S 3333

Data Security and Breach Notification Act of 2012

Congress: 112 (2011–2013, Ended)
Chamber: Senate
Policy Area: Commerce
Introduced: Jun 21, 2012
Current Status: Read twice and referred to the Committee on Commerce, Science, and Transportation.
Latest Action: Read twice and referred to the Committee on Commerce, Science, and Transportation. (Jun 21, 2012)
Official Text: https://www.congress.gov/bill/112th-congress/senate-bill/3333

Sponsor

Name: Sen. Toomey, Patrick [R-PA]
Party: Republican • **State:** PA • **Chamber:** Senate

Cosponsors (5 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Blunt, Roy [R-MO]	R · MO		Jun 21, 2012
Sen. DeMint, Jim [R-SC]	R · SC		Jun 21, 2012
Sen. Heller, Dean [R-NV]	R · NV		Jun 21, 2012
Sen. Snowe, Olympia J. [R-ME]	R · ME		Jun 21, 2012
Sen. Rubio, Marco [R-FL]	R · FL		Jul 11, 2012

Committee Activity

Committee	Chamber	Activity	Date
Commerce, Science, and Transportation Committee	Senate	Referred To	Jun 21, 2012

Subjects & Policy Tags

Policy Area:

Commerce

Related Bills

No related bills are listed.

Summary (as of Jun 21, 2012)

Data Security and Breach Notification Act of 2012 - Requires commercial entities that acquire, maintain, store, or utilize personal information (covered entities) to take reasonable measures to protect and secure data in electronic form containing personal information.

Directs a covered entity that owns or licenses such data to give notice of any breach of the security of the system that the entity reasonably believes has caused or will cause identity theft or other financial harm to each individual: (1) who is a U.S. citizen or resident; and (2) whose personal information was, or that the covered entity reasonably believes has been, accessed and acquired by an unauthorized person.

Requires a covered entity to notify the Secret Service or the Federal Bureau of Investigation (FBI) of a security breach of personal information involving more than 10,000 individuals.

Requires a third-party entity contracted to maintain, store, or process data containing personal information to notify the covered entity of a breach of security of a system. Requires a service provider to notify the covered entity if it becomes aware of a breach of security involving personal information owned or possessed by a covered entity and if such covered entity can be reasonably identified.

Allows delays of notifications to avoid impeding a civil or criminal investigation or threatening national or homeland security.

Sets forth the methods for notification under this Act.

Preempts information security practices of the Communications Act applicable to telecommunication carriers, satellite operators, and cable operators.

Sets forth civil monetary penalties for violations of this Act.

Exempts financial institutions and entities subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Actions Timeline

- **Jun 21, 2012:** Introduced in Senate
- **Jun 21, 2012:** Read twice and referred to the Committee on Commerce, Science, and Transportation.