HR 4187

Secure and Protect Americans' Data Act

Congress: 114 (2015–2017, Ended)
Chamber: House
Policy Area: Commerce
Introduced: Dec 8, 2015
Current Status: Referred to the Subcommittee on Commerce, Manufacturing, and Trade.
Latest Action: Referred to the Subcommittee on Commerce, Manufacturing, and Trade. (Dec 11, 2015)
Official Text: https://www.congress.gov/bill/114th-congress/house-bill/4187

Sponsor

Name: Rep. Schakowsky, Janice D. [D-IL-9]
Party: Democratic • **State:** IL • **Chamber:** House

Cosponsors (8 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Butterfield, G. K. [D-NC-1]	D · NC		Dec 8, 2015
Rep. Kennedy, Joseph P., III [D-MA-4]	D · MA		Dec 8, 2015
Rep. Pallone, Frank, Jr. [D-NJ-6]	D · NJ		Dec 8, 2015
Rep. Rush, Bobby L. [D-IL-1]	D · IL		Dec 8, 2015
Rep. Sarbanes, John P. [D-MD-3]	D · MD		Dec 8, 2015
Rep. Tonko, Paul [D-NY-20]	D · NY		Dec 8, 2015
Rep. Welch, Peter [D-VT-At Large]	D · VT		Dec 8, 2015
Rep. Kelly, Robin L. [D-IL-2]	D · IL		Nov 14, 2016

Committee Activity

Committee	Chamber	Activity	Date
Energy and Commerce Committee	House	Referred to	Dec 11, 2015

Subjects & Policy Tags

Policy Area:

Commerce

Related Bills

No related bills are listed.

Summary (as of Dec 8, 2015)

Secure and Protect Americans' Data Act

This bill requires the Federal Trade Commission (FTC) to promulgate regulations requiring entities regulated by the FTC, common carriers, and nonprofit organizations to establish information security practices for the treatment and protection of personal information.

At least annually, such entities must evaluate their consumer privacy programs to make any appropriate adjustments for changing technologies, threats or vulnerabilities, or business arrangements.

The bill sets forth special procedures for information brokers to: (1) submit security policies to the FTC, (2) provide for post-breach audits, and (3) establish procedures for individuals to review and correct inaccuracies in their personal information. In lieu of procedures that allow individuals to dispute information, an information broker may provide individuals a means of expressing a preference not to have their information used for marketing purposes.

The bill prohibits information brokers from obtaining or disclosing personal information by false pretenses.

Within 10 days following discovery of a security breach, entities must notify:

- the FTC;
- the Federal Bureau of Investigation;
- the U.S. Secret Service;
- for common carriers, the Federal Communications Commission (FCC); and
- attorneys general of affected states.

Within 30 days following a breach, entities must notify individuals who are U.S. citizens or residents whose personal information was, or is reasonably believed to have been, acquired or accessed by an unauthorized person, or used for an unauthorized purpose.

If an entity is required to notify more than 5,000 individuals, the entity must also notify major consumer reporting agencies. An entity must provide notices in print and broadcast media if the affected residents of a state exceed 5,000.

Notices must include information on affected individuals' entitlement to consumer credit reports or credit monitoring services.

The bill exempts entities from notification requirements if the data is unusable, unreadable, or indecipherable.

Entities complying with other federal laws that require substantially similar information security procedures or breach notifications are deemed to be in compliance with the FTC's procedures or the notification requirements of this Act.

Enforcement authority is provided to the FTC and states. States may obtain civil penalties for certain violations.

Actions Timeline

- **Dec 11, 2015:** Referred to the Subcommittee on Commerce, Manufacturing, and Trade.
- **Dec 8, 2015:** Introduced in House
- **Dec 8, 2015:** Referred to the House Committee on Energy and Commerce.