S 1027

Data Breach Notification and Punishing Cyber Criminals Act of 2015

Congress: 114 (2015–2017, Ended)
Chamber: Senate
Policy Area: Commerce
Introduced: Apr 21, 2015
Current Status: Read twice and referred to the Committee on Commerce, Science, and Transportation. (Sponsor introduc
Latest Action: Read twice and referred to the Committee on Commerce, Science, and Transportation. (Sponsor introductory remarks on measure: CR S2304) (Apr 21, 2015)
Official Text: https://www.congress.gov/bill/114th-congress/senate-bill/1027

Sponsor

Name: Sen. Kirk, Mark Steven [R-IL]
Party: Republican • **State:** IL • **Chamber:** Senate

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Gillibrand, Kirsten E. [D-NY]	D · NY		Apr 21, 2015

Committee Activity

Committee	Chamber	Activity	Date
Commerce, Science, and Transportation Committee	Senate	Referred To	Apr 21, 2015

Subjects & Policy Tags

Policy Area:

Commerce

Related Bills

No related bills are listed.

Summary (as of Apr 21, 2015)

Data Breach Notification and Punishing Cyber Criminals Act of 2015

Requires certain commercial entities that acquire, maintain, store, or utilize individuals' nonpublic personal information to protect and secure any such data that is held unencrypted in electronic form.

Directs entities that own or license such data, following discovery of a security breach, to notify each individual U.S. citizen or resident: (1) whose personal information is reasonably believed to have been accessed and acquired by an unauthorized person; or (2) who may be at risk of identity theft, fraud, actual financial harm, or other unlawful conduct.

Requires the Department of Homeland Security (DHS) to designate a federal entity to receive information from commercial entities regarding breaches, incidents, threats, and vulnerabilities. Requires the DHS-designated entity to provide such information to: (1) the U.S. Secret Service and the Federal Bureau of Investigation; (2) the Federal Trade Commission (FTC) for civil law enforcement purposes; and (3) other federal agencies for law enforcement, national security, or data security purposes.

Directs entities to notify the DHS-designated entity if a breach involves: (1) the personal information of more than 1,000 individuals, (2) a data system containing the personal information of more than 250,000 individuals, (3) federal databases, or (4) the personal information of primarily federal employees and contractors involved in national security or law enforcement.

Provides alternative compliance procedures for: (1) third parties that maintain personal data in electronic form on behalf of another entity, and (2) certain electronic data service providers.

Sets forth FTC enforcement authority.

Exempts from the requirements of this Act: (1) financial institutions subject to the Gramm-Leach-Bliley Act, and (2) entities subject to health information privacy regulations. Provides for the requirements of this Act to apply to certain entities in place of security practices and notification standards currently enforced by the Federal Communications Commission.

Increases maximum fines or terms of imprisonment for certain cyber-related criminal offenses involving identity theft or fraud.

Directs the Department of State to consult with governments of countries in which international cyber criminals are physically present (if the countries do not have a mutual legal assistance or an extradition treaty with the United States) to determine what actions those governments have taken to prosecute and prevent cyber or intellectual property crimes against U.S. interests or citizens.

Preempts certain state data security laws.

Actions Timeline

- **Apr 21, 2015:** Introduced in Senate
- **Apr 21, 2015:** Read twice and referred to the Committee on Commerce, Science, and Transportation. (Sponsor introductory remarks on measure: CR S2304)