HR 2205

Data Security Act of 2015

Congress: 114 (2015–2017, Ended)
Chamber: House
Policy Area: Finance and Financial Sector
Introduced: May 1, 2015
Current Status: Reported (Amended) by the Committee on Financial Services. H. Rept. 114-867, Part I.
Latest Action: Reported (Amended) by the Committee on Financial Services. H. Rept. 114-867, Part I. (Dec 12, 2016)
Official Text: https://www.congress.gov/bill/114th-congress/house-bill/2205

Sponsor

Name: Rep. Neugebauer, Randy [R-TX-19]
Party: Republican • **State:** TX • **Chamber:** House

Cosponsors (41 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Carney, John C., Jr. [D-DE-At Large]	D · DE		May 1, 2015
Rep. Maloney, Carolyn B. [D-NY-12]	D · NY		May 14, 2015
Rep. Pittenger, Robert [R-NC-9]	R · NC		May 14, 2015
Rep. Royce, Edward R. [R-CA-39]	R · CA		May 19, 2015
Rep. King, Peter T. [R-NY-2]	R · NY		May 21, 2015
Rep. Meeks, Gregory W. [D-NY-5]	D · NY		Jun 1, 2015
Rep. Hinojosa, Ruben [D-TX-15]	D · TX		Jun 2, 2015
Rep. Messer, Luke [R-IN-6]	R · IN		Jun 2, 2015
Rep. Scott, David [D-GA-13]	D · GA		Jun 2, 2015
Rep. Barr, Andy [R-KY-6]	R · KY		Jul 10, 2015
Rep. Poe, Ted [R-TX-2]	R · TX		Jul 10, 2015
Rep. Walz, Timothy J. [D-MN-1]	D · MN		Jul 10, 2015
Rep. Bishop, Mike [R-MI-8]	R · MI		Jul 15, 2015
Rep. Marchant, Kenny [R-TX-24]	R · TX		Jul 15, 2015
Rep. Murphy, Patrick [D-FL-18]	D · FL		Jul 27, 2015
Rep. Lummis, Cynthia M. [R-WY-At Large]	R · WY		Jul 29, 2015
Rep. Jenkins, Lynn [R-KS-2]	R · KS		Sep 15, 2015
Rep. Sherman, Brad [D-CA-30]	D · CA		Sep 17, 2015
Rep. Garamendi, John [D-CA-3]	D · CA		Sep 24, 2015
Rep. Kaptur, Marcy [D-OH-9]	D · OH		Sep 24, 2015
Rep. Moolenaar, John R. [R-MI-4]	R · MI		Oct 7, 2015
Rep. Napolitano, Grace F. [D-CA-32]	D · CA		Oct 7, 2015
Rep. Luetkemeyer, Blaine [R-MO-3]	R · MO		Oct 21, 2015
Rep. Wilson, Joe [R-SC-2]	R · SC		Oct 22, 2015
Rep. Young, Don [R-AK-At Large]	R · AK		Oct 22, 2015
Rep. Abraham, Ralph Lee [R-LA-5]	R · LA		Nov 5, 2015
Rep. Aguilar, Pete [D-CA-31]	D · CA		Nov 5, 2015
Rep. Black, Diane [R-TN-6]	R · TN		Nov 5, 2015
Rep. Rothfus, Keith J. [R-PA-12]	R · PA		Nov 19, 2015
Rep. Collins, Chris [R-NY-27]	R · NY		Dec 11, 2015
Rep. Fortenberry, Jeff [R-NE-1]	R · NE		Dec 11, 2015
Rep. Moulton, Seth [D-MA-6]	D · MA		Dec 11, 2015
Rep. Ashford, Brad [D-NE-2]	D · NE		Mar 15, 2016
Rep. McClintock, Tom [R-CA-4]	R · CA		Mar 15, 2016
Rep. Miller, Candice S. [R-MI-10]	R · MI		Mar 15, 2016
Rep. Rangel, Charles B. [D-NY-13]	D · NY		Mar 15, 2016
Rep. Hice, Jody B. [R-GA-10]	R · GA		Apr 12, 2016
Rep. Smith, Lamar [R-TX-21]	R · TX		Apr 12, 2016
Rep. Larsen, Rick [D-WA-2]	D · WA		Apr 14, 2016
Rep. McKinley, David B. [R-WV-1]	R · WV		Jun 10, 2016
Rep. Young, David [R-IA-3]	R · IA		Jul 5, 2016

Committee Activity

Committee	Chamber	Activity	Date
Energy and Commerce Committee	House	Referred to	May 8, 2015
Financial Services Committee	House	Reported By	Dec 12, 2016

Subjects & Policy Tags

Policy Area:

Finance and Financial Sector

Related Bills

Bill	Relationship	Last Action
114 S 961	Related bill	**Apr 15, 2015:** Read twice and referred to the Committee on Commerce, Science, and Transportation.

Summary (as of Dec 12, 2016)

Data Security Act of 2015

(Sec. 4) This bill requires individuals, corporations, or other non-government entities that access, maintain, communicate, or handle sensitive financial account information or nonpublic personal information to: (1) implement an information security program to protect the security and confidentiality of such information against anticipated threats, hazards, or unauthorized acquisitions; and (2) notify consumers, state and federal law enforcement, appropriate administrative agencies, payment card networks, and consumer reporting agencies of certain data breaches of sensitive information that is not encrypted, redacted, or protected and is likely to cause harm to the consumers.

The types of sensitive information subject to this bill include:

- consumer financial account numbers (including credit or debit card numbers) in combination with security codes, passwords, or personal identification information required to access an account;
- non-truncated Social Security numbers;
- the first name or initial and last name of a consumer in combination with numbers issued on government documents used to verify identity (e.g., driver's license, passport, or military identification numbers), usernames and passwords for email or consumer accounts, or consumer biometric data used to gain access to financial accounts; and
- medical and health insurance information.

The requirements of this bill do not apply to information lawfully made available to the general public that is obtained from government records or widely distributed media.

The entities subject to this bill must: (1) designate employees to coordinate their information security programs; (2) identify reasonably foreseeable internal and external risks; (3) assess, design, and implement safeguards; (4) oversee their third-party service providers; and (5) adjust security in light of risk assessments, testing, changes to operations or business arrangements, or other circumstances that may impact the security program.

Entities must require their third-party service providers by contract to implement appropriate safeguards and assess compliance with such contractual obligations.

If appropriate, entities must adopt:

- access controls and authentication procedures for information systems;
- access restrictions at physical locations;
- encryption of electronic information;
- procedures to ensure that any information system modifications are consistent with security programs;
- dual control procedures, segregation of duties, and criminal background checks for employees with access to sensitive information;
- monitoring systems to detect intrusions;
- response programs that specify actions to be taken when an entity suspects or detects unauthorized access; and
- measures to protect against destruction of information due to fire, water damage, or technological failures.

If an entity has a board of directors: (1) the board must direct the entity to have a written information security program in place and appoint personnel to oversee the program, and (2) an annual report shall be made to the board describing the

status and implementation of the entity's security program.

Entities must investigate data breaches they believe may have occurred in relation to the sensitive information they handle or that is handled on their behalf. If an entity determines that an unauthorized acquisition is reasonably likely to harm consumers, the entity must notify within the most expedient time possible:

- federal and state law enforcement;
- the Federal Trade Commission (FTC) or the appropriate federal or state administrative enforcement agency designated to enforce this bill with respect to banks or other financial institutions;
- payment card networks, if the breach involves card numbers;
- consumer reporting agencies, if the breach involves 5,000 or more consumers; and
- all consumers to whom the sensitive information relates.

An entity's notice to consumers about a breach must be provided by telephone, email, or written notification to a postal address. An entity may use a substitute notification method in print and to broadcast media if telephonic, email, or written notification is infeasible because of: (1) insufficient contact information, (2) costs exceeding $250,000, (3) the number of consumers exceeding 500,000, or (4) exigent circumstances.

Notifications may be delayed at the request of a law enforcement agency.

Third-party service providers contracted to maintain, store, or process data in electronic form on behalf of another entity must provide notice regarding a breach to: (1) such entity, and (2) consumers if so provided under the contract.

Certain electronic data carriers that provide only transmission, routing, transient storage, or network connection services must notify entities that initiate connections or transmissions that become involved in a breach involving sensitive information if: (1) the carrier becomes aware of the breach, and (2) the entity that owns or licenses the information can be reasonably identified. The entity that initiated the connection must then provide the required notices under this bill.

Financial institutions may communicate with account holders regarding breaches at other entities with access to their account information.

The bill provides alternative compliance procedures for: (1) financial institutions and affiliates under the Gramm-Leach-Bliley Act, and (2) entities complying with certain health record privacy laws under the Health Information Technology for Economic and Clinical Health Act or regulations under the Health Insurance Portability and Accountability Act of 1996.

(Sec. 5) The bill designates the federal or state administrative enforcement agencies responsible for enforcing compliance with this bill by banks, financial institutions, or entities that are not financial institutions. Depending on the type of entity, the enforcement must be conducted by the FTC, the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the National Credit Union Administration Board, the Securities and Exchange Commission, the Commodity Futures Trading Commission, the Federal Housing Finance Agency, state insurance regulators, the state of domicile, or state securities commissioners.

Cable operators, satellite operators, or telecommunications carriers whose information security practices are subject to enforcement under this bill are exempt from certain other information security and breach notification requirements under the Communications Act of 1934 and regulations promulgated by the Federal Communications Commission.

State attorneys general may enforce this bill with respect to entities that are not financial institutions.

(Sec. 6) No state law, regulatory requirement, or prohibition may be imposed with respect to the responsibilities of any

person to: (1) protect the security of consumer information, (2) safeguard consumer information from unauthorized access or acquisition, (3) investigate or provide notice of unauthorized acquisition or access, or (4) mitigate any potential or actual loss or harm resulting from unauthorized acquisition or access of consumer information.

Actions Timeline

- **Dec 12, 2016:** Reported (Amended) by the Committee on Financial Services. H. Rept. 114-867, Part I.
- **Dec 9, 2015:** Committee Consideration and Mark-up Session Held.
- **Dec 9, 2015:** Ordered to be Reported (Amended) by the Yeas and Nays: 46 - 9.
- **Dec 8, 2015:** Committee Consideration and Mark-up Session Held.
- **May 8, 2015:** Referred to the Subcommittee on Commerce, Manufacturing, and Trade.
- **May 1, 2015:** Introduced in House
- **May 1, 2015:** Referred to the Committee on Energy and Commerce, and in addition to the Committee on Financial Services, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.