115TH CONGRESS
1ST SESSION

S. _____

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 breach of security.

IN THE SENATE OF THE UNITED STATES

Mr. NELSON (for himself, Mr. BLUMENTHAL, and Ms. BALDWIN) introduced the following bill; which was read twice and referred to the Committee on _____

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 breach of security.

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''.

SEC. 2. REQUIREMENTS FOR INFORMATION SECURITY.

(a) GENERAL SECURITY POLICIES AND PROCEDURES.—

(1) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to require each covered entity that owns or possesses data containing personal information, or contracts to have any third-party entity maintain or process 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;

(C) the cost of implementing the safeguards under subparagraph (B); and

(D) the impact on small businesses and nonprofits.

(2) REQUIREMENTS.—The 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 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 each system maintained by the covered entity that contains such personal information, including regular monitoring for a breach of security of each such system.

(D) A process for taking preventive and corrective action to mitigate any vulnerabilities identified in the process required by subparagraph (C), that may include implementing any changes to information 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 destroying, 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.

(b) LIMITATIONS.—

(1) COVERED ENTITIES SUBJECT TO THE GRAMM-LEACH-BLILEY ACT.—A financial institution that is subject to title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) and is in compliance with information security requirements under that Act shall be deemed in compliance with this section.

(2) APPLICABILITY OF OTHER INFORMATION SECURITY REQUIREMENTS.—A person who is subject to, and in compliance with, the information security requirements of section 13401 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931) or of section 1173(d) of title XI, part C of the Social Security Act (42 U.S.C. 1320d–2(d)) shall be deemed in compliance with this section with respect to any data governed by section 13401 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931) or by the Health Insurance Port-

ability and Accountability Act of 1996 Security Rule (45 C.F.R. 160.103 and part 164).

SEC. 3. NOTIFICATION OF BREACH OF SECURITY.

(a) NATIONWIDE NOTIFICATION.—A covered entity that owns or possesses data in electronic form containing personal information, following the discovery of a breach of security of the system maintained by the covered entity that contains such data, shall notify—

(1) each individual who is a citizen or resident of the United States and whose personal information was or is reasonably believed to have been acquired or accessed from the covered entity as a result of the breach of security; and

(2) the Commission, unless the covered entity has notified the designated entity under section 4.

(b) SPECIAL NOTIFICATION REQUIREMENTS.—

(1) THIRD-PARTY ENTITIES.—In the event of a breach of security of a system maintained by a 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, the third-party entity shall notify the covered entity of the breach of security. Upon receiving notification from

the third party entity, such covered entity shall provide the notification required under subsection (a).

(2) 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 each major credit reporting agency of the timing and distribution of the notices, except when the only personal information that is the subject of the breach of security 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. Such notice shall be given to each credit reporting agency 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.—Notification under subsection (a) shall be made—

(1) not later than 30 days after the date of discovery of a breach of security; or

(2) as promptly as possible if the covered entity providing notice can show that providing notice within the timeframe under paragraph (1) is not feasible due to circumstances necessary—

(A) to accurately identify affected consumers;

(B) to prevent further breach or unauthorized disclosures; or

(C) to reasonably restore the integrity of the data system.

(d) METHOD AND CONTENT OF NOTIFICATION.—

(1) DIRECT NOTIFICATION.—

(A) METHOD OF DIRECT NOTIFICATION.—A covered entity shall be in compliance with the notification requirement under subsection (a)(1) if—

(i) the covered entity provides conspicuous and clearly identified notification—

(I) in writing; or

(II) by e-mail or other electronic means if—

(aa) the covered entity's primary method of communication with the individual is by e-mail or such other electronic means; or

(bb) the individual has consented to receive notification by e-mail or such other electronic

means and such 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); and

(ii) the method of notification selected under clause (i) can reasonably be expected to reach the intended individual.

(B) CONTENT OF DIRECT NOTIFICATION.—Each method of direct notification under subparagraph (A) shall include—

(i) the date, estimated date, or estimated date range of the breach of security;

(ii) a description of each type of personal information that was or is reasonably believed to have been acquired or accessed as a result of the breach of security;

(iii) a telephone number that an individual can use at no cost to the individual to contact the covered entity to inquire about the breach of security or the infor-

mation the covered entity maintained or possessed about that individual;

(iv) notice that the individual may be entitled to consumer credit reports under subsection (e)(1);

(v) instructions how an individual can request consumer credit reports under subsection (e)(1);

(vi) a telephone number, that an individual can use at no cost to the individual, and an address to contact each major credit reporting agency; and

(vii) a telephone number, that an individual can use at no cost to the individual, and an Internet Web site address to obtain information regarding identity theft from the Commission.

(2) SUBSTITUTE NOTIFICATION.—

(A) CIRCUMSTANCES GIVING RISE TO SUBSTITUTE NOTIFICATION.—A covered entity required to provide notification under subsection (a)(1) may provide substitute notification instead of direct notification under paragraph (1)—

(i) if direct notification is not feasible due to a lack of sufficient contact information for the individual required to be notified; or

(ii) if the covered entity owns or possesses data in electronic form containing personal information of fewer than 10,000 individuals and direct notification is not feasible due to 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).

(B) METHOD OF SUBSTITUTE NOTIFICATION.—Substitute notification under this paragraph shall include—

(i) conspicuous and clearly identified notification by e-mail to the extent the covered entity has an e-mail address for an individual who is entitled to notification under subsection (a)(1);

(ii) conspicuous and clearly identified notification on the Internet Web site of the

covered entity if the covered entity maintains an Internet Web site; and

(iii) notification to 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 NOTIFICATION.—Each method of substitute notification under this paragraph shall include—

(i) the date, estimated date, or estimated date range of the breach of security;

(ii) a description of each type of personal information that was or is reasonably believed to have been acquired or accessed as a result of the breach of security;

(iii) notice that an individual may be entitled to consumer credit reports under subsection (e)(1);

(iv) instructions how an individual can request consumer credit reports under subsection (e)(1);

(v) a telephone number that an individual can use at no cost to the individual to contact the covered entity to inquire

about the breach of security or the information the covered entity maintained or possessed about that individual;

(vi) a telephone number, that an individual can use at no cost to the individual, and an address to contact each major credit reporting agency; and

(vii) a telephone number, that an individual can use at no cost to the individual, and an Internet Web site address to obtain information regarding identity theft from the Commission.

(3) REGULATIONS AND GUIDANCE.—

(A) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission, by regulation under section 553 of title 5, United States Code, shall establish criteria for determining circumstances under which substitute notification may be provided under paragraph (2), including criteria for determining if direct notification under paragraph (1) is not feasible due to excessive costs to the covered entity required to provide such notification relative to the resources of such covered entity. The regulations may also identify other

circumstances where substitute notification would be appropriate, including circumstances under which the cost of providing direct notification exceeds the benefits to consumers.

(B) GUIDANCE.—In addition, the Commission, in consultation with the Small Business Administration, shall provide and publish general guidance with respect to compliance with this subsection. The guidance shall include—

(i) a description of written or e-mail notification that complies with 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 paragraph (2)(B)(iii).

(e) OTHER OBLIGATIONS FOLLOWING BREACH.—

(1) IN GENERAL.—Not later than 60 days after the date of request by an individual who received notification under subsection (a)(1) and quarterly thereafter for 2 years, a covered entity required to provide notification under subsection (a)(1) shall provide, or arrange for the provision of, to the indi-

vidual at no cost, consumer credit reports from at least 1 major credit reporting agency.

(2) LIMITATION.—This subsection shall not apply if the only personal information that is the subject of the breach of security 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.—The Commission's rulemaking under subsection (d)(3) shall include—

(A) determination of the circumstances under which a covered entity required to provide notification under subsection (a)(1) must provide or arrange for the provision of free consumer credit reports; and

(B) establishment of a simple process under which a covered entity that is a small business or small nonprofit organization may request a full or a partial waiver or a modified or an alternative means of complying with this subsection if providing free consumer credit reports is not feasible due to excessive costs relative to the resources of such covered entity and relative to the level of harm, to affected individuals, caused by the breach of security.

(f) DELAY OF NOTIFICATION AUTHORIZED FOR NATIONAL SECURITY AND LAW ENFORCEMENT PURPOSES.—

(1) IN GENERAL.—If the United States Secret Service or the Federal Bureau of Investigation determines that notification under this section would impede a criminal investigation or a national security activity, notification shall be delayed upon written notice from the United States Secret Service or the Federal Bureau of Investigation to the covered entity that experienced the breach of security. Written notice from the United States Secret Service or the Federal Bureau of Investigation shall specify the period of delay requested for national security or law enforcement purposes.

(2) SUBSEQUENT DELAY OF NOTIFICATION.—

(A) IN GENERAL.—A covered entity shall provide notification under this section not later than 30 days after the day that the delay was invoked unless a Federal law enforcement or intelligence agency provides subsequent written notice to the covered entity that further delay is necessary.

(B) WRITTEN JUSTIFICATION REQUIREMENTS.—

(i) UNITED STATES SECRET SERVICE.—If the United States Secret Service instructs a covered entity to delay notification under this section beyond the 30-day period under subparagraph (A) (referred to in this clause as ''subsequent delay''), the United States Secret Service shall submit written justification for the subsequent delay to the Secretary of Homeland Security before the subsequent delay begins.

(ii) FEDERAL BUREAU OF INVESTIGATION.—If the Federal Bureau of Investigation instructs a covered entity to delay notification under this section beyond the 30-day period under subparagraph (A) (referred to in this clause as ''subsequent delay''), the Federal Bureau of Investigation shall submit written justification for the subsequent delay to the Attorney General before the subsequent delay begins.

(3) LAW ENFORCEMENT IMMUNITY.—No cause of action shall lie in any court against any Federal agency for acts relating to the delay of notification for national security or law enforcement purposes under this Act.

(g) GENERAL EXEMPTION.—

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

(2) PRESUMPTION.—

(A) IN GENERAL.—There shall be a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security if—

(i) the data is rendered unusable, unreadable, or indecipherable through a security technology or methodology; and

(ii) the security technology or methodology under clause (i) is generally accepted by experts in the information security field.

(B) REBUTTAL.—The presumption under subparagraph (A) may be rebutted by facts demonstrating that the security technology or methodology in a specific case has been or is reasonably likely to be compromised.

(3) TECHNOLOGIES OR METHODOLOGIES.—Not later than 1 year after the date of enactment of this Act, and biennially 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 each security technology and methodology under paragraph (2). In identifying each such security technology and methodology, the Commission and the National Institute of Standards and Technology shall—

(A) consult with relevant industries, consumer organizations, data security and identity theft prevention experts, and established standards setting bodies; and

(B) consider whether and in what circumstances a security technology or methodology currently in use, such as encryption, complies with the standards under paragraph (2).

(4) COMMISSION GUIDANCE.—Not later than 1 year after the date of enactment of this Act, the Commission, after consultation with the National Institute of Standards and Technology, shall issue guidance regarding the application of the exemption under paragraph (1).

(h) EXEMPTIONS FOR NATIONAL SECURITY AND LAW ENFORCEMENT PURPOSES.—

(1) IN GENERAL.—A covered entity shall be exempt from the requirements under this section if—

(A) a determination is made—

(i) by the United States Secret Service or the Federal Bureau of Investigation that notification of the breach of security could be reasonably expected to reveal sensitive sources and methods or similarly impede the ability of the Government to conduct law enforcement or intelligence investigations; or

(ii) by the Federal Bureau of Investigation that notification of the breach of security could be reasonably expected to cause damage to the national security; and

(B) the United States Secret Service or the Federal Bureau of Investigation, as the case may be, provides written notice of its determination under subparagraph (A) to the covered entity.

(2) UNITED STATES SECRET SERVICE.—If the United States Secret Service invokes an exemption under paragraph (1), the United States Secret Service shall submit written justification for invoking the

exemption to the Secretary of Homeland Security before the exemption is invoked.

(3) FEDERAL BUREAU OF INVESTIGATION.—If the Federal Bureau of Investigation invokes an exemption under paragraph (1), the Federal Bureau of Investigation shall submit written justification for invoking the exemption to the Attorney General before the exemption is invoked.

(4) IMMUNITY.—No cause of action shall lie in any court against any Federal agency for acts relating to the exemption from notification for national security or law enforcement purposes under this Act.

(5) REPORTS.—Not later than 18 months after the date of enactment of this Act, and upon request by Congress thereafter, the United States Secret Service and Federal Bureau of Investigation shall submit to Congress a report on the number and nature of breaches of security subject to the exemptions for national security and law enforcement purposes under this subsection.

(i) FINANCIAL FRAUD PREVENTION EXEMPTION.—

(1) IN GENERAL.—A covered entity shall be exempt from the requirements under this section if the covered entity utilizes or participates in a security program that—

(A) effectively blocks the use of the personal information to initiate an unauthorized financial transaction before it is charged to the account of the individual; and

(B) provides notice to each affected individual after a breach of security that resulted in attempted fraud or an attempted unauthorized transaction.

(2) LIMITATIONS.—An exemption under paragraph (1) shall not apply if—

(A) the breach of security includes personal information, other than a credit card number or credit card security code, of any type; or

(B) the breach of security includes both the individual's credit card number and the individual's first and last name.

(j) FINANCIAL INSTITUTIONS REGULATED BY FEDERAL FUNCTIONAL REGULATORS.—

(1) IN GENERAL.—A covered financial institution shall be deemed in compliance with this section if—

(A) the Federal functional regulator with jurisdiction over the covered financial institution has issued a standard by regulation or

guideline under title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) that—

(i) requires financial institutions within its jurisdiction to provide notification to individuals following a breach of security; and

(ii) provides protections substantially similar to, or greater than, those required under this Act; and

(B) the covered financial institution is in compliance with the standard under subparagraph (A).

(2) DEFINITIONS.—In this subsection—

(A) the term ''covered financial institution'' means a financial institution that is subject to—

(i) the data security requirements of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.);

(ii) any implementing standard issued by regulation or guideline issued under that Act; and

(iii) the jurisdiction of a Federal functional regulator under that Act;

(B) the term ''Federal functional regulator'' has the meaning given the term in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809); and

(C) the term ''financial institution'' has the meaning given the term in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809).

(k) EXEMPTION; HEALTH PRIVACY.—

(1) COVERED ENTITY OR BUSINESS ASSOCIATE UNDER HITECH ACT.—To the extent that a covered entity under this Act acts as a covered entity or a business associate under section 13402 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17932), has the obligation to provide notification to individuals following a breach of security under that Act or its implementing regulations, and is in compliance with that obligation, the covered entity shall be deemed in compliance with this section.

(2) ENTITY SUBJECT TO HITECH ACT.—To the extent that a covered entity under this Act acts as a vendor of personal health records, a third party service provider, or other entity subject to section 13407 of the Health Information Technology for Economical and Clinical Health Act (42 U.S.C.

17937), has the obligation to provide notification to individuals following a breach of security under that Act or its implementing regulations, and is in compliance with that obligation, the covered entity shall be deemed in compliance with this section.

(3) LIMITATION OF STATUTORY CONSTRUCTION.—Nothing in this Act may be construed in any way to give effect to the sunset provision under section 13407(g)(2) of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17937(g)(2)) or to otherwise limit or affect the applicability, under section 13407 of that Act, of the requirement to provide notification to individuals following a breach of security for vendors of personal health records and each entity described in clause (ii), (iii), or (iv) of section 13424(b)(1)(A) of that Act (42 U.S.C. 17953(b)(1)(A)).

(l) WEB SITE NOTICE OF FEDERAL TRADE COMMISSION.—If the Commission, upon receiving notification of any breach of security that is reported to the Commission, finds that notification of the breach of security via the Commission's Internet Web site 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 Web site.

(m) 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 direct 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.

(n) 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.

SEC. 4. NOTICE TO LAW ENFORCEMENT.

(a) DESIGNATION OF GOVERNMENT ENTITY TO RECEIVE NOTICE.—Not later than 60 days after the date of enactment of this Act, the Secretary of the Department of Homeland Security shall designate a Federal Government entity to receive notice under this section.

(b) NOTICE.—A covered entity shall notify the designated entity of a breach of security if—

(1) the number of individuals whose personal information was, or is reasonably believed to have been, acquired or assessed as a result of the breach of security exceeds 10,000;

(2) the breach of security involves a database, networked or integrated databases, or other data

system containing the personal information of more than 1,000,000 individuals;

(3) the breach of security involves databases owned by the Federal Government; or

(4) the breach of security involves primarily personal information of individuals known to the covered entity to be employees or contractors of the Federal Government involved in national security or law enforcement.

(c) CONTENT OF NOTICES.—

(1) IN GENERAL.—Each notice under subsection (b) shall contain—

(A) the date, estimated date, or estimated date range of the breach of security;

(B) a description of the nature of the breach of security;

(C) a description of each type of personal information that was or is reasonably believed to have been acquired or accessed as a result of the breach of security; and

(D) a statement of each paragraph under subsection (b) that applies to the breach of security.

(2) CONSTRUCTION.—Nothing in this section shall be construed to require a covered entity to re-

veal specific or identifying information about an individual as part of the notice under paragraph (1).

(d) RESPONSIBILITIES OF THE DESIGNATED ENTITY.—The designated entity shall promptly provide each notice it receives under subsection (b) to—

(1) the United States Secret Service;

(2) the Federal Bureau of Investigation;

(3) the Federal Trade Commission;

(4) the United States Postal Inspection Service, if the breach of security involves mail fraud;

(5) the attorney general of each State affected by the breach of security; and

(6) as appropriate, other Federal agencies for law enforcement, national security, or data security purposes.

(e) TIMING OF NOTICES.—Notice under this section shall be delivered as follows:

(1) Notice under subsection (b) shall be delivered as promptly as possible, but—

(A) not less than 3 business days before notification to an individual under section 3; and

(B) not later than 10 days after the date of discovery of the events requiring notice.

(2) Notice under subsection (d) shall be delivered as promptly as possible, but not later than 1 business day after the date that the designated entity receives notice of a breach of security from a covered entity.

SEC. 5. APPLICATION AND ENFORCEMENT.

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

(1) those persons, partnerships, or corporations over which the Commission has authority under section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)); and

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

(b) OPT-IN FOR CERTAIN OTHER ENTITIES.—

(1) IN GENERAL.—Notwithstanding sections 4 and 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 44 and 45(a)(2)), the requirements of section 3 shall apply to any other covered entity not included under subsection (a) that enters into an

agreement with the Commission under which that covered entity would be subject to section 3 with respect to any acts or omissions that occur while the agreement is in effect and that may constitute a violation of section 3, if—

(A) not less than 30 days prior to entering into the agreement with the covered entity, the Commission publishes notice in the Federal Register of the Commission's intent to enter into the agreement; and

(B) not later than 14 business days after entering into the agreement with the covered entity, the Commission publishes in the Federal Register—

(i) notice of the agreement;

(ii) the identity of each person covered by the agreement; and

(iii) the effective date of the agreement.

(2) CONSTRUCTION.—

(A) OTHER FEDERAL LAW.—An agreement under paragraph (1) shall not effect a covered entity's obligation to provide notice of a breach of security or similar event under any other Federal law.

(B) NO PREEMPTION PRIOR TO VALID AGREEMENT.—Subsections (a)(2) and (b) of section 7 shall not apply to a breach of security that occurs before a valid agreement under paragraph (1) is in effect.

(c) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 2 or 3 of this Act 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) VIOLATION OF TITLE V OF THE GRAMM-LEACH-BLILEY ACT.—A violation of a regulation prescribed by the Commission under title V of the Gramm-Leach-Bliley Act for the financial institutions subject to the Commission's jurisdiction (15 U.S.C. 6801 et seq.) 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.

(3) POWERS OF COMMISSION.—The Commission shall enforce this Act in the same manner, by the same means, with the same jurisdiction, except as provided in subsections (a)(2) and (b) of this section, and with the same 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.

(4) 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.

(d) 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 section 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 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)(C) with regard to a violation of section 3, the amount determined under this paragraph is the amount calculated by multi-

plying 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 commencing 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 com-

plaint 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—

(A) to conduct investigations;

(B) to administer oaths or affirmations; or

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

(e) NOTICE TO LAW ENFORCEMENT; CIVIL ENFORCEMENT BY ATTORNEY GENERAL.—

(1) IN GENERAL.—The Attorney General may bring a civil action in the appropriate United States district court against any covered entity that engages in conduct constituting a violation of section 4.

(2) PENALTIES.—

(A) IN GENERAL.—Upon proof of such conduct by a preponderance of the evidence, a covered entity shall be subject to a civil penalty of not more than $1,000 per individual whose personal information was or is reasonably be-

lieved to have been accessed or acquired as a result of the breach of security that is the basis of the violation, up to a maximum of $100,000 per day while such violation persists.

(B) LIMITATIONS.—The total amount of the civil penalty assessed under this subsection against a covered entity for acts or omissions relating to a single breach of security shall not exceed $1,000,000, unless the conduct constituting a violation of section 4 was willful or intentional, in which case an additional civil penalty of up to $1,000,000 may be imposed.

(C) 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 subparagraphs (A) and (B) 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) INJUNCTIVE ACTIONS.—If it appears that a covered entity has engaged, or is engaged, in any act or practice that constitutes a violation of section 4,

the Attorney General may petition an appropriate United States district court for an order enjoining such practice or enforcing compliance with section 4.

(4) ISSUANCE OF ORDER.—A court may issue such an order under paragraph (3) if it finds that the conduct in question constitutes a violation of section 4.

(f) CONCEALMENT OF BREACHES OF SECURITY.—

(1) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following:

"§ 1041. Concealment of breaches of security involving personal information

''(a) IN GENERAL.—Any person who, having knowledge of a breach of security and of the fact that notification of the breach of security is required under the Data Security and Breach Notification Act, intentionally and willfully conceals the fact of the breach of security, shall, in the event that the breach of security results in economic harm to any individual in the amount of $1,000 or more, be fined under this title, imprisoned for not more than 5 years, or both.

''(b) PERSON DEFINED.—For purposes of subsection (a), the term 'person' has the same meaning as in section 1030(e)(12) of this title.

''(c) ENFORCEMENT AUTHORITY.—

''(1) IN GENERAL.—The United States Secret Service and the Federal Bureau of Investigation shall have the authority to investigate offenses under this section.

''(2) CONSTRUCTION.—The authority granted in paragraph (1) shall not be exclusive of any existing authority held by any other Federal agency.''.

(2) CONFORMING AND TECHNICAL AMENDMENTS.—The table of sections for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''1041. Concealment of breaches of security involving personal information.''.

SEC. 6. DEFINITIONS.

In this Act:

(1) BREACH OF SECURITY.—

(A) IN GENERAL.—The term ''breach of security'' means compromise of the security, confidentiality, or integrity of, or loss of, data in electronic form that results in, or there is a reasonable basis to conclude has resulted in, unauthorized access to or acquisition of personal information from a covered entity.

(B) EXCLUSIONS.—The term ''breach of security'' does not include—

(i) a good faith acquisition of personal information by a covered entity, or an employee or agent of a covered entity, if the personal information is not subject to further use or unauthorized disclosure;

(ii) any lawfully authorized investigative, protective, or intelligence activity of a law enforcement or an intelligence agency of the United States, a State, or a political subdivision of a State; or

(iii) the release of a public record not otherwise subject to confidentiality or nondisclosure requirements.

(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, including recordable tapes and other mass storage devices.

(5) DESIGNATED ENTITY.—The term ''designated entity'' means the Federal Government entity designated by the Secretary of Homeland Security under section 4.

(6) 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.

(7) 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 identity of such other person, including any contact that violates section 1028A of title 18, United States Code.

(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 (15 U.S.C. 1681a(p)).

(9) PERSONAL INFORMATION.—

(A) DEFINITION.—The term ''personal information'' means any information or compilation of information that includes—

(i) a non-truncated social security number;

(ii) a financial account number or credit or debit card number in combination with any security code, access code, or password that is required for an individual to obtain credit, withdraw funds, or engage in a financial transaction; or

(iii) an individual's first and last name or first initial and last name in combination with—

(I) a driver's license number, a passport number, or an alien registration number, or other similar number issued on a government document used to verify identity;

(II) unique biometric data such as a finger print, voice print, retina or

iris image, or any other unique physical representation;

(III) a unique account identifier, electronic identification number, user name, or routing code in combination with any associated security code, access code, or password that is required for an individual to obtain money, goods, services, or any other thing of value; or

(IV) 2 of the following:

(aa) Home address or telephone number.

(bb) Mother's maiden name, if identified as such.

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

(B) MODIFIED DEFINITION BY RULEMAKING.—If the Commission determines that the definition under subparagraph (A) is not reasonably sufficient to protect individuals from identity theft, fraud, or other unlawful conduct, the Commission by rule promulgated under section 553 of title 5, United States Code, may modify the definition of ''personal information''

under subparagraph (A) to the extent the modification will not unreasonably impede interstate commerce.

SEC. 7. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE INFORMATION SECURITY LAWS.—

(1) COVERED ENTITIES UNDER SECTION 5(a).—With respect to a covered entity subject to the Act under section 5(a), this Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State that expressly—

(A) requires information security practices and treatment of data containing personal information, as defined in section 6, similar to any of those required under section 2; or

(B) requires notification to individuals of a breach of security of personal information as defined in section 6.

(2) COVERED ENTITIES UNDER SECTION 5(b).—With respect to a covered entity subject to the Act under section 5(b), this Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State that expressly requires notification to individuals of a breach of security of personal information as defined in section 6.

(b) ADDITIONAL PREEMPTION.—

(1) IN GENERAL.—No person other than a person specified in section 5(d) 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) any 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. 8. EFFECTIVE DATE.

This Act and the amendments made by this Act shall take effect 1 year after the date of enactment of this Act.