I

116TH CONGRESS
1ST SESSION

H. R. 1282

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

FEBRUARY 14, 2019

Mr. RUSH (for himself, Ms. BLUNT ROCHESTER, and Ms. CLARKE of New York) 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 ''Data Accountability and Trust 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, that require each covered entity to establish and implement 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.—The regulations required pursuant to paragraph (1) shall include a requirement that the policies and procedures include the following:

(A) A written security policy with respect to the collection, use, sale, other dissemination, and maintenance of the 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 vulnerability in any system maintained by the covered entity that contains such data, including regular monitoring for a breach of security of any such system.

(D) A process for—

(i) taking preventive and corrective action to mitigate against any vulnerability 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

(ii) regularly testing or otherwise monitoring the effectiveness of the key con-

trols, systems, and procedures of the safeguards.

(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 safeguards.

(3) TREATMENT OF ENTITIES GOVERNED BY OTHER FEDERAL LAW.—Any covered entity who is in compliance with any other Federal law that requires the 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, 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 pursuant to subsection (a) shall include a requirement for an information broker to submit each security policy of the broker 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 the information broker's security practices during the preceding 5 years).

(3) ACCURACY OF AND INDIVIDUAL ACCESS TO PERSONAL INFORMATION.—The regulations promul-

gated pursuant to subsection (a) shall include a requirement for the following:

(A) ACCURACY.—

(i) IN GENERAL.—Each information broker to 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 infor-

mation 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 to—

(i) provide to each individual whose personal information the information broker maintains (at the individual's request at least once per year, at no cost to the individual, and after verifying the identity of the 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 the 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.

(C) DISPUTED INFORMATION.—

(i) IN GENERAL.—Whenever an individual whose information the information broker maintains makes a written request disputing the accuracy of the 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, to—

(I) correct any inaccuracy; or

(II) in the case of information that is—

(aa) 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 pro-

vides 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

(bb) 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.

(ii) STRUCTURE FOR DISPUTE PROCESS.—A basic structure for the dispute process described in clause (i) which shall be in writing, require an online option for the submission of a dispute, and provide an electronic receipt acknowledging the submission.

(D) LIMITATIONS.—A provision, including the scope of the application, that allows an in-

formation broker to 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 information already made available to the public, unless that record has been included in a report about an individual shared with a third party.

(iv) Any other circumstance in which an information broker may limit access to information that the Commission determines to be appropriate.

(E) FCRA REGULATED PERSONS.—A provision that any information broker that 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 is deemed to be in compliance with this paragraph with respect to such information.

(F) REQUIREMENT OF AUDIT LOG OF ACCESSED AND TRANSMITTED INFORMATION.—Each information broker 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.

(4) PROHIBITION ON PRETEXTING BY INFORMATION BROKERS.—The regulations promulgated pursuant to subsection (a) shall include a prohibition on the following:

(A) PROHIBITION ON OBTAINING PERSONAL INFORMATION BY FALSE PRETENSES.—An information broker to obtain, attempt to obtain, 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—

(I) to be forged, counterfeit, lost, stolen, or fraudulently obtained; or

(II) to contain a false, fictitious, or fraudulent statement or representation.

(B) PROHIBITION ON SOLICITATION TO OBTAIN PERSONAL INFORMATION UNDER FALSE PRETENSES.—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.—Not later than 1 year after the date of enactment of this Act, the Commis-

sion shall promulgate regulations under section 553 of title 5, United States Code, that require the following:

(1) IN GENERAL.—Each covered entity to, 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 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 clause 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 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 clause by a subsequent written request if further delay is necessary.

(3) COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.—If a covered entity is required to provide notification to more than 5,000 individuals under paragraph (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 credit 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.

(4) METHOD AND CONTENT OF NOTIFICATION.—

(A) GENERAL NOTIFICATION.—A covered entity required to provide notification to individuals under paragraph (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):

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

(ii) 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).

(B) 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.

(C) 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 entity 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.

(D) CONTENT OF NOTIFICATION.—

(i) IN GENERAL.—Any notification provided under subparagraph (A), (B), or (C) 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 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;

(III) 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 10 years, or credit monitoring or other service that enables consumers to detect the misuse of their personal information for a period of 10 years, and instructions to the individual on requesting such reports or service from the covered entity;

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

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

(ii) DIRECT BUSINESS RELATIONSHIP.—Any notification provided under this subsection shall identify the covered

entity that has a direct business relationship with the individual.

(E) SUBSTITUTE NOTIFICATION.—Criteria for determining circumstances under which substitute notification may be provided in lieu of direct notification required by subparagraph (A), including criteria for determining if notification under subparagraph (A) 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 the form and content of substitute notification.

(5) NOTIFICATION FOR LAW ENFORCEMENT AND OTHER PURPOSES.—A covered entity to, as expeditiously as practicable and without unreasonable delay, but not later than 7 days following the discovery of a breach of security, provide notification of the breach to—

(A) the Commission;

(B) the Federal Bureau of Investigation;

(C) the Secret Service;

(D) for common carriers, the Federal Communications Commission;

(E) for entities that provide a consumer financial product or service (as defined in section

1002 of the Consumer Financial Protection Act of 2010 (12 U.S.C. 5481)), the Consumer Financial Protection Bureau; and

(F) 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.

(6) OTHER OBLIGATIONS FOLLOWING BREACH.—

(A) IN GENERAL.—A covered entity required to provide notification under subsection (a) to, 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—

(i) consumer credit reports from the major credit reporting agencies beginning not later than 60 days following the individual's request and continuing on a quarterly basis for a period of 10 years thereafter; or

(ii) a credit monitoring or other service that 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 10 years.

(B) RULEMAKING.—The circumstances under which a covered entity required to provide notification under paragraph (1) shall provide or arrange for the provision of free consumer credit reports or credit monitoring or other service to affected individuals.

(b) WEBSITE NOTIFICATION.—

(1) FEDERAL TRADE COMMISSION.—If the Commission, upon receiving notification of any breach of security that is reported to the Commission under subsection (a)(5)(A), finds that notification of such a breach of security through the website of the Commission 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 the website.

(2) OTHER FEDERAL AGENCY.—If another Federal agency (such as the Federal Communications Commission, the Consumer Financial Protection Bu-

reau, or the Department of Justice) receives notice of a breach of security from a covered entity and finds that notification of such a breach of security through the website of the Commission would be in the public interest or for the protection of consumers, that Federal agency shall place such a notification in a clear and conspicuous location on the website of that agency.

(c) 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 through 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.

(d) 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.

(e) 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.

(f) WEBSITE ON DATA SECURITY BEST PRACTICES.—The Commission shall establish and maintain an internet website containing non-binding 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.

(g) 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 product or technology, including any specific computer software or hardware.

(h) 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 pro-

vide notification to individuals following a breach of security, 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 a regulation promulgated under 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 Act.

(2) COORDINATION WITH FEDERAL COMMUNICATIONS COMMISSION.—In the case of enforcement under this Act that relates to entities subject to the authority of the Federal Communications Commission, enforcement actions by the Commission

shall be coordinated with the Federal Communications Commission.

(3) COORDINATION WITH CONSUMER FINANCIAL PROTECTION BUREAU.—In the case of enforcement under this Act that relates to entities that provide a consumer financial product or service (as defined in section 1002 of the Consumer Financial Protection Act of 2010 (12 U.S.C. 5481)), enforcement actions by the Commission shall 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 appropriate 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 section 2 or 3, as applicable;

(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 to be determined by the Commission. Such amount determined by the Commission shall be adjusted as described in the Federal Civil Penalties Inflation Adjustment Act of 1990 (Public Law 101–410; 28 U.S.C. 2461 note).

(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 to be determined by the Commission. Each failure to send notification as required under section 3 to a citizen or 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) IN GENERAL.—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 a 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, sale of, release of, or use of data containing personal information.

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

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

(A) any person, partnership, or corporation 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.

(4) NONPROFIT ORGANIZATION.—The term ''nonprofit organization'' means an organization described in section 501(c) of the Internal Revenue

Code of 1986 that is exempt from taxation under section 501(a) of such Code.

(5) INFORMATION BROKER.—The term ''information broker'' means any individual, person, partnership, or corporation that collects personal information, sells personal information, or profits from personal information in any way.

(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 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 fingerprint, voice print, retina or iris image, facial recognition data, or any other unique physical representation.

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

(vii) Any security code, access code, password, or source code that could be used to generate such codes or passwords, in combination with either 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.

(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 communication such as a text, SMS, MMS, RCS, and other electronic message or other user-created content such as an email, photograph, or video.

(xiii) Any record or information concerning payroll, income, financial account, mortgage, loan, line of credit, utility bill, accumulated purchase, or any other information regarding a financial asset, obligation, or spending habit.

(xiv) Any additional element the Commission defines as personal information in accordance with subparagraph (B).

(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) SMALL BUSINESS CONCERN.—The term ''small business concern'' has the meaning given that term in section 3 of the Small Business Act (15 U.S.C. 632).

(8) 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) EFFECT ON STATE DATA SECURITY AND BREACH NOTIFICATION LAWS.—This Act supersedes any provision of a statute or regulation of a State or political subdivision of a State, with respect to a covered entity, that expressly—

(1) requires information security practices for the treatment and protection of personal information similar to any of those required under section 2; or

(2) requires notification to individuals of a breach of security of personal information.

(b) EFFECT ON OTHER STATE LAWS.—Except as provided in subsection (a), 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) 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

(3) 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.

(c) PRESERVATION OF AUTHORITY.—Nothing in this Act may be construed in any way to limit or affect the authority of the Commission, the Federal Communication Commission, or the Consumer Financial Protection Bureau 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.

○