of employees or contractors involved in national security or law enforcement. Notification at least 72 hours before individual notice is sent or no later than 10 days after discovery.	appropriate State insurance authority, and (vii) the FTC.	individuals; (iii) A database owned by the federal government; or (iv) That involves the information of employees or contractors involved in national security or law enforcement.	individuals; (iii) A database owned by the federal government; or (iv) That involves the information of employees or contractors involved in national security or law enforcement. Notice delivered as promptly as possible, no later than 10 days after discovery.	
Delay Provisions	The Secret Service or FBI may delay notification if it would harm an ongoing investigation or the national	The Secret Service or FBI may delay notification if it would harm an ongoing investigation or the national	Regulations must allow for law enforcement delay where notification would harm an ongoing investigation the national security.	The Secret Service or FBI may delay notification if it would harm an ongoing investigation or the national security; and Reasonable	The Secret Service or FBI may delay notification if it would harm an ongoing investigation or the national security; and Reasonable time	The regulators under S. 1897 are: (i) the FDIC, Federal Reserve Board, (ii) National Credit

Summary Comparison of Current Senate Data Security and Breach Notification Bills **2/25/2014**

Topic	S. 1193; (Toomey)	S. 1897 (Leahy)	S. 1927 (Carper/Blunt)	S. 1976 (Rockefeller)	S. 1995 (Blumenthal)	Comments
	security; and Reasonable time needed to assess the breach and restore the system.	security; and Reasonable time needed to assess the breach and restore the system (not to exceed 60 days without FTC approval).		time needed to assess the breach and restore the system.	needed to assess the breach and restore the system.	Union Administration Board, (iii) SEC, (iv) CFTC, (v) Federal Housing Enterprise Oversight, (vi) the appropriate State insurance authority, and (vii) the FTC.
Criminal Penalties for Concealment of a Security Breach	None	Intentional concealment of a breach that results in economic harm of $1,000 or more to an individual. Violations are punishable by fines, up to 5 years in prison, or both.	None	Intentional concealment of a breach that results in economic harm of $1,000 or more to an individual. Violations are punishable by fines, up to 5 years in prison, or both.	Intentional concealment of a breach that results in economic harm or substantial emotional distress to 1 or more persons. Violations are punishable by fines, up to 5 years in prison, or both.	N/A
Civil Enforcement	A violation of the Bill would be treated as an unfair or deceptive act or practice and enforced by the	(i) The Attorney General; (ii) State attorneys general (if no Fed. action); Cap of $1,000,000 for	The appropriate regulator would be required to enforce the Bill. The regulators under the Bill are:	(i) The FTC would be authorized to enforce a violation as an unfair or deceptive act; (ii) State attorneys general if there is	(i) The Attorney General; (ii) State attorneys general (if no Fed. action); (iii) FTC; (iv) Private individual. Each section and enforcer	Only S. 1995 provides for a private right of action.

Summary Comparison of Current Senate Data Security and Breach Notification Bills **2/25/2014**

Topic	S. 1193; (Toomey)	S. 1897 (Leahy)	S. 1927 (Carper/Blunt)	S. 1976 (Rockefeller)	S. 1995 (Blumenthal)	Comments
	FTC. Penalty caps of $500,000 per section violated. .	the same act or omission. Additional $1,000,000 for willfulness. FTC may also enforce as an unfair or deceptive practice, subject to a $1,000,000 penalty cap, with an additional $1,000,000 if the act was willful.	(i) the FDIC, Federal Reserve Board, (ii) National Credit Union Administration Board, (iii) SEC, (iv) CFTC, (v) Federal Housing Enterprise Oversight, (vi) the appropriate State insurance authority, and (vii) the FTC.	no federal action pending. Penalty caps of $5,000,000 per section violated. The Attorney General may enforce the **law enforcement notification requirements**. Cap of $1,000,000, with an additional $1,000,000 for willfulness.	has different penalty caps.	
Preemption	Any state law relating to data security or breach notification.	Any state law relating to data security or breach notification. Nothing in the Bill will modify GLBA or HIPAA requirements.	Any state law relating to data security or breach notification.	Any state law relating to data security or breach notification. No limit on state common law of tort, contract, or fraud. No limit FTC authority.	Any state law relating to data security or breach notification. No limit on state common law of tort, contract, or fraud.	N/A
Credit Monitoring or	None	None	None	Free credit report provided for by the	Free credit report provided for by the	N/A

Summary Comparison of Current Senate Data Security and Breach Notification Bills **2/25/2014**

Topic	S. 1193; (Toomey)	S. 1897 (Leahy)	S. 1927 (Carper/Blunt)	S. 1976 (Rockefeller)	S. 1995 (Blumenthal)	Comments
Reports				breached entity quarterly for two years after a request is made. May not be required depending on type of information breached.	breached entity quarterly for two years after a request is made. Free credit monitoring provided for by the breached entity quarterly for two years after a request is made. Free credit freeze provided for by the breached entity that will remain in place until the individual requests its removal.	