I

114TH CONGRESS
1ST SESSION

H. R. 4187

To require certain entities who collect and maintain personal information of individuals to secure such information and to provide notice to such individuals in the case of a breach of security involving such information, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

DECEMBER 8, 2015

Ms. SCHAKOWSKY (for herself, Mr. PALLONE, Mr. RUSH, Mr. TONKO, Mr. WELCH, Mr. KENNEDY, Mr. SARBANES, and Mr. BUTTERFIELD) introduced the following bill; which was referred to the Committee on Energy and Commerce

---

A BILL

To require certain entities who collect and maintain personal information of individuals to secure such information and to provide notice to such individuals in the case of a breach of security involving such information, 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 ‘‘Secure and Protect Americans’ Data Act’’.

SEC. 2. REQUIREMENTS FOR INFORMATION SECURITY.

(a) GENERAL SECURITY POLICIES AND PROCEDURES.—

(1) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to require each covered entity to establish and implement reasonable policies and procedures regarding information security practices for the treatment and protection of personal information taking into consideration—

(A) the size of, and the nature, scope, and complexity of the activities engaged in by such covered entity;

(B) the sensitivity of any personal information at issue;

(C) the current state of the art in administrative, technical, and physical safeguards for protecting such information; and

(D) the cost of implementing such safeguards.

(2) REQUIREMENTS.—Such regulations shall require the policies and procedures to include the following:

(A) A written security policy with respect to the collection, use, sale, other dissemination, and maintenance of such personal information.

(B) The identification of an officer or other individual as the point of contact with responsibility for the management of information security.

(C) A process for identifying and assessing any reasonably foreseeable vulnerabilities in the system or systems maintained by such covered entity that contains such data, which shall include regular monitoring for a breach of security of such system or systems.

(D) A process for taking preventive and corrective action to mitigate against any vulnerabilities identified in the process required by subparagraph (C), which may include implementing any changes to security practices and the architecture, installation, or implementation of network or operating software, and for regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures.

(E) A process for disposing of data containing personal information by shredding, permanently erasing, or otherwise modifying the personal information contained in such data to make such personal information permanently unreadable or undecipherable.

(F) A process for overseeing persons to whom personal information is disclosed, or who have access to Internet-connected devices, by—

(i) taking reasonable steps to select and retain persons that are capable of maintaining appropriate safeguards for the personal information or Internet-connected devices at issue; and

(ii) requiring all such persons to implement and maintain such security measures.

(G) A process for employee training and supervision for implementation of the policies and procedures required by this subsection.

(3) PERIODIC ASSESSMENT AND CONSUMER PRIVACY AND DATA SECURITY MODERNIZATION.—Not less than every 12 months, each covered entity shall monitor, evaluate, and adjust, as appropriate, the consumer privacy and data security program of such covered entity in light of any relevant changes in—

(A) technology;

(B) internal or external threats and vulnerabilities to personal information; and

(C) the changing business arrangements of the covered entity, such as—

(i) mergers and acquisitions;

(ii) alliances and joint ventures;

(iii) outsourcing arrangements;

(iv) bankruptcy; and

(v) changes to personal information systems.

(4) TREATMENT OF ENTITIES GOVERNED BY OTHER FEDERAL LAW.—Any covered entity who is in compliance with any other Federal law that requires such covered entity to maintain standards and safeguards for information security and protection of personal information that, taken as a whole and as the Commission shall determine in the rulemaking required under this subsection, requires covered entities to provide protections substantially similar to, or greater than, those required under this subsection, shall be deemed to be in compliance with this subsection.

(b) SPECIAL REQUIREMENTS FOR INFORMATION BROKERS.—

(1) SUBMISSION OF POLICIES TO THE FTC.—The regulations promulgated under subsection (a) shall require each information broker to submit its security policies to the Commission in conjunction with a notification of a breach of security under section 3 or upon request of the Commission.

(2) POST-BREACH AUDIT.—For any information broker required to provide notification under section 3, the Commission may conduct audits of the information security practices of such information broker, or require the information broker to conduct independent audits of such practices (by an independent auditor who has not audited such information broker's security practices during the preceding 5 years).

(3) ACCURACY OF AND INDIVIDUAL ACCESS TO PERSONAL INFORMATION.—

(A) ACCURACY.—

(i) IN GENERAL.—Each information broker shall establish reasonable procedures to assure the maximum possible accuracy of the personal information the information broker collects, assembles, or maintains, and any other information the information broker collects, assembles, or maintains that specifically identifies an individual, other than information which merely identifies an individual's name or address.

(ii) LIMITED EXCEPTION FOR FRAUD DATABASES.—The requirement in clause (i) shall not prevent the collection or maintenance of information that may be inaccurate with respect to a particular individual when that information is being collected or maintained solely—

(I) for the purpose of indicating whether there may be a discrepancy or irregularity in the personal information that is associated with an individual; and

(II) to help identify, or authenticate the identity of, an individual, or to protect against or investigate fraud or other unlawful conduct.

(B) CONSUMER ACCESS TO INFORMATION.—Each information broker shall—

(i) provide to each individual whose personal information the information broker maintains, at the individual's request at least once per year and at no cost to the individual, and after verifying the identity of such individual, a means for the individual to review any personal information regarding such individual maintained by the information broker and any other information maintained by the information broker that specifically identifies such individual, other than information which merely identifies an individual's name or address; and

(ii) place a conspicuous notice on the Internet website of the information broker (if the information broker maintains such a website) instructing individuals how to request access to the information required to be provided under clause (i), and, as applicable, how to express a preference with respect to the use of personal information for marketing purposes under subparagraph (D).

(C) DISPUTED INFORMATION.—Whenever an individual whose information the information broker maintains makes a written request disputing the accuracy of any such information, the information broker, after verifying the identity of the individual making such request and unless there are reasonable grounds to believe such request is frivolous or irrelevant, shall—

(i) correct any inaccuracy; or

(ii) in the case of information that is—

(I) public record information, inform the individual of the source of the information, and, if reasonably available, where a request for correction may be directed and, if the individual provides proof that the public record has been corrected or that the information broker was reporting the information incorrectly, correct the inaccuracy in the information broker's records; or

(II) nonpublic information, note the information that is disputed, including the individual's statement disputing such information, and take reasonable steps to independently verify such information under the procedures outlined in subparagraph (A) if such information can be independently verified.

(D) ALTERNATIVE PROCEDURE FOR CERTAIN MARKETING INFORMATION.—In accordance with regulations issued under subparagraph (F), an information broker that maintains any information described in subparagraph (A) which is used, shared, or sold by such information broker for marketing purposes, may, in lieu of complying with the access and dispute requirements set forth in subparagraphs (B) and (C), provide each individual whose information the information broker maintains with a reasonable means of expressing a preference not to have his or her information used for such purposes. If the individual expresses such a preference, the information broker may not use, share, or sell the individual's information for marketing purposes.

(E) LIMITATIONS.—An information broker may limit the access to information required under subparagraph (B)(i) and is not required to provide notice to individuals as required under subparagraph (B)(ii) in the following circumstances:

(i) If access of the individual to the information is limited by law or legally recognized privilege.

(ii) If the information is used for a legitimate governmental or fraud prevention purpose that would be compromised by such access.

(iii) If the information consists of a published media record, unless that record has been included in a report about an individual shared with a third party.

(F) RULEMAKING.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to carry out this paragraph and to facilitate the purposes of this Act. In addition, the Commission shall issue regulations, as necessary, under section 553 of title 5, United States Code, on the scope of the application of the limitations in subparagraph (E), including any additional circumstances in which an information broker may limit access to information under such clause that the Commission determines to be appropriate.

(G) FCRA REGULATED PERSONS.—Any information broker who is engaged in activities subject to the Fair Credit Reporting Act and who is in compliance with sections 609, 610, and 611 of such Act (15 U.S.C. 1681g; 1681h; 1681i) with respect to information subject to such Act, shall be deemed to be in compliance with this paragraph with respect to such information.

(4) REQUIREMENT OF AUDIT LOG OF ACCESSED AND TRANSMITTED INFORMATION.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to require information brokers to establish measures which facilitate the auditing or retracing of any internal or external access to, or transmissions of, any data containing personal information collected, assembled, or maintained by such information broker.

(5) PROHIBITION ON PRETEXTING BY INFORMATION BROKERS.—

(A) PROHIBITION ON OBTAINING PERSONAL INFORMATION BY FALSE PRETENSES.—It shall be unlawful for an information broker to obtain or attempt to obtain, or cause to be disclosed or attempt to cause to be disclosed to any person, personal information or any other information relating to any person by—

(i) making a false, fictitious, or fraudulent statement or representation to any person; or

(ii) providing any document or other information to any person that the information broker knows or should know to be forged, counterfeit, lost, stolen, or fraudulently obtained, or to contain a false, fictitious, or fraudulent statement or representation.

(B) PROHIBITION ON SOLICITATION TO OBTAIN PERSONAL INFORMATION UNDER FALSE PRETENSES.—It shall be unlawful for an information broker to request a person to obtain personal information or any other information relating to any other person, if the information broker knew or should have known that the person to whom such a request is made will obtain or attempt to obtain such information in the manner described in subparagraph (A).

SEC. 3. NOTIFICATION OF INFORMATION SECURITY BREACH.

(a) INDIVIDUAL NOTIFICATION.—

(1) IN GENERAL.—Each covered entity shall, following the discovery of a breach of security, notify each individual who is a citizen or resident of the United States whose personal information was, or is reasonably believed to have been, acquired or accessed by an unauthorized person, or used for an unauthorized purpose.

(2) TIMELINESS OF NOTIFICATION.—

(A) IN GENERAL.—Unless subject to a delay authorized under subparagraph (B), a notification required under paragraph (1) shall be made as expeditiously as practicable and without unreasonable delay, but not later than 30 days following the discovery of a breach of security.

(B) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—

(i) LAW ENFORCEMENT.—If a Federal or State law enforcement agency, including an attorney general of a State, determines that the notification required under this section would impede a civil or criminal investigation, such notification shall be delayed upon the written request of the law enforcement agency for 30 days or such lesser period of time which the law enforcement agency determines is reasonably necessary and requests in writing. Such a law enforcement agency may, by a subsequent written request, revoke such delay or extend the period of time set forth in the original request made under this paragraph if further delay is necessary.

(ii) NATIONAL SECURITY.—If a Federal national security agency or homeland security agency determines that the notification required under this section would threaten national or homeland security, such notification may be delayed for a period of time of up to 60 days which the national security agency or homeland security agency determines is reasonably necessary and requests in writing. A Federal national security agency or homeland security agency may revoke such delay or extend the period of time set forth in the original request made under this paragraph by a subsequent written request if further delay is necessary.

(b) COORDINATION OF NOTIFICATION WITH CONSUMER REPORTING AGENCIES.—If a covered entity is required to provide notification to more than 5,000 individuals under subsection (a)(1), the covered entity shall also notify the major consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, of the timing and distribution of the notifications. Such notification shall be given to the consumer reporting agencies without unreasonable delay and, if such notification will not delay notification to the affected individuals, prior to the distribution of notifications to the affected individuals.

(c) METHOD AND CONTENT OF NOTIFICATION.—

(1) GENERAL NOTIFICATION.—A covered entity required to provide notification to individuals under subsection (a)(1) shall be in compliance with such requirement if the covered entity provides conspicuous and clearly identified notification by one of the following methods (provided the selected method can reasonably be expected to reach the intended individual):

(A) Written notification to the last known home mailing address of the individual in the records of the covered entity.

(B) Notification by email or other electronic means, if—

(i) the covered entity's primary method of communication with the individual is by email or such other electronic means; or

(ii) the individual has consented to receive such notification and the notification is provided in a manner that is consistent with the provisions permitting electronic transmission of notifications under section 101 of the Electronic Signatures in Global Commerce Act (15 U.S.C. 7001).

(2) WEBSITE NOTIFICATION.—The covered entity shall also provide conspicuous notification on the Internet website of the covered entity (if such covered entity maintains such a website) for a period of not less than 90 days.

(3) MEDIA NOTIFICATION.—If the number of residents of a State whose personal information was, or is reasonably believed to have been acquired or accessed by an unauthorized person, or used for an unauthorized purpose exceeds 5,000, the covered en-

tity shall also provide notification in print and to broadcast media, including major media in metropolitan and rural areas where the individuals whose personal information was, or is reasonably believed to have been, acquired or accessed by an unauthorized person, or used for an unauthorized purpose, reside.

(4) CONTENT OF NOTIFICATION.—

(A) IN GENERAL.—Regardless of the method by which notification is provided to an individual under paragraphs (1), (2), and (3), such notification shall include—

(i) a description of the personal information that was, or is reasonably believed to have been, acquired or accessed by an unauthorized person, or used for an unauthorized purpose;

(ii) a general description of the incident and the date or estimated date of the security breach and the date range during which the personal information was compromised;

(iii) the acts the covered entity, or the agent of the covered entity, has taken to protect personal information from further security breach;

(iv) a telephone number that the individual may use, at no cost to such individual, to contact the covered entity, or agent of the covered entity, to inquire about the breach of security or the information the covered entity maintained about that individual;

(v) notification that the individual is entitled to receive, at no cost to such individual, consumer credit reports on a quarterly basis for a period of 2 years, or credit monitoring or other service that enables consumers to detect the misuse of their personal information for a period of 2 years, and instructions to the individual on requesting such reports or service from the covered entity, except when the only information which has been the subject of the security breach is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code;

(vi) the toll-free contact telephone numbers and addresses for the major consumer reporting agencies; and

(vii) a toll-free telephone number and Internet website address for the Commission whereby the individual may obtain information regarding identity theft.

(B) DIRECT BUSINESS RELATIONSHIP.—The notification required under subsection (a) shall identify the covered entity that has a direct business relationship with the individual.

(5) REGULATIONS FOR SUBSTITUTE NOTIFICATION.—Not later than 1 year after the date of enactment of this Act, the Commission shall, by regulation under section 553 of title 5, United States Code—

(A) establish criteria for determining circumstances under which substitute notification may be provided in lieu of direct notification required by paragraph (1), including criteria for determining if notification under paragraph (1) is not feasible due to excessive costs to the covered entity required to provide such notification relative to the resources of such covered entity; and

(B) establish the form and content of substitute notification.

(d) NOTIFICATION FOR LAW ENFORCEMENT AND OTHER PURPOSES.—A covered entity shall, as expeditiously as practicable and without unreasonable delay, but not later than 10 days following the discovery of a breach of security, provide notification of the breach to—

(1) the Commission;

(2) the Federal Bureau of Investigation;

(3) the Secret Service;

(4) for common carriers, the Federal Communications Commission; and

(5) the attorney general of each State in which the personal information of a resident or residents of the State was, or is reasonably believed to have been, acquired or accessed by an unauthorized person, or used for an unauthorized purpose.

(e) OTHER OBLIGATIONS FOLLOWING BREACH.—

(1) IN GENERAL.—A covered entity required to provide notification under subsection (a) shall, upon request of an individual whose personal information was included in the breach of security, provide or arrange for the provision of, to each such individual and at no cost to such individual—

(A) consumer credit reports from all of the major consumer reporting agencies beginning not later than 60 days following the individual's request and continuing on a quarterly basis for a period of 2 years thereafter; or

(B) a credit monitoring or other service that—

(i) enables consumers to detect the misuse of their personal information, beginning not later than 60 days following the individual's request and continuing for a period of 2 years; and

(ii) includes monitoring of the individual's credit file at all of the major consumer reporting agencies.

(2) LIMITATION.—This subsection shall not apply if the only personal information which has been the subject of the security breach is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code.

(3) RULEMAKING.—As part of the Commission's rulemaking described in subsection (c)(5), the Commission shall determine the circumstances under which a covered entity required to provide notifica-

tion under subsection (a) shall provide or arrange for the provision of free consumer credit reports or credit monitoring or other service to affected individuals.

(f) EXEMPTION.—

(1) GENERAL EXEMPTION.—A covered entity shall be exempt from the requirements under this section if the data containing personal information that was, or is reasonably believed to have been, acquired or accessed by an unauthorized person, or used for an unauthorized purpose, is unusable, unreadable, or indecipherable because of security technologies or methodologies generally accepted by experts in the field of information security at the time the breach of security occurred. This exemption does not apply with regard to the use of encryption technology generally accepted by experts in the field of information security at the time the breach of security occurred if any cryptographic keys necessary to enable decryption of such data are also accessed or acquired without authorization.

(2) FTC GUIDANCE.—Not later than 1 year after the date of enactment of this Act the Commission shall issue guidance regarding the application of the exemption in paragraph (1).

(g) WEBSITE NOTIFICATION OF FEDERAL TRADE COMMISSION.—If the Commission, upon receiving notification of any breach of security that is reported to the Commission under subsection (d)(1), finds that notification of such a breach of security via the Commission's Internet website would be in the public interest or for the protection of consumers, the Commission shall place such a notification in a clear and conspicuous location on its Internet website.

(h) WEBSITE NOTIFICATION OF STATE ATTORNEYS GENERAL.—If a State attorney general, upon receiving notification of any breach of security that is reported to the Commission under subsection (d)(5), finds that notification of such a breach of security via the State attorney general's Internet website would be in the public interest or for the protection of consumers, the State attorney general shall place such a notification in a clear and conspicuous location on its Internet website.

(i) FTC STUDY ON NOTIFICATION IN LANGUAGES IN ADDITION TO ENGLISH.—Not later than 1 year after the date of enactment of this Act, the Commission shall conduct a study on the practicality and cost effectiveness of requiring the notification required by subsection (c)(1) to be provided in a language in addition to English to individuals known to speak only such other language.

(j) EDUCATION AND OUTREACH FOR SMALL BUSINESSES.—The Commission shall conduct education and outreach for small business concerns on data security practices and how to prevent hacking and other unauthorized access to, acquisition of, or use of data maintained by such small business concerns.

(k) WEBSITE ON DATA SECURITY BEST PRACTICES.—The Commission shall establish and maintain an Internet website containing nonbinding best practices for businesses regarding data security and how to prevent hacking and other unauthorized access to, acquisition of, or use of data maintained by such businesses.

(l) GENERAL RULEMAKING AUTHORITY.—

(1) IN GENERAL.—The Commission may promulgate regulations necessary under section 553 of title 5, United States Code, to effectively enforce the requirements of this section.

(2) LIMITATION.—In promulgating rules under this Act, the Commission shall not require the deployment or use of any specific products or technologies, including any specific computer software or hardware.

(m) TREATMENT OF PERSONS GOVERNED BY OTHER LAW.—A covered entity who is in compliance with any other Federal law that requires such covered entity to provide notification to individuals following a breach of security in at least the same or substantially similar circumstances and in at the least same or substantially similar manner as required to be provided under this Act, shall be deemed to be in compliance with this section with respect to activities and information covered under such Federal law.

SEC. 4. APPLICATION AND ENFORCEMENT.

(a) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 2 or 3 shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices and shall be subject to enforcement by the Commission under that Act with respect to any covered entity. All of the functions and powers of the Commission under the Federal Trade Commission Act are available to the Commission to enforce compliance by any person with the requirements imposed under this title, irrespective of whether that person is engaged in commerce or meets any other jurisdic-

tional tests under the Federal Trade Commission Act.

(2) COORDINATION WITH FEDERAL COMMUNICATIONS COMMISSION.—Where enforcement relates to entities subject to the authority of the Federal Communications Commission, enforcement actions by the Commission will be coordinated with the Federal Communications Commission.

(3) COORDINATION WITH CONSUMER FINANCIAL PROTECTION BUREAU.—Where enforcement relates to financial information or information associated with the provision of financial products or services, enforcement actions by the Commission will be coordinated with the Consumer Financial Protection Bureau.

(b) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) IN GENERAL.—If the chief law enforcement officer of a State, or an official or agency designated by a State, has reason to believe that any covered entity has violated or is violating section 2 or 3 of this Act, the attorney general, official, or agency of the State, in addition to any authority it may have to bring an action in State court under its consumer protection law, may bring a civil action in any ap-

propriate United States district court or in any other court of competent jurisdiction, including a State court, to—

(A) enjoin further such violation by the defendant;

(B) enforce compliance with this such section;

(C) obtain civil penalties in the amount determined under paragraph (2); and

(D) obtain damages, restitution, or other compensation on behalf of residents of the State.

(2) CIVIL PENALTIES.—

(A) CALCULATION.—

(i) TREATMENT OF VIOLATIONS OF SECTION 2.—For purposes of paragraph (1)(C) with regard to a violation of section 2, the amount determined under this paragraph is the amount calculated by multiplying the number of days that a covered entity is not in compliance with such section by an amount not greater than $16,500.

(ii) TREATMENT OF VIOLATIONS OF SECTION 3.—For purposes of paragraph

(1)(C) with regard to a violation of section 3, the amount determined under this paragraph is the amount calculated by multiplying the number of violations of such section by an amount not greater than $16,500. Each failure to send notification as required under section 3 to a resident of the United States shall be treated as a separate violation.

(B) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index is first published by the Bureau of Labor Statistics that is after 1 year after the date of enactment of this Act, and each year thereafter, the amounts specified in clauses (i) and (ii) of subparagraph (A) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(3) NOTICE AND INTERVENTION BY THE FTC.—

(A) The attorney general of a State shall provide prior written notice of any action under paragraph (1) to the Commission and provide the Commission with a copy of the complaint in the action, except in any case in which such prior notice is not feasible, in which case the attorney general 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) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING.—If the Commission has instituted a civil action for violation of this Act, no State attorney general, or official or agency of a State, may bring an action under this subsection during the pendency of that action against any defendant named in the complaint of the Commission for any violation of this Act alleged in the complaint.

(4) RELATIONSHIP WITH STATE-LAW CLAIMS.—If the attorney general of a State has authority to bring an action under State law directed at acts or practices that also violate this Act, the attorney general may assert the State-law claim and a claim under this Act in the same civil action.

SEC. 5. DEFINITIONS.

In this Act:

(1) BREACH OF SECURITY.—The term ''breach of security'' means unauthorized access to, acquisition of, or use of data containing personal information.

(2) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(3) CONSUMER REPORTING AGENCY.—The term ''consumer reporting agency'' has the meaning given that term in section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a).

(4) COVERED ENTITY.—The term ''covered entity'' means—

(A) any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2));

(B) 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.); and

(C) notwithstanding sections 4 and 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 44 and 45(a)(2)), any nonprofit organization, including any organization described in section 501(c) of the Internal Revenue Code of 1986 that is exempt from taxation under section 501(a) of the Internal Revenue Code of 1986.

(5) INFORMATION BROKER.—The term "information broker"—

(A) means a commercial entity whose business is to collect, assemble, or maintain personal information concerning individuals who are not current or former customers of such entity in order to sell such information or provide access to such information to any nonaffiliated third party in exchange for consideration, whether such collection, assembly, or maintenance of personal information is performed by the information broker directly, or by contract or subcontract with any other entity; and

(B) does not include a commercial entity to the extent that such entity processes information collected by and received from a nonaffiliated third party concerning individuals who are current or former customers or employees of the third party to enable the third party to provide benefits for the employees or directly transact business with the customers.

(6) PERSONAL INFORMATION.—

(A) DEFINITION.—The term "personal information" means any information or compilation of information that includes any of the following:

(i) An individual's first name or initial and last name in combination with any 2 or more of the following data elements for that individual:

(I) Home address or telephone number.

(II) Mother's maiden name.

(III) Month, day, and year of birth.

(IV) User name or electronic mail address.

(ii) Driver's license number, passport number, military identification number, alien registration number, or other similar number issued on a government document used to verify identity.

(iii) Unique account identifier, including a financial account number, or credit or debit card number, electronic identification number, user name, or routing code.

(iv) Partial or complete Social Security number.

(v) Unique biometric or genetic data such as a faceprint, fingerprint, voice print, a retina or iris image, or any other unique physical representations.

(vi) Information that could be used to access an individual's account, such as user name and password or email address and password.

(vii) Any two or more of the following data elements:

(I) An individual's first and last name or first initial and last name.

(II) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.

(III) Any security code, access code, or password, or source code that could be used to generate such codes or passwords.

(viii) Information generated or derived from the operation or use of an electronic communications device that is sufficient to identify the street name and name of the city or town in which the device is located.

(ix) Any information regarding an individual's medical history, mental or physical condition, medical treatment or diagnosis by a health care professional, or the provision of health care to the individual, including health information provided to a website or mobile application.

(x) A health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual, or any information in an individual's health insurance application and claims history, including any appeals records.

(xi) Digitized or other electronic signature.

(xii) Nonpublic communications or other user-created content such as emails, photographs, or videos.

(xiii) Any record or information concerning payroll, income, financial accounts, mortgages, loans, lines of credit, utility bills, accumulated purchases, or any other information regarding financial assets, obligations, or spending habits.

(xiv) Any additional element the Commission defines as personal information.

(B) MODIFIED DEFINITION BY RULEMAKING.—The Commission may, by rule promulgated under section 553 of title 5, United States Code, modify the definition of ''personal information'' under subparagraph (A).

(7) STATE.—The term ''State'' means each of the several States, the District of Columbia, the Commonwealth of Puerto Rico, Guam, American Samoa, the United States Virgin Islands, the Commonwealth of the Northern Mariana Islands, any other territory or possession of the United States, and each federally recognized Indian tribe.

SEC. 6. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE DATA SECURITY AND BREACH NOTIFICATION LAWS.—No State or political subdivision thereof shall have any authority to establish or continue in effect any standard or requirement relating to information security practices for the treatment and protection of personal information as defined in section 5(5)(A) or as subsequently amended by the Federal Trade Commission under section 5(5)(B), or notification to individuals of a breach of security of personal information as defined in section 5(5)(A) or as subsequently amended by the Federal Trade Commission under section 5(5)(B), that is not identical to the standards and requirements established under this Act.

(b) EFFECT ON STATE LAW.—In the case of a provision of the law of a State that is superseded by subsection (a), this Act may be enforced in the same manner and to the same extent as the State law could have been enforced under State law.

(c) EFFECT ON OTHER STATE LAWS.—Nothing in this Act shall be construed to—

(1) preempt or limit any provision of any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State, including any State consumer protection law,

any State law relating to acts of fraud or deception, and any State trespass, contract, or tort law;

(2) preempt or limit any provision of any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State regarding post-data breach services, including security or credit freezes, credit monitoring, identity theft monitoring, and identity theft services;

(3) prevent or limit the attorney general of a State from exercising the powers conferred upon the attorney general by the laws of the State, including conducting investigations, administering oaths or affirmations, or compelling the attendance of witnesses or the production of documentary and other evidence; or

(4) preempt or limit any provision of any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State with respect to any person that is not a covered entity under section 5(4).

(d) PRESERVATION OF AUTHORITY.—

(1) FEDERAL TRADE COMMISSION.—Nothing in this Act may be construed in any way to limit the Commission's authority under any other provision of law.

(2) FEDERAL COMMUNICATIONS COMMISSION.—Nothing in this Act may be construed in any way to limit or affect the Federal Communications Commission's authority under any other provision of law.

(3) CONSUMER FINANCIAL PROTECTION BUREAU.—Nothing in this Act may be construed in any way to limit or affect the Consumer Financial Protection Bureau's authority under any other provision of law.

SEC. 7. EFFECTIVE DATE.

This Act shall take effect 90 days after the date of enactment of this Act.

○