S 1408

Data Breach Notification Act of 2011

Congress: 112 (2011–2013, Ended)
Chamber: Senate
Policy Area: Crime and Law Enforcement
Introduced: Jul 22, 2011
Current Status: Placed on Senate Legislative Calendar under General Orders. Calendar No. 310.
Latest Action: Placed on Senate Legislative Calendar under General Orders. Calendar No. 310. (Feb 6, 2012)
Official Text: https://www.congress.gov/bill/112th-congress/senate-bill/1408

Sponsor

Name: Sen. Feinstein, Dianne [D-CA]
Party: Democratic • **State:** CA • **Chamber:** Senate

Cosponsors

No cosponsors are listed for this bill.

Committee Activity

Committee	Chamber	Activity	Date
Judiciary Committee	Senate	Reported By	Feb 6, 2012

Subjects & Policy Tags

Policy Area:

Crime and Law Enforcement

Related Bills

Bill	Relationship	Last Action
112 S 1151	Related bill	**Nov 7, 2011:** By Senator Leahy from Committee on the Judiciary filed written report. Report No. 112-91. Additional and Minority views filed.
112 S 1535	Related bill	**Sep 22, 2011:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 182.

Summary (as of Feb 6, 2012)

Data Breach Notification Act of 2011 - (Sec. 2) Requires any federal agency or business entity engaged in interstate commerce that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information, following the discovery of a security breach, to notify: (1) any U.S. resident whose information has been, or is reasonably believed to have been, accessed or acquired; and (2) any owner or licensee of such information. Requires notifications to be made without unreasonable delay following the discovery of a security breach. Allows a delay of notification for law enforcement and national security purposes if written justification for such delay is provided to the Secretary of Homeland Security (DHS) by the U.S. Secret Service and to the Attorney General by the Federal Bureau of Investigation (FBI).

(Sec. 3) Exempts agencies or business entities from notification requirements if: (1) the Secret Service or the FBI determines that notification of a security breach could reveal sensitive sources and methods or impede law enforcement or intelligence investigations, or the FBI determines that such notification may damage national security; (2) a risk assessment concludes that there is no significant risk that a security breach has resulted in, or will result in, identity theft, economic loss or harm, or physical harm to individuals whose sensitive personally identifiable information was subject to the security breach; (3) an agency or business entity notifies the Federal Trade Commission (FTC) of intent to invoke a risk assessment exemption; or (4) a business entity participates in a security program that effectively blocks the use of sensitive personally identifiable information and provides for notice to affected individuals of a security breach.

(Sec. 4) Requires: (1) written notice of a security breach to individuals by mail, telephone, and e-mail; and (2) notice to major media outlets if a security breach involves more than 5,000 individuals.

(Sec. 5) Requires a notification of a security breach to include: (1) a description of the categories of sensitive personally identifiable information acquired by an unauthorized person, (2) a toll-free telephone number for contacting an agency or business entity to ascertain the types of personal information maintained by such agency or entity, and (3) the toll-free telephone numbers and addresses for the major credit reporting agencies. Authorizes a state to require that a notification also include information about victim protection assistance provided by that state.

(Sec. 6) Directs an agency or business entity that is required to provide notification to more than 5,000 individuals to also notify all nationwide consumer reporting agencies of the timing and distribution of the notices.

(Sec. 7) Requires the DHS Secretary to designate a federal government entity to receive notices of security breaches (designated entity). Requires such designated entity to provide the notices and other information it receives to the Secret Service, the FBI, the FTC, the U.S. Postal Inspection Service (if fraud is involved), state attorneys general, and other federal law enforcement agencies.

Requires any business entity or agency to notify the designated entity of a security breach if: (1) the number of individuals whose sensitive personally identifying information was acquired by an unauthorized person exceeds 10,000, (2) the breach involves a data system containing information on more than 1 million individuals nationwide, (3) the breach involves databases owned by the federal government, or (4) the breach involves primarily sensitive personally identifiable information of individuals known to be employees and contractors of the federal government involved in national security or law enforcement.

(Sec. 8) Authorizes the Attorney General to bring civil and administrative actions against business entities for violations of this Act and to seek injunctive relief or civil penalties, including increased penalties for willful or intentional violations.

(Sec. 9) Authorizes state attorneys general or state or local law enforcement agencies to bring a civil action on behalf of

state residents who have been threatened or adversely affected by a business entity violating provisions of this Act and to obtain injunctive relief or civil penalties. Requires a state attorney general bringing a civil action to provide written notice to the Attorney General who may then move to stay the action, move to consolidate all pending actions, intervene, and file petitions for appeal.

(Sec. 10) Amends the federal criminal code to impose a prison term of up to five years and/or a fine on any individual who has knowledge of a security breach and intentionally and willfully conceals such breach, resulting in economic harm of $1,000 or more to any individual. Grants the Secret Service and the FBI authority to investigate criminal concealments of security breaches.

(Sec. 11) Provides that this Act shall supersede any other provision of federal law (except the data security requirements of the Gramm-Leach-Bliley Act and certain health privacy provisions) or state law relating to notification by an interstate business entity or agency of a security breach.

(Sec. 12) Authorizes appropriations for the cost of investigations, risk assessments, and civil actions relating to security breaches under this Act.

(Sec. 13) Directs the FTC, not later than 18 months after the enactment of this Act, to report on: (1) the number and nature of the security breaches described in notices filed by business entities invoking the risk assessment exemption under this Act, and (2) the response of the FTC to such notices. Excludes from such report the contents of any risk assessment provided to the FTC.

Directs the Secret Service and FBI, not later than 18 months after the enactment of this Act, to report on the number and nature of security breaches subject to the national security and law enforcement exemptions under this Act.

(Sec. 14) Sets forth definitions for purposes of this Act, including a definition of "sensitive personally identifiable information."

Actions Timeline

- **Feb 6, 2012:** Committee on the Judiciary. Reported by Senator Leahy with an amendment in the nature of a substitute. Without written report.
- **Feb 6, 2012:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 310.
- **Sep 22, 2011:** Committee on the Judiciary. Ordered to be reported with an amendment in the nature of a substitute favorably.
- **Jul 22, 2011:** Introduced in Senate
- **Jul 22, 2011:** Sponsor introductory remarks on measure. (CR S4846-4847)
- **Jul 22, 2011:** Read twice and referred to the Committee on the Judiciary. (text of measure as introduced: CR S4847-4849)