S 177

Data Security and Breach Notification Act of 2015

Congress: 114 (2015–2017, Ended)
Chamber: Senate
Policy Area: Commerce
Introduced: Jan 13, 2015
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. (Jan 13, 2015)
Official Text: https://www.congress.gov/bill/114th-congress/senate-bill/177

Sponsor

Name: Sen. Nelson, Bill [D-FL]
Party: Democratic • **State:** FL • **Chamber:** Senate

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Blumenthal, Richard [D-CT]	D · CT		Apr 20, 2015

Committee Activity

Committee	Chamber	Activity	Date
Commerce, Science, and Transportation Committee	Senate	Referred To	Jan 13, 2015

Subjects & Policy Tags

Policy Area:

Commerce

Related Bills

No related bills are listed.

Summary (as of Jan 13, 2015)

Data Security and Breach Notification Act of 2015

Requires the Federal Trade Commission (FTC) to promulgate regulations requiring commercial entities, nonprofit and for-profit corporations, estates, trusts, cooperatives, and other specified entities that own or possess data containing personal information (covered entities), or that contract to have a third-party maintain or process such data for the entity, to implement information security policies and procedures for the treatment and protection of personal information.

Establishes procedures to be followed in the event of an information security breach. Requires a covered entity that discovers a breach to notify the FTC (unless the covered entity has already notified a federal entity designated by the Department of Homeland Security [DHS] to receive such information) and affected individuals. Sets forth requirements concerning such notification, including methods of notification and timeliness requirements. Allows an exemption from notification requirements if such entity reasonably concludes that there is no reasonable risk of identity theft, fraud, or other unlawful conduct. Establishes a presumption that there is no such risk for encrypted data.

Directs DHS to designate a federal entity that covered entities would be required to notify if a security breach involves: (1) the personal information of more than 10,000 individuals, (2) a database containing the personal information of more than 1 million individuals, (3) federal government databases, or (4) the personal information of federal employees or contractors known to be involved in national security or law enforcement.

Requires the designated entity to provide each notice it receives to:

- the U.S. Secret Service;
- the Federal Bureau of Investigation;
- the FTC;
- the U.S. Postal Inspection Service, if mail fraud is involved;
- attorneys general of affected states; and
- appropriate federal agencies for law enforcement, national security, or data security purposes.

Sets forth enforcement provisions for the FTC, state attorneys general, and the Attorney General.

Establishes criminal penalties of a fine, imprisonment for up to five years, or both, for concealment of a security breach that results in economic harm of at least $1,000 to an individual.

Actions Timeline

- **Jan 13, 2015:** Introduced in Senate
- **Jan 13, 2015:** Read twice and referred to the Committee on Commerce, Science, and Transportation.