114TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 114–867
Part 1

DATA SECURITY ACT OF 2015

DECEMBER 12, 2016.—Ordered to be printed

Mr. HENSARLING, from the Committee on Financial Services, submitted the following

R E P O R T

together with

MINORITY VIEWS

[To accompany H.R. 2205]

[Including cost estimate of the Congressional Budget Office]

The Committee on Financial Services, to whom was referred the bill (H.R. 2205) to protect financial information relating to consumers, to require notice of security breaches, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Data Security Act of 2015".

SEC. 2. PURPOSES.

The purposes of this Act are—

(1) to establish strong and uniform national data security and breach notification standards for electronic data;

(2) to expressly preempt any related laws of a State, the District of Columbia, or a territory of the United States; and

(3) to provide the Federal Trade Commission with authority to enforce such standards for entities covered under this Act that are not otherwise regulated by one of the enumerated enforcement agencies in the Act.

SEC. 3. DEFINITIONS.

For purposes of this Act, the following definitions shall apply:

(1) AFFILIATE.—The term "affiliate" means any company that controls, is controlled by, or is under common control with another company.

(2) AGENCY.—The term "agency" has the same meaning as in section 551(1) of title 5, United States Code.

(3) BREACH OF DATA SECURITY.—

(A) IN GENERAL.—The term "breach of data security" means the unauthorized acquisition of sensitive financial account information or sensitive personal information.

(B) EXCEPTION FOR DATA THAT IS NOT IN USABLE FORM.—The term "breach of data security" does not include the unauthorized acquisition of sensitive financial account information or sensitive personal information that is encrypted, redacted, or otherwise protected by another method that renders the information unreadable and unusable if the encryption, redaction, or protection process or key is not also acquired without authorization.

(4) CARRIER.—The term "carrier" means any entity that—

(A) provides electronic data transmission, routing, intermediate, and transient storage, or connections to its system or network;

(B) does not select or modify the content of the electronic data;

(C) is not the sender or the intended recipient of the data; and

(D) does not differentiate sensitive financial account information or sensitive personal information from other information that the entity transmits, routes, stores in intermediate or transient storage, or for which such entity provides connections.

(5) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(6) CONSUMER.—The term "consumer" means an individual.

(7) CONSUMER REPORTING AGENCY THAT COMPILES AND MAINTAINS FILES ON CONSUMERS ON A NATIONWIDE BASIS.—The term "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" has the same meaning as in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

(8) COVERED ENTITY.—

(A) IN GENERAL.—The term "covered entity" means any individual, partnership, corporation, trust, estate, cooperative, association, or entity that accesses, maintains, communicates, or handles sensitive financial account information or sensitive personal information.

(B) EXCEPTION.—The term "covered entity" does not include any agency or any other unit of Federal, State, or local government or any subdivision of the unit.

(9) FINANCIAL INSTITUTION.—The term "financial institution" has the same meaning as in section 509(3) of the Gramm-Leach-Bliley Act (15 U.S.C. 6809(3)).

(10) INFORMATION SECURITY PROGRAM.—The term "information security program" means the administrative, technical, and physical safeguards that a covered entity uses to protect the confidentiality and security of sensitive financial account information and sensitive personal information when accessing, collecting, distributing, processing, protecting, storing, using, transmitting, disposing of, or otherwise handling sensitive financial account information and sensitive personal information.

(11) SENSITIVE FINANCIAL ACCOUNT INFORMATION.—The term "sensitive financial account information" means a financial account number relating to a consumer, including a credit card number or debit card number, in combination with any security code, access code, password, or other personal identification information required to access the financial account.

(12) SENSITIVE PERSONAL INFORMATION.—

(A) IN GENERAL.—The term "sensitive personal information" includes—

(i) a non-truncated Social Security number;

(ii) the first name or initial and last name of a consumer in combination with—

(I) the consumer's driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

(II) information that could be used to access a consumer's account, such as a user name and password or e-mail and password; or

(III) biometric data of the consumer used to gain access to financial accounts of the consumer; and

(iii) medical information and health insurance information.

(B) EXCEPTION.—The term "sensitive personal information" does not include publicly available information that is lawfully made available to the general public and obtained from—

(i) Federal, State, or local government records; or

(ii) widely distributed media.

(13) THIRD-PARTY SERVICE PROVIDER.—The term "third-party service provider" means any person that maintains, processes, or otherwise is permitted access to sensitive financial account information or sensitive personal information in connection with providing services to a covered entity.

SEC. 4. PROTECTION OF INFORMATION AND SECURITY BREACH NOTIFICATION.

(a) SECURITY PROCEDURES REQUIRED.—

(1) IN GENERAL.—Each covered entity shall develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards that are reasonably designed to achieve the objectives in paragraph (2).

(2) OBJECTIVES.—The objectives of this subsection are to—

(A) protect security and confidentiality of sensitive financial account information and sensitive personal information;

(B) protect against any anticipated threats or hazards to the security or integrity of such information; and

(C) protect against unauthorized acquisition of such information that could result in harm to the individuals to whom such information relates.

(3) LIMITATION.—A covered entity's information security program under paragraph (1) shall be appropriate to—

(A) the size and complexity of the covered entity;

(B) the nature and scope of the activities of the covered entity; and

(C) the sensitivity of the consumer information to be protected.

(4) ELEMENTS.—In order to develop, implement, maintain, and enforce its information security program, a covered entity shall—

(A) designate an employee or employees to coordinate the information security program;

(B) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of sensitive financial account information and sensitive personal information and assess the sufficiency of any safeguards in place to control these risks, including consideration of risks in each relevant area of the covered entity's operations, including—

(i) employee training and management;

(ii) information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and

(iii) detecting, preventing, and responding to attacks, intrusions, or other systems failures;

(C) design and implement safeguards to control the risks identified in its risk assessment, and regularly assess the effectiveness of the safeguards' key controls, systems, and procedures;

(D) oversee third-party service providers by—

(i) taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate safeguards for the sensitive financial account information or sensitive personal information at issue;

(ii) requiring third-party service providers by contract to implement and maintain such safeguards; and

(iii) reasonably oversee or obtain an assessment of the third-party service provider's compliance with contractual obligations, where appropriate; and

(E) evaluate and adjust the information security program in light of the results of the risk assessments and testing and monitoring required by subparagraphs (C) and (D) and any material changes to the covered entity's operations or business arrangements, or any other circumstances that the covered entity knows or has reason to know may have a material impact on its information security program.

(5) SECURITY CONTROLS.—Each covered entity shall—

(A) consider whether the following security measures are appropriate for the covered entity and, if so, adopt those measures that the covered entity concludes are appropriate—

(i) access controls on information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing sensitive financial account information or sensitive personal information to unauthorized individuals who may seek to obtain this information through fraudulent means;

(ii) access restrictions at physical locations containing sensitive financial account information or sensitive personal information, such as

buildings, computer facilities, and records storage facilities, to permit access only to authorized individuals;

(iii) encryption of electronic sensitive financial account information or sensitive personal information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

(iv) procedures designed to ensure that information system modifications are consistent with the covered entity's information security program;

(v) dual control procedures, segregation of duties, and criminal background checks for employees with responsibilities for, or access to, sensitive financial account information or sensitive personal information;

(vi) monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(vii) response programs that specify actions to be taken when the covered entity suspects or detects that unauthorized individuals have gained access to information systems; and

(viii) measures to protect against destruction, loss, or damage of sensitive financial account information or sensitive personal information due to potential environmental hazards, such as fire and water damage or technological failures;

(B) develop, implement, and maintain appropriate measures to properly dispose of sensitive financial account information and sensitive personal information; and

(C) train staff to implement the covered entity's information security program.

(6) ADMINISTRATIVE REQUIREMENTS.—

(A) BOARD OVERSIGHT.—If a covered entity has a board of directors, the covered entity's board of directors or an appropriate committee of the board shall direct that the covered entity has a written information security program in place and appoint committees or personnel to oversee the development and implementation of the information security program.

(B) REPORT TO THE BOARD.—If a covered entity has a board of directors, a report shall be made to its board or an appropriate committee of the board at least annually, including describing—

(i) the overall status of the information security program and the covered entity's compliance with this Act; and

(ii) material matters related to the development and implementation of the covered entity's program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security breaches or violations and management's responses, and recommendations for changes in the information security program.

(b) INVESTIGATION REQUIRED.—If a covered entity believes that a breach of data security has or may have occurred in relation to sensitive financial account information or sensitive personal information that is maintained, communicated, or otherwise handled by, or on behalf of, the covered entity, the covered entity shall conduct an investigation to—

(1) assess the nature and scope of the incident;

(2) identify any sensitive financial account information or sensitive personal information that may have been involved in the incident;

(3) determine if the sensitive financial account information or sensitive personal information has been acquired without authorization; and

(4) take reasonable measures to restore the security and confidentiality of the systems compromised in the breach.

(c) NOTICE REQUIRED.—

(1) IN GENERAL.—If a covered entity determines under subsection (b) that the unauthorized acquisition of sensitive financial account information or sensitive personal information involved in a breach of data security is reasonably likely to cause harm to the consumers to whom the information relates, the covered entity, or a third party acting on behalf of the covered entity, shall—

(A) notify, within the most expedient time possible and without unreasonable delay—

(i) an appropriate Federal and State law enforcement agency;

(ii) the appropriate agency or authority identified in section 5 to enforce this section;

(iii) any relevant payment card network, if the breach involves a breach of payment card numbers;

(iv) each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, if the breach involves sensitive personal information or sensitive financial account information relating to 5,000 or more consumers; and

(v) all consumers to whom the sensitive financial account information or sensitive personal information relates;

(B) provide notice to consumers by—

(i) written notification sent to the postal address of the consumer in the records of the covered entity;

(ii) telephonic notification to the number of the consumer in the records of the covered entity;

(iii) e-mail notification to the consumer (or via other electronic means) in the records of the covered entity; or

(iv) substitute notification in print and to broadcast media where the individual whose personal information was acquired resides, if providing written, telephonic, or e-mail notification is not feasible due to—

(I) lack of sufficient contact information for the consumers that must be notified;

(II) the anticipated cost of such notification exceeding $250,000;

(III) the number of consumers to be notified exceeds 500,000; or

(IV) exigent circumstances; and

(C) provide notice that includes—

(i) a description of the type of sensitive financial account information or sensitive personal information involved in the breach of data security;

(ii) a general description of the actions taken by the covered entity to restore the security and confidentiality of the sensitive financial account information or sensitive personal information involved in the breach of data security; and

(iii) a summary of rights of victims of identity theft prepared under section 609(d) of the Fair Credit Reporting Act (15 U.S.C. 1681g(d)), if the breach of data security involves sensitive personal information.

(2) DELAY PERMITTED WHEN REQUESTED BY LAW ENFORCEMENT.—A covered entity may delay any notification described under paragraph (1) if such delay is requested by a law enforcement agency.

(d) CLARIFICATION.—A financial institution shall have no obligation under this Act for a breach of security at another covered entity involving sensitive financial account information relating to an account owned by the financial institution.

(e) SPECIAL NOTIFICATION REQUIREMENTS.—

(1) THIRD-PARTY SERVICE PROVIDERS.—In the event of a breach of security of a system maintained by a third-party service provider that has been contracted to maintain, store, or process data in electronic form containing sensitive financial account information or sensitive personal information on behalf of a covered entity who owns or possesses such data, such third-party service provider shall—

(A) notify the covered entity; and

(B) notify consumers if it is agreed that the third-party service provider will provide such notification on behalf of the covered entity.

(2) CARRIER OBLIGATIONS.—

(A) IN GENERAL.—If a carrier becomes aware of a breach of security involving data in electronic form containing sensitive financial account information or sensitive personal information that is owned or licensed by a covered entity that connects to or uses a system or network provided by the carrier for the purpose of transmitting, routing, or providing intermediate or transient storage of such data, such carrier shall notify the covered entity who initiated such connection, transmission, routing, or storage of the data containing sensitive financial account information or sensitive personal information, if such covered entity can be reasonably identified. If a service provider is acting solely as a third-party service provider for purposes of this subsection, the service provider has no other notification obligations under this section.

(B) COVERED ENTITIES WHO RECEIVE NOTICE FROM CARRIERS.—Upon receiving notification from a service provider under paragraph (1), a covered entity shall provide notification as required under this section.

(3) COMMUNICATIONS WITH ACCOUNT HOLDERS.—If a covered entity that is not a financial institution experiences a breach of security involving sensitive financial account information, a financial institution that issues an account to which the sensitive financial account information relates may communicate with the account holder regarding the breach, including—

(A) an explanation that the financial institution was not breached, and that the breach occurred at a third-party that had access to the consumer's sensitive financial account information; or

(B) identify the covered entity that experienced the breach after the covered entity has provided notice consistent with this Act.

(f) COMPLIANCE.—

(1) IN GENERAL.—An entity shall be deemed to be in compliance with—

(A) in the case of a financial institution—

(i) subsection (a), if the financial institution maintains policies and procedures to protect the confidentiality and security of sensitive financial account information and sensitive personal information that are consistent with the policies and procedures of the financial institution that are designed to comply with the requirements of section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) and any regulations or guidance prescribed under that section that are applicable to the financial institution; and

(ii) subsections (b) and (c), if the financial institution—

(I)(aa) maintains policies and procedures to investigate and provide notice to consumers of breaches of data security that are consistent with the policies and procedures of the financial institution that are designed to comply with the investigation and notice requirements established by regulations or guidance under section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) that are applicable to the financial institution;

(bb) is an affiliate of a bank holding company that maintains policies and procedures to investigate and provide notice to consumers of breaches of data security that are consistent with the policies and procedures of a bank that is an affiliate of the financial institution, and the policies and procedures of the bank are designed to comply with the investigation and notice requirements established by any regulations or guidance under section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) that are applicable to the bank; or

(cc)(AA) is an affiliate of a savings and loan holding company that maintains policies and procedures to investigate and provide notice to consumers of data breaches of data security that are consistent with the policies and procedures of a savings association that is an affiliate of the financial institution; and

(BB) the policies and procedures of the savings association are designed to comply with the investigation and notice requirements established by any regulations or guidelines under section 501(b) of the Gramm-Leach-Bliley Act (15 U.S. 6801(b)) that are applicable to savings associations; and

(II) provides for notice to the entities described under clauses (ii), (iii), and (iv) of subsection (c)(1)(A), if notice is provided to consumers pursuant to the policies and procedures of the financial institution described in subclause (I); and

(B) subsections (a), (b), and (c)—

(i) if the entity is a covered entity for purposes of the regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note), to the extent that the entity is in compliance with such regulations; or

(ii) if the entity is in compliance with sections 13402 and 13407 of the HITECH Act (42 U.S.C. 17932 and 17937).

(2) DEFINITIONS.—In this subsection—

(A) the terms "bank holding company" and "bank" have the meanings given the terms in section 2 of the Bank Holding Company Act of 1956 (12 U.S.C. 1841);

(B) the term "savings and loan holding company" has the meaning given the term in section 10 of the Home Owners' Loan Act (12 U.S.C. 1467a); and

(C) the term "savings association" has the meaning given the term in section 2 of the Home Owners' Loan Act (12 U.S.C. 1462).

SEC. 5. ADMINISTRATIVE ENFORCEMENT.

(a) IN GENERAL.—Notwithstanding any other provision of law and except as provided in subsection (c), section 4 shall be enforced exclusively under—

(1) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), in the case of—

(A) a national bank, a Federal branch or Federal agency of a foreign bank, or any subsidiary thereof (other than a broker, dealer, person providing insurance, investment company, or investment adviser), or a savings association, the deposits of which are insured by the Federal Deposit Insurance Corporation, or any subsidiary thereof (other than a broker, dealer, person providing insurance, investment company, or investment adviser), by the Office of the Comptroller of the Currency;

(B) a member bank of the Federal Reserve System (other than a national bank), a branch or agency of a foreign bank (other than a Federal branch, Federal agency, or insured State branch of a foreign bank), a commercial lending company owned or controlled by a foreign bank, an organization operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601, 611), or a bank holding company and its nonbank subsidiary or affiliate (other than a broker, dealer, person providing insurance, investment company, or investment adviser), by the Board of Governors of the Federal Reserve System; and

(C) a bank, the deposits of which are insured by the Federal Deposit Insurance Corporation (other than a member of the Federal Reserve System), an insured State branch of a foreign bank, or any subsidiary thereof (other than a broker, dealer, person providing insurance, investment company, or investment adviser), by the Board of Directors of the Federal Deposit Insurance Corporation;

(2) the Federal Credit Union Act (12 U.S.C. 1751 et seq.), by the National Credit Union Administration Board with respect to any federally insured credit union;

(3) the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.), by the Securities and Exchange Commission with respect to any broker or dealer;

(4) the Investment Company Act of 1940 (15 U.S.C. 80a–1 et seq.), by the Securities and Exchange Commission with respect to any investment company;

(5) the Investment Advisers Act of 1940 (15 U.S.C. 80b–1 et seq.), by the Securities and Exchange Commission with respect to any investment adviser registered with the Securities and Exchange Commission under that Act;

(6) the Commodity Exchange Act (7 U.S.C. 1 et seq.), by the Commodity Futures Trading Commission with respect to any futures commission merchant, commodity trading advisor, commodity pool operator, or introducing broker;

(7) the provisions of title XIII of the Housing and Community Development Act of 1992 (12 U.S.C. 4501 et seq.), by the Director of Federal Housing Enterprise Oversight (and any successor to the functional regulatory agency) with respect to the Federal National Mortgage Association, the Federal Home Loan Mortgage Corporation, and any other entity or enterprise (as defined in that title) subject to the jurisdiction of the functional regulatory agency under that title, including any affiliate of any the enterprise;

(8) State insurance law, in the case of any covered entity engaged in providing insurance, by the applicable—

(A) lead State insurance regulator for an insurance group of an insurance company, if the sensitive financial account information or sensitive personal information is owned by such insurance group; or

(B) State of domicile of the covered entity if subparagraph (A) does not apply;

(9) State securities law, in the case of any investment adviser required to be registered with a State securities commissioner (or any agency or office performing like functions), by the applicable securities commissioner (or any agency or office performing like functions) of the State in which the investment adviser is required to be registered; and

(10) the Federal Trade Commission Act (15 U.S.C. 41 et seq.), by the Commission for any financial institution or covered entity that is not subject to the jurisdiction of any agency or authority described under paragraphs (1) through (9), including—

(A) notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.);

(B) notwithstanding the Federal Aviation Act of 1958 (49 U.S.C. App. 1301 et seq.), include the authority to enforce compliance by air carriers and foreign air carriers; and

(C) notwithstanding the Packers and Stockyards Act (7 U.S.C. 181 et seq.), include the authority to enforce compliance by persons, partnerships, and corporations subject to the provisions of that Act.

(b) APPLICATION TO CABLE OPERATORS, SATELLITE OPERATORS, AND TELECOMMUNICATIONS CARRIERS.—

(1) DATA SECURITY AND BREACH NOTIFICATION.—Sections 201, 202, 222, 338, and 631 of the Communications Act of 1934 (47 U.S.C. 201, 202, 222, 338, and 551), and any regulations promulgated in accordance with those sections, shall not apply with respect to the information security practices, including practices relating to the notification of unauthorized access to data in electronic form, of any covered entity otherwise subject to those sections.

(2) RULE OF CONSTRUCTION.—Nothing in this subsection limits authority of the Federal Communication Commission with respect to sections 201, 202, 222, 338, and 631 of the Communications Act of 1934 (47 U.S.C. 201, 202, 222, 338, and 551).

(c) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) IN GENERAL.—Notwithstanding subsection (a)(10), with respect to a covered entity that is not a financial institution, section 4 may be enforced by the attorney general of a State, in any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by a covered entity that violates section 4 of this Act, by the State (as parens patriae) bringing a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to—

(A) enjoin further violation of such section by the defendant;

(B) compel compliance with such section; or

(C) obtain civil penalties.

(2) INTERVENTION BY THE FEDERAL TRADE COMMISSION.—

(A) NOTICE AND INTERVENTION.—In all cases, the State shall provide prior written notice of any action under paragraph (1) to the Commission and provide the Commission with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon instituting such action. The Commission shall have the right—

(i) to intervene in the action;

(ii) upon so intervening, to be heard on all matters arising therein; and

(iii) to file petitions for appeal.

(B) PENDING PROCEEDINGS.—If the Commission initiates a Federal civil action for a violation of this Act, no State attorney general may bring an action for a violation of this Act that resulted from the same or related acts or omissions against a defendant named in the civil action initiated by the Commission.

(3) RULE OF CONSTRUCTION.—Nothing in this subsection may be construed as permitting an attorney general of a State to bring an action pursuant to paragraph (1) against any covered entity that is a financial institution.

SEC. 6. RELATION TO STATE LAW.

No requirement or prohibition may be imposed under the laws, rules, or regulations of any State, the District of Columbia, or any territory of the United States with respect to the responsibilities of any person to—

(1) protect the security of information relating to consumers that is maintained, communicated, or otherwise handled by, or on behalf of, the person;

(2) safeguard information relating to consumers from—

(A) unauthorized access; and

(B) unauthorized acquisition;

(3) investigate or provide notice of the unauthorized acquisition of, or access to, information relating to consumers, or the potential misuse of the information, for fraudulent, illegal, or other purposes; or

(4) mitigate any potential or actual loss or harm resulting from the unauthorized acquisition of, or access to, information relating to consumers.

SEC. 7. DELAYED EFFECTIVE DATE FOR CERTAIN PROVISIONS.

Sections 4 and 6 shall take effect 1 year after the date of enactment of this Act.

PURPOSE AND SUMMARY

H.R. 2205 establishes a national data security standard and a national data breach notification standard with a strong Federal enforcement mechanism overseen by the Federal Trade Commission (FTC). The bill would replace the current patchwork of state and federal regulations for data breaches with a national law that provides uniform protections across the country.

H.R. 2205 creates a scalable standard commensurate to the size and complexity of the organization, the nature and scope of the activities of the organization, and the sensitivity of the consumer information to be protected. The data security standard is technology neutral and process specific.

Additionally, H.R. 2205 implements requirements for consumer and law enforcement notification after a breach, with the trigger for notification occurring only after a company confirms that hackers have acquired sensitive account or sensitive personal information that can be used for identity theft or financial fraud.

BACKGROUND AND NEED FOR LEGISLATION

Data security is a critical issue for financial institutions, businesses, and the customers they serve. The patchwork of state laws that currently exist around data security and breach notification have caused confusion and a lack of accountability as cyber criminals continue to steal valuable personal information from consumers.

Often, consumers are unaware of the data breach until long after it occurs. A uniform national standard for data protection ensures that institutions in the payments ecosystem are up to par with the standards for financial institutions set forth in the Gramm-Leach-Bliley Act of 1999 (GLBA), eliminating any gaps or weak links in protections for consumers, while a single, consistent standard for both data security and breach notifications that will protect consumers throughout the stream of commerce.

Because companies come in many sizes, and rarely remain static in growth, a national data security solution should recognize the relative economies of scale involved in implementing consumer data protections across all businesses. A national data security and breach notification standard must be inclusive enough to ensure that all companies are able to comply without compromising consumer confidence. Scalable and adaptable technology-neutral standards permit companies of all sizes to have effective data security programs. This flexibility gives smaller businesses the ability to tailor their security efforts to fit the size, nature, and scope of their business, thus avoiding unnecessary and disproportionate burdens and costs.

In a letter of support for H.R. 2205 dated October 15, 2015, the Electronic Payments Coalition, Independent Community Bankers of America, Credit Union National Association, National Association of Federal Credit Unions, Consumer Bankers Association, American Bankers Association, and Financial Services Roundtable wrote:

> H.R. 2205 ensures that all entities that handle consumers' sensitive financial data have in place robust processes to protect data which should help prevent data breaches in the first place.
>
> Because data security should be a shared responsibility by all participants in the payments ecosystem, we strongly urge you to cosponsor H.R. 2205, which will help ensure that minimum standards are in place to protect your constituents' sensitive financial and personal information.

HEARINGS

The Committee on Financial Services' Subcommittee on Financial Institutions held a hearing examining matters relating to H.R. 2205 on May 19, 2015.

COMMITTEE CONSIDERATION

The Committee on Financial Services met in open session on December 8, 2015 and December 9, 2015, and considered the bill. An amendment in the nature of a substitute was offered by Mr. Neugebauer. An amendment to the amendment in the nature of a substitute offered by Ms. Waters was not agreed to by a recorded vote of 20 to 36 (FC–79). The Neugebauer substitute amendment was then adopted by voice vote. The Committee ordered H.R. 2205 to be reported favorably to the House as amended by a recorded vote of 46 yeas to 9 nays (recorded vote no. FC–80), a quorum being present.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the record votes on the motion to report legislation and amendments thereto. The amendment offered by Ms. Waters was defeated by a recorded vote of 20 ayes to 36 nays (Record vote no. FC–79). The second and final record vote in Committee was a motion by Chairman Hensarling to report the bill favorably to the House without amendment. That motion was agreed to by a recorded vote of 46 yeas to 9 nays (Record vote no. FC–80), a quorum being present.

Record vote no. FC-79

Representative	Yea	Nay	Present	Representative	Yea	Nay	Present
Mr. Hensarling		X		Ms. Waters (CA)	X		
Mr. King (NY)		X		Mrs. Maloney (NY)	X		
Mr. Royce		X		Ms. Velázquez	X		
Mr. Lucas		X		Mr. Sherman		X	
Mr. Garrett		X		Mr. Meeks	X		
Mr. Neugebauer		X		Mr. Capuano	X		
Mr. McHenry				Mr. Hinojosa			
Mr. Pearce		X		Mr. Clay			
Mr. Posey		X		Mr. Lynch	X		
Mr. Fitzpatrick		X		Mr. David Scott (GA)	X		
Mr. Westmoreland		X		Mr. Al Green (TX)	X		
Mr. Luetkemeyer		X		Mr. Cleaver	X		
Mr. Huizenga (MI)		X		Ms. Moore	X		
Mr. Duffy		X		Mr. Ellison	X		
Mr. Hurt (VA)		X		Mr. Perlmutter			
Mr. Stivers		X		Mr. Himes	X		
Mr. Fincher		X		Mr. Carney		X	
Mr. Stutzman		X		Ms. Sewell (AL)	X		
Mr. Mulvaney		X		Mr. Foster	X		
Mr. Hultgren		X		Mr. Kildee	X		
Mr. Ross		X		Mr. Murphy (FL)	X		
Mr. Pittenger		X		Mr. Delaney	X		
Mrs. Wagner		X		Ms. Sinema		X	
Mr. Barr		X		Mrs. Beatty	X		
Mr. Rothfus		X		Mr. Heck (WA)	X		
Mr. Messer		X		Mr. Vargas	X		
Mr. Schweikert		X					
Mr. Guinta		X					
Mr. Tipton		X					
Mr. Williams		X					
Mr. Poliquin		X					
Mrs. Love		X					
Mr. Hill		X					
Mr. Emmer		X					

Record vote no. FC-80

Representative	Yea	Nay	Present	Representative	Yea	Nay	Present
Mr. Hensarling	X			Ms. Waters (CA)		X	
Mr. King (NY)	X			Mrs. Maloney (NY)	X		
Mr. Royce	X			Ms. Velázquez		X	
Mr. Lucas	X			Mr. Sherman	X		
Mr. Garrett	X			Mr. Meeks	X		
Mr. Neugebauer	X			Mr. Capuano		X	
Mr. McHenry				Mr. Hinojosa			
Mr. Pearce	X			Mr. Clay			
Mr. Posey	X			Mr. Lynch		X	
Mr. Fitzpatrick	X			Mr. David Scott (GA)	X		
Mr. Westmoreland		X		Mr. Al Green (TX)		X	
Mr. Luetkemeyer	X			Mr. Cleaver	X		
Mr. Huizenga (MI)	X			Ms. Moore	X		
Mr. Duffy				Mr. Ellison		X	
Mr. Hurt (VA)	X			Mr. Perlmutter			
Mr. Stivers	X			Mr. Himes	X		
Mr. Fincher	X			Mr. Carney	X		
Mr. Stutzman	X			Ms. Sewell (AL)	X		
Mr. Mulvaney	X			Mr. Foster	X		
Mr. Hultgren	X			Mr. Kildee		X	
Mr. Ross	X			Mr. Murphy (FL)	X		
Mr. Pittenger	X			Mr. Delaney		X	
Mrs. Wagner	X			Ms. Sinema	X		
Mr. Barr	X			Mrs. Beatty	X		
Mr. Rothfus	X			Mr. Heck (WA)	X		
Mr. Messer	X			Mr. Vargas	X		
Mr. Schweikert	X						
Mr. Guinta	X						
Mr. Tipton	X						
Mr. Williams	X						
Mr. Poliquin	X						
Mrs. Love	X						
Mr. Hill	X						
Mr. Emmer	X						

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the findings and recommendations of the committee based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the Committee states that H.R. 2205 will protect consumers' personal information by creating a national data security and breach notification standard to replace the current patchwork of state data security laws.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the estimate of new budget authority, entitlement authority, or tax expenditures or revenues contained in the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

COMMITTEE COST ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

CONGRESSIONAL BUDGET OFFICE ESTIMATES

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, September 29, 2016.

Hon. JEB HENSARLING,
Chairman, Committee on Financial Services,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 2205, the Data Security Act of 2015.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Kim Cawley.

Sincerely,

KEITH HALL.

Enclosure.

H.R. 2205—Data Security Act of 2015

H.R. 2205 would establish a new law to require businesses to take reasonable steps to protect personal information they maintain in electronic form. Further, H.R. 2205 would require those en-

tities, in the event of a breach in their security systems, to notify individuals whose personal information has been accessed and acquired as a result of the breach. Forty-seven states have laws that govern data security; H.R. 2205 would pre-empt many of those statutes. Finally, H.R. 2205 would require the Federal Trade Commission (FTC) and many of the financial regulatory agencies to enforce the requirements of the bill.

Federal budgetary effects

CBO estimates that implementing H.R. 2205 would cost the FTC, the Securities and Exchange Commission, and the Commodity Futures Trading Commission about $2 million over the 2016–2021 period, assuming appropriation of the necessary amounts. CBO expects those agencies would hire additional staff, at a cost of less than $500,000 per year, on average, to carry out the new regulatory requirements because current laws that cover the businesses regulated by those agencies do not address all of the data security issues covered by H.R. 2205.

H.R. 2205 also would require the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the National Credit Union Administration, and the Federal Reserve to ensure compliance with the requirements of the bill for the depository institutions that they regulate. The costs to those regulators would be recorded in the federal budget as increases in direct spending (or as a reduction in revenues, in the case of the Federal Reserve). As a result, pay-as-you-go procedures apply to the bill. However, because provisions of the bill would deem compliance with current laws that apply to depository institutions as complying with the provisions of H.R. 2205, CBO estimates that under the bill the additional costs for those regulators would be negligible.

CBO estimates that enacting H.R. 2205 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2027.

Intergovernmental mandates

H.R. 2205 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA) because it would explicitly preempt laws in at least 47 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands that require businesses to notify individuals in the event of a security breach. The bill also would preempt laws in at least 12 states that have enacted data security laws. Finally, the bill would impose notification requirements and limitations on state attorneys general. Because the limits on state authority would impose no duties with costs and because the notification requirements would result in minimal additional spending, CBO estimates compliance costs would be small and would not exceed the threshold established in UMRA for intergovernmental mandates ($77 million in 2016, adjusted annually for inflation).

Private-sector mandates

H.R. 2205 also contains private-sector mandates as defined in UMRA because it would impose information security and notification requirements on businesses and other entities that use or han-

dle personal information. Specifically, the bill would require businesses and other entities to:

- Protect sensitive financial and personal information from unauthorized access by implementing and maintaining security measures that comply with the standards outlined in the bill (for example, entities would be required to designate an employee to coordinate their security programs, to periodically conduct vulnerability assessments and to adjust security programs based on those assessments); and
- Notify affected consumers, certain federal or state authorities, each consumer reporting agency, and any payment card network as appropriate whenever sensitive personal information has been compromised as a result of a breach.

In addition the bill would require:

- Businesses that have a board of directors to produce a written information security program and to report to the board annually on that status of the program; and
- Third-party service providers and Internet service providers that handle personal information on behalf of a business to notify the affected business in the event of a breach.

Entities already in compliance with the requirements under Gramm-Leach-Bliley, the Health Insurance Portability and Accountability Act, or the Health Information Technology for Economic and Clinical Health Act would be deemed to be in compliance with the bill's provisions.

The net cost of the mandates would equal the additional costs incurred, offset by any savings associated with complying with the bill's requirements. Most businesses already notify consumers in the event of a breach, so CBO expects that the bill's notification requirements would not have a substantial cost. Many of those businesses would experience a savings, because the bill would establish a uniform national standard that would preempt state laws, some of which are more stringent than the notification requirements proposed by the bill. In addition, some costs of the mandate may be mitigated because most businesses already employ data security measures and the bill would allow covered entities some flexibility to adopt security measures that are appropriate for their size, nature, and complexity of operations. However, millions of entities in the private sector may need to implement new or enhanced security measures if the bill is enacted, so that even a relatively low incremental cost per firm could amount to substantial costs in total. Consequently, CBO estimates that, in aggregate, the net cost to comply with the mandates in the bill would probably exceed the annual threshold established in UMRA for private-sector mandates ($154 million in 2016, adjusted annually for inflation) in at least one of the first five years the mandates are in effect.

The CBO staff contacts for this estimate are Kim Cawley (for federal costs), Rachel Austin (for intergovernmental mandates), and Logan Smith (for private-sector mandates). The estimate was approved by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of the section 102(b)(3) of the Congressional Accountability Act.

EARMARK IDENTIFICATION

H.R. 2205 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9 of rule XXI.

DUPLICATION OF FEDERAL PROGRAMS

Pursuant to section 3(g) of H. Res. 5, 114th Cong. (2015), the Committee states that no provision of H.R. 2205 establishes or reauthorizes a program of the Federal Government known to be duplicative of another Federal program, a program that was included in any report from the Government Accountability Office to Congress pursuant to section 21 of Public Law 111–139, or a program related to a program identified in the most recent Catalog of Federal Domestic Assistance.

DISCLOSURE OF DIRECTED RULEMAKING

Pursuant to section 3(k) of H. Res. 5, 114th Cong. (2015), the Committee states that H.R. 2205 contains no directed rulemaking.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This Section cites H.R. 2205 as the "Data Security Act of 2015".

Section 2. Purpose

This Section describes the purpose of this act as establishing a uniform national data security and data breach notification system.

Section 3. Definitions

This section defines terms as they relate to this Act.

Section 4. Protection of information and security breach notification

This section addresses data security, investigation of potential breaches, and breach notification. Each covered entity should develop, implement and maintain a comprehensive information security program that contains administrative, technical and physical safeguards that are designed to protect personal information. Furthermore, the program should be appropriate to the size and complexity of the covered entity. If a breach occurs, a covered entity

should conduct a complete investigation into the scope of the breach, the information that was compromised and the steps that can be taken to prevent further access to confidential personal information. Lastly, if personal information was compromised in a breach, the covered entity should inform the appropriate law enforcement agency, regulatory agency and all consumers to whom the sensitive account information or sensitive personal information relates.

Section 5. Administrative enforcement

This section describes which regulatory agencies will have enforcement authority under this Act.

Section 6. Relation to state law

This section prohibits certain state laws from being imposed for information security and breach notification purposes.

Section 7. Delayed effective date

This section states that the Act will take effect 1 year after the date of enactment.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

H.R. 2205 does not repeal or amend any section of a statute. Therefore, the Office of Legislative Counsel did not prepare the report contemplated by Clause 3(e)(1)(B) of rule XIII of the House of Representatives.

MINORITY VIEWS

The growing frequency and scale of data breaches around the country, which increasingly results in significant financial, personal, and emotional harm to American consumers, is deeply troubling.

According to the Privacy Rights Clearinghouse (Clearinghouse), the number of records exposed in cyber-attacks has been increasing since 2005. While the Clearinghouse notes that there were 157 data breaches exposing about 66.9 million records in 2005, there were 783 data breaches exposing about 85.61 million records in 2014. This represents a staggering 500 percent increase in less than 10 years.

We share the view that it is important to require all businesses that handle consumers' sensitive financial or personal information to take appropriate steps to protect this information, regardless of what type of business it is or where it is headquartered. Yet, only 12 states currently apply data security requirements to merchants. However, 47 states currently require consumers to be notified when a breach occurs.

While H.R. 2205 does extend protections to consumers in states that do not currently have them, the sweeping Federal preemption provision included in the bill also eliminates a number protections currently enjoyed by millions of consumers with existing state laws and rules on data security and breach notification matters. In addition to eliminating existing protections for consumers in certain states, the preemption provision included in the bill also restricts states' ability to enact laws and rules that offer greater consumer protections.

Specifically, we are concerned that H.R. 2205 eliminates the existing right of consumers in at least 16 states to sue companies that fail properly to notify them or protect their financial or personal information. The bill's overly broad Federal preemption provision will also eliminate many other consumer protections under state laws or rules that are related to unauthorized disclosures of consumers' information. In the state of California, for example, the bill will eliminate the existing right for identity theft victims to obtain free credit freezes from the major consumer reporting bureaus and free identity theft monitoring services.

While we support the principle of strengthening the requirements on all businesses to safeguard consumers' sensitive financial or personal information through Federal legislation, we oppose Federal legislation that accomplishes this worthwhile goal at the cost of taking away existing consumer protections provided through state laws or rules on this matter. Rather than enact Federal legislation that creates new protections for some consumers but also eliminates existing protections for other consumers, we believe a better approach would be to codify the most progressive state

standards and preserve states' ability to keep pace with the evolving nature of cyber threats by allowing them to retain authority to enact laws and implement rules that provide greater protections for consumers going forward. While the amended version of H.R. 2205 that was favorably reported to the full House by the Committee addresses some of our concerns with respect to enforcement and the harm trigger, it still does not go far enough to address our serious concerns discussed above.

For the foregoing reasons, we oppose H.R. 2205.

MAXINE WATERS.
WM. LACY CLAY.
RUBÉN HINOJOSA.
KEITH ELLISON.
AL GREEN.

○