I

112TH CONGRESS
1ST SESSION

H. R. 1841

To protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information, and to provide for nationwide notice in the event of a security breach.

IN THE HOUSE OF REPRESENTATIVES

MAY 11, 2011

Mr. STEARNS (for himself and Mr. MATHESON) introduced the following bill; which was referred to the Committee on Energy and Commerce

---

A BILL

To protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information, and to provide for nationwide notice in the event of a security breach.

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 (DATA) of 2011''.

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 person engaged in interstate commerce that owns or possesses data in electronic form containing personal information, or contracts to have any third party entity maintain such data for such person, 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 person;

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

(C) the cost of implementing such safeguards.

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

(A) A 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 maintained by such person that contains such electronic data, which shall include regular monitoring for a breach of security of such system.

(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.

(E) A process for disposing of obsolete data in electronic form 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.

(3) TREATMENT OF ENTITIES GOVERNED BY OTHER LAW.—In promulgating the regulations under this subsection, the Commission may determine to be in compliance with this subsection any person who is required under any other Federal law to maintain standards and safeguards for information security and protection of personal information that provide equal or greater protection than those required under this subsection.

(b) DESTRUCTION OF OBSOLETE PAPER RECORDS CONTAINING PERSONAL INFORMATION.—

(1) STUDY.—Not later than 1 year after the date of enactment of this Act, the Commission shall conduct a study on the practicality of requiring a standard method or methods for the destruction of obsolete paper documents and other non-electronic data containing personal information by persons engaged in interstate commerce who own or possess such paper documents and non-electronic data. The study shall consider the cost, benefit, feasibility, and effect of a requirement of shredding or other permanent destruction of such paper documents and non-electronic data.

(2) REGULATIONS.—The Commission may promulgate regulations under section 553 of title 5, United States Code, requiring a standard method or methods for the destruction of obsolete paper documents and other non-electronic data containing personal information by persons engaged in interstate commerce who own or possess such paper documents and non-electronic data if the Commission finds that—

(A) the improper disposal of obsolete paper documents and other non-electronic data creates a reasonable risk of identity theft, fraud, or other unlawful conduct;

(B) such a requirement would be effective in preventing identity theft, fraud, or other unlawful conduct;

(C) the benefit in preventing identity theft, fraud, or other unlawful conduct would outweigh the cost to persons subject to such a requirement; and

(D) compliance with such a requirement would be practicable.

In enforcing any such regulations, the Commission may determine to be in compliance with such regulations any person who is required under any other

Federal law to dispose of obsolete paper documents and other non-electronic data containing personal information if such other Federal law provides equal or greater protection of personal information than the regulations promulgated under this subsection.

(c) SPECIAL REQUIREMENTS FOR INFORMATION BROKERS.—

(1) SUBMISSION OF POLICIES TO THE FTC.—The regulations promulgated under subsection (a) shall require information brokers to submit their 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 shall conduct an audit of the information security practices of such information broker, or require the information broker to conduct an independent audit of such practices (by an independent auditor who has not audited such information broker's security practices during the preceding 5 years). The Commission may conduct or require additional audits for a period of 5 years following the breach of security or until the Commission determines that the security practices of the information

broker are in compliance with the requirements of this section and are adequate to prevent further breaches of security.

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

(A) VERIFICATION.—Each information broker shall establish reasonable procedures to verify the accuracy of the personal information it collects, assembles, or maintains, and any other information it collects, assembles, or maintains that specifically identifies an individual, other than information which merely identifies an individual's name or address.

(B) CONSUMER ACCESS TO INFORMATION.—

(i) ACCESS.—Each information broker shall—

(I) provide to each individual whose personal information it maintains, at the individual's request at least 1 time 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 its Internet website (if the information broker maintains such a website) instructing individuals how to request access to the information required to be provided under subclause (I).

(ii) 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)(aa) in the case of information that is public record information, inform the individual of the source of the information, and, if reasonably available, where a request for correction may be directed; or

(bb) in the case of information that is non-public 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.

(iii) LIMITATIONS.—An information broker may limit the access to information required under subparagraph (B) 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.

(iv) RULEMAKING.—The Commission shall issue regulations, as necessary, under section 553 of title 5, United States Code, on the application of the limitations in clause (iii).

(C) TREATMENT OF ENTITIES GOVERNED BY OTHER LAW.—The Commission may promulgate rules (under section 553 of title 5, United States Code) to determine to be in compliance with this paragraph any person who is a consumer reporting agency, as defined in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f)), with respect to those products and services that are subject to and in compliance with the requirements of that Act.

(4) REQUIREMENT OF AUDIT LOG OF ACCESSED AND TRANSMITTED INFORMATION.—Not later than 1 year after the date of the 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 in

electronic form 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 infor-

mation 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).

(d) EXEMPTION FOR TELECOMMUNICATIONS CARRIER, CABLE OPERATOR, PROVIDER OF INFORMATION SERVICE, OR INTERACTIVE COMPUTER SERVICE.—Nothing in this section shall apply to any electronic communication by a third party stored by a telecommunications carrier (as defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153)), cable operator (as defined in section 602 of such Act (47 U.S.C. 522)), provider of information service (as defined in such section 3), or interactive computer service (as defined in section 230(f)(2) of such Act (47 U.S.C. 230(f)(2))).

SEC. 3. NOTIFICATION OF INFORMATION SECURITY BREACH.

(a) NATIONWIDE NOTIFICATION.—Any person engaged in interstate commerce that owns or possesses data in electronic form containing personal information shall, following the discovery of a breach of security of the system maintained by such person that contains such data—

(1) notify each individual who is a citizen or resident of the United States whose personal information was acquired by an unauthorized person as a result of such a breach of security; and

(2) notify the Commission.

(b) SPECIAL NOTIFICATION REQUIREMENT FOR CERTAIN ENTITIES.—

(1) THIRD PARTY AGENTS.—In the event of a breach of security by any third party entity that has been contracted to maintain or process data in electronic form containing personal information on behalf of any other person who owns or possesses such data, such third party entity shall be required only to notify such person of the breach of security. Upon receiving such notification from such third party, such person shall provide the notification required under subsection (a).

(2) TELECOMMUNICATIONS CARRIERS, CABLE OPERATORS, PROVIDERS OF INFORMATION SERVICE, AND INTERACTIVE COMPUTER SERVICES.—If a telecommunications carrier (as defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153)), cable operator (as defined in section 602 of such Act (47 U.S.C. 522)), provider of information service (as defined in such section 3), or interactive computer

service (as defined in section 230(f)(2) of such Act (47 U.S.C. 230(f)(2))) becomes aware of a breach of security during the transmission of data in electronic form containing personal information that is owned or possessed by another person utilizing the means of transmission of such telecommunications carrier, cable operator, provider of information service, or interactive computer service, such telecommunications carrier, cable operator, provider of information service, or interactive computer service shall be required only to notify the person who initiated such transmission of such a breach of security if such person can be reasonably identified. Upon receiving such notification from a telecommunications carrier, cable operator, provider of information service, or interactive computer service, such person shall provide the notification required under subsection (a). Notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), the Commission shall have the authority to enforce this paragraph with respect to a telecommunications carrier.

(3) BREACH OF HEALTH INFORMATION.—If the Commission receives a notification of a breach of security and determines that information included in

such breach is individually identifiable health information (as such term is defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6))), the Commission shall send a copy of such notification to the Secretary of Health and Human Services.

(c) TIMELINESS OF NOTIFICATION.—All notifications required under subsection (a) shall be made as promptly as possible and without unreasonable delay following the discovery of a breach of security of the system and consistent with any measures necessary to determine the scope of the breach, prevent further breach or unauthorized disclosures, and reasonably restore the integrity of the data system.

(d) METHOD AND CONTENT OF NOTIFICATION.—

(1) DIRECT NOTIFICATION.—

(A) METHOD OF NOTIFICATION.—A person required to provide notification to individuals under subsection (a)(1) shall be in compliance with such requirement if the person 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.

(ii) Email notification, if—

(I) the person's primary method of communication with the individual is by email; 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 notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).

(B) CONTENT OF NOTIFICATION.—Regardless of the method by which notification is provided to an individual under subparagraph (A), such notification shall include—

(i) a description of the personal information that was acquired by an unauthorized person;

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

(iii) notice 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, and instructions to the individual on requesting such reports from the person;

(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.

(2) SUBSTITUTE NOTIFICATION.—

(A) CIRCUMSTANCES GIVING RISE TO SUBSTITUTE NOTIFICATION.—A person required to provide notification to individuals under subsection (a)(1) may provide substitute notification in lieu of the direct notification required by paragraph (1) if—

(i) the person owns or possesses data in electronic form containing personal information of fewer than 1,000 individuals; and

(ii) such direct notification is not feasible due to—

(I) excessive cost to the person required to provide such notification relative to the resources of such person, as determined in accordance with the regulations issued by the Commission under paragraph (3)(A); or

(II) lack of sufficient contact information for the individual required to be notified.

(B) FORM OF SUBSTITUTE NOTICE.—Such substitute notification shall include—

(i) email notification to the extent that the person has email addresses of individuals to whom it is required to provide notification under subsection (a)(1);

(ii) a conspicuous notice on the Internet website of the person (if such person maintains such a website); and

(iii) notification in print and to broadcast media, including major media in metropolitan and rural areas where the individuals whose personal information was acquired reside.

(C) CONTENT OF SUBSTITUTE NOTICE.—Each form of substitute notice under this paragraph shall include—

(i) notice that individuals whose personal information is included in the breach of security are entitled to receive, at no cost to the individuals, consumer credit reports on a quarterly basis for a period of 2 years, and instructions on requesting such reports from the person; and

(ii) a telephone number by which an individual can, at no cost to such individual, learn whether that individual's personal information is included in the breach of security.

(3) FEDERAL TRADE COMMISSION REGULATIONS AND GUIDANCE.—

(A) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall, by regulations under section 553 of title 5, United States Code, establish criteria for determining the circumstances under which substitute notification may be provided under paragraph (2), including criteria for determining if notification under paragraph (1) is

not feasible due to excessive cost to the person required to provide such notification relative to the resources of such person.

(B) GUIDANCE.—In addition, the Commission shall provide and publish general guidance with respect to compliance with this section. Such guidance shall include—

(i) a description of written or email notification that complies with the requirements of paragraph (1); and

(ii) guidance on the content of substitute notification under paragraph (2)(B), including the extent of notification to print and broadcast media that complies with the requirements of such paragraph.

(e) OTHER OBLIGATIONS FOLLOWING BREACH.—A person 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, consumer credit reports from at least one of the major credit reporting agencies beginning not later than 2 months following the discovery of a breach of security and continuing on a quarterly basis for a period of 2 years thereafter.

(f) EXEMPTION.—

(1) GENERAL EXEMPTION.—A person shall be exempt from the requirements under this section if, following a breach of security, such person determines that there is no reasonable risk of identity theft, fraud, or other unlawful conduct.

(2) PRESUMPTIONS.—

(A) ENCRYPTION.—The encryption of data in electronic form shall establish a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security of such data. Any such presumption may be rebutted by facts demonstrating that the encryption has been or is reasonably likely to be compromised.

(B) ADDITIONAL METHODOLOGIES OR TECHNOLOGIES.—Not later than 270 days after the date of the enactment of this Act, the Commission shall, by rule pursuant to section 553 of title 5, United States Code, identify any additional security methodology or technology, other than encryption, which renders data in electronic form unreadable or indecipherable, that shall, if applied to such data, establish a presumption that no reasonable risk of identity

theft, fraud, or other unlawful conduct exists following a breach of security of such data. Any such presumption may be rebutted by facts demonstrating that any such methodology or technology has been or is reasonably likely to be compromised. In promulgating such a rule, the Commission shall consult with relevant industries, consumer organizations, and data security and identity theft prevention experts and established standards setting bodies.

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

(g) WEBSITE NOTICE OF FEDERAL TRADE COMMISSION.—If the Commission, upon receiving notification of any breach of security that is reported to the Commission under subsection (a)(2), finds that notification of such a breach of security via the Commission's Internet website would be in the public interest or is necessary for the protection of consumers, the Commission shall place such a notice in a clear and conspicuous location on its Internet website.

(h) 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 (d)(1) to be provided in a language in addition to English to individuals known to speak only such other language.

SEC. 4. 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.

(2) POWERS OF COMMISSION.—The Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any person who violates such regulations shall be subject to the penalties and entitled to the privileges and immunities provided in that Act.

(3) RULES.—

(A) IN GENERAL.—The Commission shall promulgate, under section 553 of title 5, United States Code, such rules as may be necessary to carry out the provisions of this Act.

(B) 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.

(b) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) CIVIL ACTION.—In any case in which the attorney general of a State, or an official or agency of a State, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any person who violates section 2 or 3 of this Act, the attorney general, official, or agency of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction—

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

(B) to compel compliance with such section; or

(C) to obtain civil penalties in the amount determined under paragraph (2).

(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 violations of such section by an amount not greater than $11,000. Each day that a person is not in compliance with the requirements of such section shall be treated as a separate violation. The maximum civil penalty calculated under this clause shall not exceed $5,000,000.

(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 $11,000. Each failure to send notification as required under section 3 to a resident of the State shall be treated as a separate violation. The maximum civil penalty calculated under this clause shall not exceed $5,000,000.

(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) INTERVENTION BY THE FTC.—

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

instituting such action. The Commission shall have the right—

(i) to intervene in the action;

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

(iii) to file petitions for appeal.

(B) 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) CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(c) AFFIRMATIVE DEFENSE FOR A VIOLATION OF SECTION 3.—It shall be an affirmative defense to an enforcement action brought under subsection (a), or a civil action brought under subsection (b), based on a violation of section 3, that all of the personal information contained in the data in electronic form that was acquired as a result of a breach of security of the defendant is public record information that is lawfully made available to the general public from Federal, State, or local government records and was acquired by the defendant from such records.

SEC. 5. DEFINITIONS.

In this Act the following definitions apply:

(1) BREACH OF SECURITY.—The term ''breach of security'' means the unauthorized acquisition of data in electronic form containing personal information.

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

(3) DATA IN ELECTRONIC FORM.—The term ''data in electronic form'' means any data stored electronically or digitally on any computer system or

other database and includes recordable tapes and other mass storage devices.

(4) ENCRYPTION.—The term ''encryption'' means the protection of data in electronic form in storage or in transit using an encryption technology that has been adopted by an established standards setting body which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data. Such encryption must include appropriate management and safeguards of such keys to protect the integrity of the encryption.

(5) IDENTITY THEFT.—The term ''identity theft'' means the unauthorized use of another person's personal information for the purpose of engaging in commercial transactions under the name of such other person.

(6) INFORMATION BROKER.—The term ''information broker'' 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.

(7) PERSONAL INFORMATION.—

(A) DEFINITION.—The term ''personal information'' means an individual's first name or initial and last name, or address, or phone number, in combination with any 1 or more of the following data elements for that individual:

(i) Social Security number.

(ii) Driver's license number or other State identification number.

(iii) Financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual's financial account.

(B) MODIFIED DEFINITION BY RULEMAKING.—The Commission may, by rule, modify the definition of ''personal information'' under subparagraph (A) to the extent that such modification is necessary to accommodate changes in technology or practices, will not unreasonably impede interstate commerce, and will accomplish the purposes of this Act.

(8) PUBLIC RECORD INFORMATION.—The term ''public record information'' means information about an individual which has been obtained originally from records of a Federal, State, or local government entity that are available for public inspection.

(9) NON-PUBLIC INFORMATION.—The term ''non-public information'' means information about an individual that is of a private nature and neither available to the general public nor obtained from a public record.

SEC. 6. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE INFORMATION SECURITY LAWS.—This Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State, with respect to those entities covered by the regulations issued pursuant to this Act, that expressly—

(1) requires information security practices and treatment of data in electronic form containing personal information similar to any of those required under section 2; and

(2) requires notification to individuals of a breach of security resulting in unauthorized acquisition of data in electronic form containing personal information.

(b) ADDITIONAL PREEMPTION.—

(1) IN GENERAL.—No person other than the attorney general of a State may bring a civil action under the laws of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act.

(2) PROTECTION OF CONSUMER PROTECTION LAWS.—This subsection shall not be construed to limit the enforcement of any State consumer protection law by an attorney general of a State.

(c) PROTECTION OF CERTAIN STATE LAWS.—This Act shall not be construed to preempt the applicability of—

(1) State trespass, contract, or tort law; or

(2) other State laws to the extent that those laws relate to acts of fraud.

(d) PRESERVATION OF FTC AUTHORITY.—Nothing in this Act may be construed in any way to limit or affect the Commission's authority under any other provision of law, including the authority to issue advisory opinions (under subpart A of part 1 of title 16, Code of Federal Regulations), policy statements, or guidance regarding this Act.

SEC. 7. EFFECTIVE DATE AND SUNSET.

(a) EFFECTIVE DATE.—This Act shall take effect 1 year after the date of enactment of this Act.

(b) SUNSET.—This Act shall cease to be in effect on September 30, 2016.

SEC. 8. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated to the Commission $1,000,000 for each of fiscal years 2012 through 2016 to carry out this Act.

○