111TH CONGRESS
2D SESSION

S. 3742

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

IN THE SENATE OF THE UNITED STATES

AUGUST 5, 2010

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

---

A BILL

To protect consumers by requiring reasonable security policies and procedures to protect 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 Security and Breach Notification Act of 2010''.

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 every covered entity that owns or possesses data containing personal information, or contracts to have any third party entity maintain such data for such 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 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 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.

(E) A process for disposing of 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 indecipherable.

(F) A standard method or methods for the destruction of paper documents and other non-electronic data containing personal information.

(3) TREATMENT OF ENTITIES GOVERNED BY OTHER LAW.—Any covered entity that 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 paragraph (1), 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 of a security breach under section 3, the Commission may con-

duct 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 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.

(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 indi-

vidual 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.—

(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), and, as applicable, how to express a preference with respect to the use of personal information for marketing purposes under clause (iii).

(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 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

(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) ALTERNATIVE PROCEDURE FOR CERTAIN MARKETING INFORMATION.—In

accordance with regulations issued under clause (v), an information broker that maintains any information described in clause (i) 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 clauses (i) and (ii), provide each individual whose information it 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.

(iv) LIMITATIONS.—An information broker may limit the access to information required under subparagraph (B)(i)(I) and is not required to provide notice to individuals as required under subparagraph (B)(i)(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, child protection, 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.

(v) RULEMAKING.—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 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 clause (iv), including any additional circumstances in which an information broker may limit access to information under such clause that the Commission determines to be appropriate.

(C) 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 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 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 transmission of, any data containing personal information collected, assembled, or maintained by such information broker. The Commission may provide exceptions to such requirements for the purposes of furthering or protecting law enforcement or national security activities.

(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).

(c) EXEMPTION FOR CERTAIN SERVICE PROVIDERS.—Nothing in this section shall apply to a service provider for any electronic communication by a third party to the extent that the service provider is exclusively engaged in the transmission, routing, or temporary, intermediate, or transient storage of that communication.

SEC. 3. NOTIFICATION OF INFORMATION SECURITY BREACH.

(a) NATIONWIDE NOTIFICATION.—Any covered entity 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 covered entity that contains such data—

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

(2) notify the Commission.

(b) SPECIAL NOTIFICATION REQUIREMENTS.—

(1) THIRD PARTY AGENTS.—In the event of a breach of security of the system maintained 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 covered entity who owns or possesses such data, such third

party entity shall be required to notify such covered entity of the breach of security. Upon receiving such notification from such third party, such covered entity shall provide the notification required under subsection (a).

(2) SERVICE PROVIDERS.—If a service provider becomes aware of a breach of security of data in electronic form containing personal information that is owned or possessed by another covered entity that connects to or uses a system or network provided by the service provider for the purpose of transmitting, routing, or providing intermediate or transient storage of such data, such service provider shall be required to notify of such a breach of security only the covered entity who initiated such connection, transmission, routing, or storage if such covered entity can be reasonably identified. Upon receiving such notification from a service provider, such covered entity shall provide the notification required under subsection (a).

(3) COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.—If a covered entity is required to provide notification to more than 5,000 individuals under subsection (a)(1), the covered entity also shall notify the major credit report-

ing agencies that compile and maintain files on consumers on a nationwide basis, of the timing and distribution of the notices. Such notice shall be given to the credit reporting agencies without unreasonable delay and, if it will not delay notice to the affected individuals, prior to the distribution of notices to the affected individuals.

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—Unless subject to a delay authorized under paragraph (2), a notification required under subsection (a) shall be made not later than 60 days following the discovery of a breach of security, unless the covered entity providing notice can show that providing notice within such a time frame is not feasible due to circumstances necessary to accurately identify affected consumers, or to prevent further breach or unauthorized disclosures, and reasonably restore the integrity of the data system, in which case such notification shall be made as promptly as possible.

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

(A) LAW ENFORCEMENT.—If a Federal, State, or local law enforcement agency deter-

mines 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. 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.

(B) 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 paragraph

by a subsequent written request if further delay is necessary.

(d) METHOD AND CONTENT OF NOTIFICATION.—

(1) DIRECT NOTIFICATION.—

(A) METHOD OF 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):

(i) Written notification.

(ii) Notification by e-mail or other electronic means, if—

(I) the covered entity's primary method of communication with the individual is by e-mail 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 notices under section 101 of the Elec-

tronic Signatures in Global 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) the date, estimated date, or estimated date range of the breach of security;

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

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

(iv) 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, 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;

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

(vi) 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 covered entity 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 the covered entity owns or possesses data in electronic form containing personal information of fewer than

1,000 individuals and such direct notification is not feasible due to—

(i) excessive cost to the covered entity required to provide such notification relative to the resources of such covered entity, 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 NOTIFICATION.—Such substitute notification shall include—

(i) e-mail notification to the extent that the covered entity has e-mail 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 covered entity (if such covered entity maintains such a website); and

(iii) notification in print and to broadcast media, including major media in met-

ropolitan 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, 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 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; and

(ii) a telephone number by which an individual can, at no cost to such indi-

vidual, learn whether that individual's personal information is included in the breach of security.

(3) REGULATIONS AND GUIDANCE.—

(A) REGULATIONS.—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, establish criteria for determining 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 costs to the covered entity required to provided such notification relative to the resources of such covered entity. Such regulations may also identify other circumstances where substitute notification would be appropriate for any covered entity, including circumstances under which the cost of providing notification exceeds the benefits to consumers.

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

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

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

(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 at least one of 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 2 years thereafter; or

(B) 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 2 years.

(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 (d)(3), the Commission shall—

(A) determine the circumstances under which a covered entity required to provide notification under subsection (a)(1) shall provide or arrange for the provision of free consumer credit reports or credit monitoring or other service to affected individuals; and

(B) establish a simple process under which a covered entity that is a small business or small non-profit organization may request a partial waiver or a modified or alternative means of responding if providing or arranging for such reports, monitoring, or service is not feasible due to excessive costs relative to the resources of the small business or small non-profit entity and the level of harm to consumers caused by the data breach.

(f) EXEMPTION.—

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

(2) PRESUMPTION.—

(A) IN GENERAL.—If the data in electronic form containing personal information is rendered unusable, unreadable, or indecipherable through a security technology or methodology (if the technology or methodology is generally accepted by experts in the information security field), there shall be 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 security technologies or methodologies in a specific case, have been or are reasonably likely to be compromised.

(B) METHODOLOGIES OR TECHNOLOGIES.—Not later than 1 year after the date of the enactment of this Act and bian-

nually thereafter, the Commission, after consultation with the National Institute of Standards and Technology, shall issue rules (pursuant to section 553 of title 5, United States Code) or guidance to identify security methodologies or technologies, such as encryption, which render data in electronic form unusable, 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 in a specific case has been or is reasonably likely to be compromised. In issuing such rules or guidance, the Commission also 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, after consultation with the National Institute of Standards and Technology, shall issue guid-

ance 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 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.

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

(j) 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 secu-

rity, and that, taken as a whole, provides protections substantially similar to, or greater than, those required under this section, as the Commission shall determine by rule (under section 553 of title 5, United States Code), shall be deemed to be in compliance with this section.

SEC. 4. APPLICATION AND ENFORCEMENT.

(a) GENERAL APPLICATION.—The requirements of sections 2 and 3 apply to—

(1) those persons, partnerships, or corporations 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)); and

(2) notwithstanding section 4 and section 5(a)(2) of that Act (15 U.S.C. 44 and 45(a)(2)), any non-profit 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 such Code.

(b) 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 covered entity who violates such regulations shall be subject to the penalties and entitled to the privileges and immunities provided in that Act.

(3) 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.

(c) 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 covered entity 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;

(C) to obtain damages, restitution, or other compensation on behalf of such residents, or to obtain such further and other relief as the court may deem appropriate; or

(D) 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)(D) 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 $11,000.

(ii) TREATMENT OF VIOLATIONS OF SECTION 3.—For purposes of paragraph (1)(D) 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.

(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) and in clauses (i) and (ii) of subparagraph (C) 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.

(C) MAXIMUM TOTAL LIABILITY.—Notwithstanding the number of actions which may be brought against a covered entity under this

subsection the maximum civil penalty for which any covered entity may be liable under this subsection shall not exceed—

(i) $5,000,000 for each violation of section 2; and

(ii) $5,000,000 for all violations of section 3 resulting from a single breach of security.

(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.

(d) AFFIRMATIVE DEFENSE FOR A VIOLATION OF SECTION 3.—

(1) IN GENERAL.—It shall be an affirmative defense to an enforcement action brought under subsection (b), or a civil action brought under subsection (c), based on a violation of section 3, that all of the personal information contained in the data in electronic form that was acquired or accessed 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.

(2) NO EFFECT ON OTHER REQUIREMENTS.—Nothing in this subsection shall be construed to exempt any covered entity from the requirement to notify the Commission of a breach of security as required under section 3(a).

SEC. 5. DEFINITIONS.

In this Act the following definitions apply:

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

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

(3) COVERED ENTITY.—The term ''covered entity'' means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity, and any charitable, educational, or nonprofit organization, that acquires, maintains, or utilizes personal information.

(4) 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.

(5) 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.

(6) 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.

(7) 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 or on behalf of and received from or on behalf of a nonaffiliated third party concerning individuals who are current or former customers or employees of such third party to enable such third party directly or through parties acting on its behalf to: (1) provide benefits for its employees; or (2) directly transact business with its customers.

(8) MAJOR CREDIT REPORTING AGENCY.—The term ''major credit reporting agency'' means a consumer reporting agency that compiles and maintains files on consumers on a nationwide basis within the meaning of section 603(p) of the Fair Credit Reporting Act (5 U.S.C. 1681a(p)).

(9) 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, passport number, military identification number, or other similar number issued on a government document used to verify identity.

(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 promulgated under section 553 of title 5, United States Code, modify the definition of ''personal information'' under subparagraph (A)—

(i) for the purpose of section 2 to the extent that such modification will not unreasonably impede interstate commerce, and will accomplish the purposes of this Act; or

(ii) for the purpose of section 3, 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.

(10) 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.

(11) 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.

(12) SERVICE PROVIDER.—The term ''service provider'' means a covered entity that provides electronic data transmission, routing, intermediate and transient storage, or connections to its system or network, where the covered entity providing such services does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and such covered entity trans-

mits, routes, stores, or provides connections for personal information in a manner that personal information is undifferentiated from other types of data that such covered entity transmits, routes, stores, or provides connections. Any such covered entity shall be treated as a service provider under this Act only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage or connections.

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 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 access to or acquisition of data in electronic form containing personal information.

(b) ADDITIONAL PREEMPTION.—

(1) IN GENERAL.—No person other than a person specified in section 4(c) 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.—Except as provided in subsection (a) of this section, 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.

SEC. 7. EFFECTIVE DATE.

This Act shall take effect 1 year after the date of enactment of this Act.

SEC. 8. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Commission $1,000,000 for each of fiscal years 2011 through 2015 to carry out this Act.

○