

S 3742

Data Security and Breach Notification Act of 2010

Congress: 111 (2009–2011, Ended)

Chamber: Senate

Policy Area: Commerce

Introduced: Aug 5, 2010

Current Status: Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety

Latest Action: Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety, and Insurance . Hearings held. With printed Hearing: S.Hrg. 111-1040. (Sep 22, 2010)

Official Text: <https://www.congress.gov/bill/111th-congress/senate-bill/3742>

Sponsor

Name: Sen. Pryor, Mark L. [D-AR]

Party: Democratic • **State:** AR • **Chamber:** Senate

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Rockefeller, John D., IV [D-WV]	D · WV		Aug 5, 2010

Committee Activity

Committee	Chamber	Activity	Date
Commerce, Science, and Transportation Committee	Senate	Hearings By (subcommittee)	Sep 22, 2010

Subjects & Policy Tags

Policy Area:

Commerce

Related Bills

Bill	Relationship	Last Action
111 HR 2221	Related bill	Dec 9, 2009: Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation.

Data Security and Breach Notification Act of 2010 - Requires the Federal Trade Commission (FTC) to promulgate regulations requiring each covered entity (proprietorships, partnerships, estates, trusts, cooperatives, and nonprofit and for-profit corporations) engaged in interstate commerce owning or possessing data containing personal information to establish specified security policies and procedures to treat and protect such information.

Requires the regulations to include methods for disposing of both electronic and nonelectronic data.

Requires information brokers to submit their security policies to the FTC in conjunction with a notification of a security breach notification or on FTC request. Authorizes the FTC to conduct information security practices audits of brokers or require brokers to conduct independent audits.

Requires information brokers to: (1) establish procedures to verify the accuracy of information that identifies individuals; (2) provide to individuals whose personal information it maintains a means to review it; (3) place a conspicuous notice on the Internet instructing individuals how to request access to such information; and (4) correct inaccurate information.

Directs the FTC to require information brokers to establish measures which facilitate the auditing or retracing of access to, or transmissions of, any data containing personal information.

Makes it unlawful for information brokers to obtain or disclose personal information by false pretenses (pretexting).

Requires a covered entity to notify the FTC and affected individuals of information security breaches. Sets forth requirements concerning such notification, including method of notification requirements and timeliness requirements. Allows an exemption from notification requirements if the covered entity determines that there is no reasonable risk of identity theft, fraud, or other unlawful conduct.

Preempts state information security laws.

Actions Timeline

- **Sep 22, 2010:** Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety, and Insurance . Hearings held. With printed Hearing: S.Hrg. 111-1040.
- **Aug 5, 2010:** Introduced in Senate
- **Aug 5, 2010:** Read twice and referred to the Committee on Commerce, Science, and Transportation.