114TH CONGRESS
1ST SESSION

S. 961

To protect information relating to consumers, to require notice of security breaches, and for other purposes.

IN THE SENATE OF THE UNITED STATES

APRIL 15, 2015

Mr. CARPER (for himself and Mr. BLUNT) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To protect information relating to consumers, to require notice of security breaches, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

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; and

(2) to expressly preempt any related State laws in order to provide the Federal Trade Commission with authority to enforce such standards for entities covered under this 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 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 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 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 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, or physical safeguards that a covered entity uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or

otherwise handle sensitive account information and sensitive personal information.

(11) SENSITIVE ACCOUNT INFORMATION.—The term ''sensitive 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'' means—

(i) a Social Security number; or

(ii) the first 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.

(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) SUBSTANTIAL HARM OR INCONVENIENCE.—The term ''substantial harm or inconvenience'' means—

(A) identity theft; or

(B) fraudulent transactions on financial accounts.

(14) THIRD-PARTY SERVICE PROVIDER.—The term ''third-party service provider'' means any person that maintains, processes, or otherwise is permitted access to sensitive 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) ensure the security and confidentiality of sensitive 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 substantial 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, and maintain 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 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 information 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 service providers by—

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

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

(iii) reasonably oversee or obtain an assessment of the service provider's compliance with contractual obligations, where appropriate in light of the covered entity's risk assessment; and

(E) evaluate and adjust the information security program in light of the results of the risk assessments and testing and monitoring re-

quired 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 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 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 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 employee background checks for employees with responsibilities for, or access to, sensitive 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 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 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—

(i) approve the covered entity's written information security program; and

(ii) oversee the development, implementation, and maintenance of the covered entity's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

(B) REPORT TO THE BOARD.—If a covered entity has a board of directors, the covered entity shall report 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 its 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.—

(1) IN GENERAL.—If a covered entity believes that a breach of data security has or may have occurred in relation to sensitive 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—

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

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

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

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

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

(1) notify, without unreasonable delay—

(A) an appropriate Federal law enforcement agency;

(B) the appropriate agency or authority identified in section 5;

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

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

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

(2) provide notice to consumers by—

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

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

(C) e-mail of the consumer or other electronic means in the records of the covered entity; or

(D) substitute notification in print and to broadcast media where the individual whose personal information was acquired resides, if

providing written or e-mail notification is not feasible due to—

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

(ii) excessive cost to the covered entity; or

(iii) exigent circumstances; and

(3) provide notice that includes—

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

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

(C) a summary of rights of victims of identity theft prepared by the Commission 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.

(d) CLARIFICATION.—A financial institution shall have no obligation under this Act for a breach of security at another covered entity involving sensitive account infor-

mation 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 data security of a system maintained by a third-party entity that has been contracted to maintain, store, or process data in electronic form containing sensitive account information or sensitive personal information on behalf of a covered entity who owns or possesses such data, such third-party shall—

(A) notify the covered entity; and

(B) notify consumers if it is agreed in writing 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 data security involving data in electronic form containing sensitive 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 account information or sensitive personal information, if such covered entity can be reasonably identified. If a service provider is acting solely as a 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 data security involving sensitive account information, a financial institution that issues an account to which the sensitive 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 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 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 subparagraphs (B), (C), and (D) of subsection (c)(1), 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 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 person engaged in providing insurance, by the applicable State insurance authority of the State in which the person is domiciled; and

(9) the Federal Trade Commission Act (15 U.S.C. 41 et seq.), by the Commission for any other covered entity that is not subject to the jurisdiction of any agency or authority described under paragraphs (1) through (8), 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 promul-

gated 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 otherwise 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) NO PRIVATE RIGHT OF ACTION.—

(1) IN GENERAL.—This Act may not be construed to provide a private right of action, including a class action with respect to any Act or practice regulated under this Act.

(2) EXCEPTION.—A consumer or entity that suffers financial harm as a result of a covered entity's violation of this Act may bring an action in a district court of the United States for the judicial district in which the consumer or entity suffered the harm against the covered entity to recover—

(A) in the case of a negligent violation of this Act, actual financial damages, court costs

allowed by the rules of the court, and reasonable attorney's fees; and

(B) in the case of a knowing violation of this Act, the damages, costs, and attorney's fees described in subparagraph (A) of this subsection and punitive damages.

SEC. 6. RELATION TO STATE LAW.

No requirement or prohibition may be imposed under the laws of any State 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.

○