S 239

Notification of Risk to Personal Data Act of 2007

Congress: 110 (2007–2009, Ended)
Chamber: Senate
Policy Area: Crime and Law Enforcement
Introduced: Jan 10, 2007
Current Status: Placed on Senate Legislative Calendar under General Orders. Calendar No. 180.
Latest Action: Placed on Senate Legislative Calendar under General Orders. Calendar No. 180. (May 31, 2007)
Official Text: https://www.congress.gov/bill/110th-congress/senate-bill/239

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	May 31, 2007

Subjects & Policy Tags

Policy Area:

Crime and Law Enforcement

Related Bills

No related bills are listed.

Summary (as of May 31, 2007)

Notification of Risk to Personal Data Act of 2007 - (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 may have been accessed or acquired; and (2) the owner or licensee of any such information that the agency or business does not own or license.

(Sec. 3) Exempts: (1) agencies and business entities from notification requirements for national security and law enforcement purposes and for security breaches that a risk assessment concludes do not have a significant risk of resulting in harm if specified certification or notice is provided, which is subject to review by the U.S. Secret Service; and (2) business entities from notification requirements if such an entity utilizes a security program that blocks the use of sensitive personally identifiable information to initiate unauthorized financial transactions and provides notice of a breach to affected individuals. Sets forth a presumption that there was no significant risk of harm to an individual whose sensitive personally identifiable information was subject to a security breach if such information: (1) was encrypted; or (2) was rendered indecipherable through the use of best practices or methods, such as redaction, access controls, or other such mechanisms, that are widely accepted as an effective industry practice, or an effective industry standard.

(Sec. 4) Provides that an agency or business entity shall be in compliance with such requirements if it provides both individual notice and media notice.

(Sec. 5) Requires notice to include: (1) a description of the categories of sensitive personally identifiable information acquired by an unauthorized person; (2) a toll-free number that the individual may use to contact the agency or business entity to learn what types of personal information the agency or entity maintained; and (3) the toll-free telephone numbers and addresses for the major credit reporting agencies. Authorizes a state to require that a notice also include information regarding 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 any business entity or agency to notify the Secret Service of the fact that a security breach has occurred 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 the agency or business entity to be employees and contractors of the federal government involved in national security or law enforcement.

Requires notifications regarding security breaches under specified circumstances to the Secret Service, the Federal Bureau of Investigation, the United States Postal Inspection Service, and state attorneys general.

(Sec. 8) Authorizes the Attorney General to bring a civil action in U.S. district court against any business entity that violates this Act. Sets daily and maximum civil penalties for violations by a business entity.

Amends the Fair Credit Reporting Act to require agencies to include a fraud alert in the file of a consumer that submits evidence of compromised financial information to a consumer reporting agency.

(Sec. 9) Authorizes civil actions by state attorneys general to enforce this Act.

(Sec. 10) Provides that this Act shall not supersede any other provision of federal law or of state law relating to notification by a business entity engaged in interstate commerce or an agency of a security breach.

(Sec. 11) Authorizes appropriations for costs incurred by the Secret Service to investigate and conduct risk assessments of security breaches.

(Sec. 12) Directs the Secret Service to report to Congress on the number and nature of security breaches: (1) described in the notices filed by those business entities invoking the risk assessment exemption; and (2) subject to the national security and law enforcement exemptions. Prohibits any report submitted from disclosing the contents of any risk assessment provided to the Secret Service under this Act.

Actions Timeline

- **May 31, 2007:** Committee on the Judiciary. Reported by Senator Leahy under authority of the order of the Senate of 05/25/2007 with an amendment in the nature of a substitute. Without written report.
- **May 31, 2007:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 180.
- **May 3, 2007:** Committee on the Judiciary. Ordered to be reported with an amendment in the nature of a substitute favorably.
- **Jan 10, 2007:** Introduced in Senate
- **Jan 10, 2007:** Sponsor introductory remarks on measure. (CR S378-379)
- **Jan 10, 2007:** Read twice and referred to the Committee on the Judiciary. (text of measure as introduced: CR S379-381)