109TH CONGRESS
1ST SESSION

S. 768

To provide for comprehensive identity theft prevention.

IN THE SENATE OF THE UNITED STATES

APRIL 12, 2005

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

A BILL

To provide for comprehensive identity theft prevention.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Comprehensive Identity Theft Prevention Act''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

SEC. 2. DEFINITIONS.

In this Act:

(1) COVERED PERSON.—Except as otherwise provided, the term ''covered person'' means a commercial entity.

(2) SENSITIVE PERSONAL INFORMATION.—The term ''sensitive personal information'' means the following information with regard to an individual:

(A) The social security number of such individual.

(B) The medical condition and legal drugs, therapies, or medical products or equipment used by such individual.

(C) The bank or investment account number of such individual.

(D) The credit card or debit card number of such individual.

(E) The payment history of such individual.

(F) The State driver's license identification number or State resident identification number of such individual.

(G) Any other information regarding an individual determined appropriate by the Federal Trade Commission.

SEC. 3. ESTABLISHMENT OF OFFICE OF IDENTITY THEFT.

(a) ESTABLISHMENT.—There is established in the Federal Trade Commission an Office of Identity Theft.

(b) JURISDICTION.—The Office of Identity Theft shall have civil jurisdiction of any covered person that collects, maintains, sells, or transfers sensitive personal information, or attempts to collect, maintain, sell, or transfer sensitive personal information.

(c) REGULATIONS.—Consistent with this Act, the Federal Trade Commission shall promulgate regulations to enable the Office of Identity Theft to protect consumers' sensitive personal information collected, maintained, sold, or transferred, or attempted to be collected, maintained, sold, or transferred by covered persons.

(d) CIVIL ENFORCEMENT.—The Office of Identity Theft may take civil enforcement actions against covered persons that violate the requirements of this Act and the Office of Identity Theft's rules promulgated to carry out this Act.

(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for the Office of Identity Theft $60,000,000 for fiscal year 2006 and each of the 4 succeeding fiscal years.

SEC. 4. HELPING CONSUMERS RECAPTURE THEIR STOLEN IDENTITIES.

The Office of Identity Theft shall carry out the following activities:

(1) Establish a website, easily and conspicuously accessible from ftc.gov, dedicated to assisting consumers with the retrieval of the consumer's stolen or compromised sensitive personal information.

(2) Maintain a toll-free phone number to help answer questions concerning identity theft from consumers.

(3) Establish online and offline consumer-service teams to assist consumers seeking the retrieval of the consumer's sensitive personal information.

(4) Establish a reasonable standard for determining when an individual becomes a victim of identity theft.

(5) Issue certifications to individuals who, under the standard described in paragraph (4), are identity theft victims.

(6) Permit an individual to use the Office of Identity Theft certification in all Federal, State, and local jurisdictions, in lieu of a police report or any other document required by State or local law, as a prerequisite to accessing business records of transactions done by someone claiming to be the individual.

(7) In addition to the requirements in paragraphs (1) through (6), the Federal Trade Commission shall promulgate regulations that enable the Office of Identity Theft to help consumers restore their stolen or otherwise compromised sensitive personal information quickly and inexpensively.

SEC. 5. REASONABLE STEPS TO PROTECT SENSITIVE PERSONAL INFORMATION.

(a) REGULATIONS.—Not later than 9 months after the date of enactment of this Act, the Federal Trade Commission shall promulgate regulations governing the sale, maintenance, collection, or transfer of sensitive personal information by covered persons, including a requirement that covered persons take reasonable steps to prevent unauthorized access to sensitive personal information the covered person sells, maintains, collects, or transfers.

(b) PENALTIES.—A covered person that violates subsection (a) shall be subject to a civil penalty of not more than $500 per person per violation.

(c) ACTIONS.—An action to enforce a violation of subsection (a) may be brought by the Federal Trade Commission in any appropriate United States district court or any other court of competent jurisdiction.

SEC. 6. LIMITATIONS ON SALE OR TRANSFER OF SENSITIVE PERSONAL INFORMATION.

(a) DATA MERCHANT.—

(1) IN GENERAL.—In this section, except as provided in paragraph (2), the term ''data merchant'' means any covered person that engages in collecting, assembling, or selling sensitive personal information in a significant manner or that is a significant part of the operations of such person, whether such collection, assembly, or sale of personally identifiable information is performed by the covered person directly, or by contract or subcontract with another entity .

(2) EXCLUSIONS.—The term ''data merchant'' shall not include either of the following:

(A) An organization described in section 501(c) or 527 of the Internal Revenue Code of 1986.

(B) An entity that only collects, assembles, or sells information that is completely de-identified.

(3) CREDIT BUREAUS.—

(A) IN GENERAL.—

(i) REGULATION OF CREDIT HEADER INFORMATION FURNISHED OUTSIDE A FULL CONSUMER REPORT.—A credit bureau that furnishes information regarding the social security numbers and any other nonpublic personal information of a consumer, or any derivative thereof, to any person other than in a full consumer report furnished in accordance with section 604 of the Fair Credit Reporting Act (15 U.S.C. 1681b), shall be a data merchant for purposes of this section and shall register with the Office of Identity Theft pursuant to subsection (b), and such transaction of furnishing such information outside of a full consumer report shall be subject to the provisions of this section and regulations promulgated to carry out this section.

(ii) FCRA AND FACTA TO APPLY TO FULL CONSUMER REPORTS.—Except as provided in clause (i), to the extent that an activity or transaction of a credit bureau is covered under the Fair Credit Reporting Act (15 U.S.C. 1601 et seq.) or the Fair and Accurate Credit Transactions Act of 2003 (Public Law 108–159), including furnishing information regarding the social security numbers and any other nonpublic personal information of a consumer, or any derivative thereof, to a person in a full consumer report, such activity or transaction shall be governed by such Acts and not under this section.

(B) NONPUBLIC PERSONAL INFORMATION.—In this paragraph, the term ''nonpublic personal information'' has the meaning given such term in section 509(4) of the Gramm-Leach-Bliley Act.

(b) REGISTRATION.—

(1) IN GENERAL.—Each data merchant shall register with the Office of Identity Theft.

(2) FAILURE TO REGISTER.—A data merchant that does not register with the Office of Identity

Theft within 9 months of the date of enactment of this Act shall be subject to a fine of not more than $75 for each consumer's record the data merchant keeps for each day the data merchant failed to timely register with the Office of Identity Theft as a data merchant.

(c) RESTRICTIONS.—

(1) IN GENERAL.—Not later than 9 months after the date of enactment of this Act, the Federal Trade Commission shall promulgate rules governing the sale or transfer of sensitive personal information by data merchants registered pursuant to this section.

(2) RULES.—The rules described in paragraph (1) shall include the following:

(A) AUTHENTICATION PROCESS.—A requirement that each data merchant to have a secure and dependable authentication process for each third party whom the data merchant permits to have access to consumer's sensitive personal information kept in the data merchant's custody.

(B) PASSWORDS.—A requirement that each data merchant adopt a password for each individual employee of a third party customer of

consumer's sensitive personal information, including a requirement that each data merchant only allow an individual employee of a third party customer who has passed a reasonably effective background check to have access to such password.

(C) TRACKING.—A requirement that each data merchant have the ability to track who accessed what records containing sensitive personal information and for what purpose the records were accessed.

(D) SAFEGUARDS.—A requirement that each data merchant have safeguards in place to prevent access to sensitive personal information by unauthorized parties.

(E) REPORT.—Standards for the creation of a simple procedure that would permit a consumer to request and receive a report from any data merchant holding the consumer's sensitive personal information. Such procedure shall be a nearly identical procedure to the procedure outlined for requests for consumer reports provided under sections 612 and 609(c) of the Fair Credit Reporting Act (15 U.S.C. 1681j and 1681g(c)) and section 211 of the Fair and Ac-

curate Credit Transactions Act of 2003 (Public Law 108–159), and shall include the following:

(i) CONTENT OF REPORT.—The report shall provide the consumer with a status of what sensitive personal information the data merchant has with regard to the requesting consumer, what the data merchant has done, if anything, with the consumer's sensitive personal information in the data merchant's custody, the names of the third parties who have gained access, or who have sought to gain access, to the consumer's sensitive personal information, and the purposes for which the third party gained access, or sought to gain access, to the consumer's sensitive personal information.

(ii) FREE REPORT.—Each year, the consumer shall be permitted 1 free report, but shall be permitted to request additional reports within a calendar year for a reasonable fee to be set by the Office of Identity Theft.

(iii) PROCESS.—The process for requesting a report from the Office of Iden-

tity Theft shall closely follow the process for requesting consumer reports under section 211 of the Fair and Accurate Credit Transactions Act of 2003 (Public Law 108–159) and the amendments made by such section.

(iv) CORRECTION.—The procedure shall permit consumers to demand and receive prompt correction of errors found in the data merchant's records.

(F) ACCURACY.—A requirement for data merchants for dealing with the data that guarantees the same standard of accuracy as expected under the Fair Credit Reporting Act (15 U.S.C. 1601 et seq.) for entities within the jurisdiction of such Act.

(d) PENALTY.—A data merchant that violates a requirement of this section or regulations promulgated by the Federal Trade Commission pursuant to this section shall be subject to a civil penalty of not more than $1,000 per individual record per violation.

(e) ACTIONS.—An action to enforce a violation of this section or regulations promulgated by the Federal Trade Commission pursuant to this section may be brought by the Federal Trade Commission or the appropriate State

attorney general in any appropriate United States district court or any other court of competent jurisdiction.

(f) EXEMPTION.—The Federal Trade Commission, in promulgating regulations under this section, may exempt any data merchant from such regulations, in whole or in part, if the Commission determines that granting such an exemption is in the public interest, and if the data merchant's collecting, assembling, or selling of sensitive personal information is only incidental to the data merchant's primary business.

SEC. 7. COORDINATING INTERNATIONAL ACTION AGAINST IDENTITY THEFT.

There is established within the Office of Identity Theft an international directorate that shall be devoted to coordinating international responses to identity theft and the international development of best practices to protect consumers worldwide from identity theft.

SEC. 8. NOTIFICATION OF INFORMATION BREACHES.

(a) IN GENERAL.—If a covered person has sensitive personal information regarding an individual and such individual's unencrypted sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person in combination with the individual's first name or first initial and last name or any combination of identifying information that would allow the unau-

thorized person to reasonably be able to identify the individual, the covered person shall—

(1) give notice to the individual whose unencrypted sensitive personal information was, or is reasonable believed to have been, acquired by an unauthorized person; and

(2) notify the Office of Identity Theft, if the covered person holds sensitive personal information for more than 1,000 individuals.

(b) METHODS OF NOTICE.—

(1) IN GENERAL.—A covered person that is required to provide notification pursuant to subsection (a) shall notify the individual either in writing or by electronic mail.

(2) TIMING.—Except as provided in paragraph (3), notifications required under this section shall be made in the most expedient time possible and without unreasonable delay consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(3) DELAY.—A notification may be delayed if either of the following occur:

(A) If Federal, State, or local law enforcement determines that notification would impede a criminal investigation, notification may be de-

layed as long as the law enforcement agency determines reasonably necessary.

(B) The Office of Identity Theft certifies that the covered person showed cause of exigent circumstance meriting further delay.

(c) PENALTIES AND ACTIONS FOR VIOLATIONS.—

(1) PENALTY.—Any covered person that violates the notice requirements under this section shall be subject to a civil penalty of not more than $1,000 per violation per individual record accessed.

(2) ACTIONS.—An action to enforce a violation of this section may be brought by the Federal Trade Commission or the appropriate State attorney general in any appropriate United States district court or any other court of competent jurisdiction.

(d) CONSUMER REDRESS.—

(1) IN GENERAL.—After receiving a notification under this section, an individual may request in writing that the covered person expunge the individual's sensitive personal information from the covered person's records.

(2) COVERED PERSON.—In this subsection, the term ''covered person'' does not include credit bureaus.

SEC. 9. SOCIAL SECURITY NUMBER PROTECTION.

(a) PROHIBITION OF UNNECESSARY SOLICITATION OF SOCIAL SECURITY NUMBERS.—

(1) IN GENERAL.—No person may solicit any social security number unless—

(A) such number is necessary for the normal course of business; and

(B) there is a specific use of the social security number for which no other identifying number can be used.

(2) ENFORCEMENT.—

(A) IN GENERAL.—An action to enforce a violation of paragraph (1) may be brought by the Federal Trade Commission or the appropriate State attorney general in any appropriate United States district court or any other court of competent jurisdiction.

(B) CIVIL PENALTY.—A civil money penalty of not more than $1,000 may be imposed for each violation of this subsection.

(b) PROHIBITION OF THE DISPLAY OF PERSONAL IDENTIFICATION NUMBERS ON EMPLOYEE IDENTIFICATION CARDS OR TAGS.—

(1) IN GENERAL.—Section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)) is

amended by adding at the end the following new clause:

''(x) No employer (including any executive, legislative, or judicial agency or instrumentality of the Federal Government or of a State or political subdivision thereof), and no person offering benefits in connection with an employee benefit plan maintained by such employer or acting as an agent of such employer, may display the social security account number (or any derivative of such number) on any card or tag that is commonly provided to employees of such employer (or to their family members) for purposes of identification.''.

(2) EFFECTIVE DATE.—The amendment made by this subsection shall apply with respect to cards or tags issued on or after the date that is 1 year after the date of enactment of this Act.

(c) PROHIBITION OF INMATE ACCESS TO SOCIAL SECURITY ACCOUNT NUMBERS.—

(1) IN GENERAL.—Section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)), as amended by subsection (b), is amended by adding at the end the following new clause:

''(xi) No executive, legislative, or judicial agency or instrumentality of the Federal Government or of a State or political subdivision thereof (or person acting as an

agent of such an agency or instrumentality) may employ, or enter into a contract for the use or employment of, prisoners in any capacity that would allow such prisoners access to the social security account numbers of other individuals. For purposes of this clause, the term 'prisoner' means an individual confined in a jail, prison, or other penal institution or correctional facility.''.

(2) EFFECTIVE DATE.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the amendment made by this subsection shall apply with respect to employment of prisoners, or entry into contract for the use or employment of prisoners, on or after the date of enactment of this Act.

(B) TREATMENT OF CURRENT ARRANGEMENTS.—In the case of—

(i) prisoners employed as described in clause (xi) of section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)), as added by paragraph (1), on the date of enactment of this Act, and

(ii) contracts described in such clause in effect on such date,

the amendment made by this section shall take effect 90 days after the date of enactment of this Act.

(d) PROHIBITION OF THE SALE, PURCHASE, OR DISPLAY TO THE GENERAL PUBLIC OF THE SOCIAL SECURITY ACCOUNT NUMBER IN THE PRIVATE SECTOR.—

(1) IN GENERAL.—Title II of the Social Security Act (42 U.S.C. 401 et seq.) is amended by inserting after section 208 the following new section:

''PROHIBITION OF THE SALE, PURCHASE, OR DISPLAY TO THE GENERAL PUBLIC OF THE SOCIAL SECURITY ACCOUNT NUMBER IN THE PRIVATE SECTOR

''SEC. 208A. (a) In this section:

''(1) PERSON.—

''(A) IN GENERAL.—Subject to subparagraph (B), the term 'person' means any individual, partnership, corporation, trust, estate, cooperative, association, or any other entity.

''(B) GOVERNMENTAL ENTITIES.—Such term does not include a governmental entity. Nothing in this subparagraph shall be construed to authorize, in connection with a governmental entity, an act or practice otherwise prohibited under this section or section 205(c)(2)(C).

''(2) SELLING AND PURCHASING.—

''(A) IN GENERAL.—Subject to subparagraph (B)—

''(i) SELL.—The term 'sell', in connection with a social security account number, means to obtain, directly or indirectly, anything of value in exchange for such number.

''(ii) PURCHASE.—The term 'purchase', in connection with a social security account number, means to provide, directly or indirectly, anything of value in exchange for such number.

''(B) EXCEPTIONS.—The terms 'sell' and 'purchase', in connection with a social security account number, do not include the submission of such number as part of—

''(i) the process for applying for any type of Government benefits or programs (such as grants or loans or welfare or other public assistance programs); or

''(ii) the administration of, or provision of benefits under, an employee benefit plan.

''(3) DISPLAY TO THE GENERAL PUBLIC.—The term 'display to the general public' means, in con-

nection with a social security account number, to intentionally place such number in a viewable manner on an Internet site that is available to the general public or to make such number available in any other manner intended to provide access to such number by the general public.

''(4) SOCIAL SECURITY ACCOUNT NUMBER.—The term 'social security account number' means a social security account number assigned by the Commissioner under section 205(c)(2)(B).

''(b) PROHIBITION.—Except as provided in subsection (c), it shall be unlawful for any person to—

''(1) sell or purchase a social security account number or display to the general public a social security account number or any derivative thereof; or

''(2) obtain or use any individual's social security account number for the purpose of locating or identifying such individual with the intent to physically injure or harm such individual or using the identity of such individual for any illegal purpose.

''(c) EXCEPTIONS.—

''(1) IN GENERAL.—Notwithstanding subsection (b), a social security account number may be sold, purchased, or displayed to the general public by any

person to the extent provided in this subsection (and for no other purpose) as follows:

"(A) To the extent necessary for law enforcement, including the enforcement of a child support obligation, as determined under regulations of the Attorney General issued under section 205(c)(2)(I).

"(B) To the extent necessary for national security purposes, as determined under regulations of the Attorney General issued under section 205(c)(2)(I).

"(C) To the extent necessary for public health purposes.

"(D) To the extent necessary in emergency situations to protect the health or safety of 1 or more individuals.

"(E) To the extent necessary for research conducted for the purpose of advancing public knowledge, on the condition that the researcher provides adequate assurances that—

"(i) the social security account numbers will not be used to harass, target, or publicly reveal information concerning any identifiable individuals;

''(ii) information about identifiable individuals obtained from the research will not be used to make decisions that directly affect the rights, benefits, or privileges of specific individuals; and

''(iii) the researcher has in place appropriate safeguards to protect the privacy and confidentiality of any information about identifiable individuals.

''(F) To the extent consistent with an individual's voluntary and affirmative written consent to the sale, purchase, or display to the general public of a social security account number that has been assigned to that individual.

''(G) Under such other circumstances as the Attorney General may determine appropriate in regulations issued under section 205(c)(2)(I).

''(H) To the extent necessary for use by an established fraud prevention unit that shall use such number only for fraud prevention purposes and each individual member of such unit shall have passed a reasonably effective background check.

''(2) DECEASED INDIVIDUALS.—This section does not apply with respect to the social security account number of a deceased individual.

''(d) PENALTIES AND ACTIONS FOR VIOLATIONS.—

''(1) PENALTY.—Any person that violates this section shall be subject to a civil penalty of not more than $1,000 per individual social security number per violation.

''(2) ACTIONS.—An action to enforce a violation of this section may be brought by the Federal Trade Commission or the appropriate State attorney general in any appropriate United States district court or any other court of competent jurisdiction.''.

(2) EFFECTIVE DATE.—The amendment made by this subsection shall apply with respect to violations occurring on or after the date that is 1 year after the date of the issuance by the Attorney General of the United States of final regulations under section 205(c)(2)(I) of the Social Security Act (as added by subsection (e)(1)).

(e) REGULATORY AUTHORITY OF THE ATTORNEY GENERAL.—

(1) IN GENERAL.—Section 205(c)(2) of the Social Security Act (42 U.S.C. 405(c)(2)) is amended

by adding at the end the following new subparagraph:

''(I)(i) Regulations issued by the Attorney General pursuant to subparagraphs (A) and (B) of section 208A(c)(1) shall be issued in accordance with section 553 of title 5, United States Code. In issuing such regulations, the Attorney General shall consult with the Commissioner of Social Security, the Secretary of Homeland Security, the Federal Trade Commission, State attorneys general, and such other governmental agencies and instrumentalities as the Attorney General considers appropriate.

''(ii) In issuing the regulations described in clause (i) pursuant to the provisions of subparagraphs (A) and (B) of section 208A(c)(1) (relating to law enforcement and national security), the Attorney General may authorize the sale, purchase, or display to the general public of social security account numbers only if the Attorney General determines that—

''(I) such sale, purchase, or display would serve a compelling public interest that cannot reasonably be served through alternative measures, and

''(II) such sale, purchase, or display will not pose an undue risk of bodily, emotional, or financial harm to an individual (taking into account any restrictions and conditions that the Attorney General

imposes on the sale, purchase, or disclosure to the general public of social security account numbers).

''(iii) If the Attorney General authorizes the sale, purchase, or display to the general public of social security account numbers, in regulations issued pursuant to subparagraph (C), (D), (E), (F), (G), or (H) of section 208A(c)(1), the Attorney General shall impose restrictions and conditions on the sale, purchase, or display to the general public to the extent necessary—

''(I) to provide reasonable assurances that social security account numbers will not be used to commit or facilitate fraud, deception, or crime, and

''(II) to prevent an undue risk of bodily, emotional, or financial harm to an individual.

''(iv) For purposes of clause (iii), the Attorney General shall consider, among other relevant factors—

''(I) the cost or burden to the general public, businesses, commercial enterprises, nonprofit organizations, and to Federal, State, and local governments of complying with the restrictions and conditions imposed by the Attorney General;

''(II) the benefit to the general public, businesses, commercial enterprises, nonprofit associations, and to Federal, State, and local governments

derived from the imposition of such restrictions and conditions; and

''(III) in connection with subclause (II) of clause (iii), the nature, likelihood, and severity of the anticipated harm described in such subclause that could result from the sale, purchase, or display to the general public of social security account numbers, together with the nature, likelihood, and extent of any benefits that could be realized therefrom.

''(v) For purposes of this subparagraph, the terms 'sell', 'purchase', and 'display to the general public' shall have the meanings provided such terms under section 208A(a).

''(vi) For purposes of this subparagraph, the term 'social security account number' includes any derivative of such number.''.

(2) REGULATIONS.—The Attorney General shall promulgate regulations required under this subsection not later than 1 year after the date of enactment of this Act.

SEC. 10. INFORMATION SHARING REQUIREMENTS.

(a) DISCLOSURE BOX.—A covered person that requests on an online or offline form sensitive personal information from a customer and intends to sell or transfer such sensitive personal information for anything of value

to an unaffiliated third party at any point, shall provide a notification to the customer in accordance with subsection (b).

(b) NOTIFICATION.—

(1) IN GENERAL.—The notification required under subsection (a) shall include in a clear and conspicuous box on the form the following: ''This information be may sold or transferred to an unaffiliated third party without your additional consent.'' (referred to in this subsection as a ''Disclosure Box'').

(2) TYPEFACE AND LOCATION.—The text in the Disclosure Box shall appear in not less than 12-point typeface directly above either the final signature block on a written document or the final online submission button on an online form on which the customer would agree to submit sensitive personal information to the covered person.

SEC. 11. IMPROVING CYBERSECURITY.

(a) SHORT TITLE.—This section may be cited as the ''Department of Homeland Security Cybersecurity Enhancement Act of 2005''.

(b) ASSISTANT SECRETARY FOR CYBERSECURITY.—

(1) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended by adding at the end the following:

"SEC. 203. ASSISTANCE SECRETARY FOR CYBERSECURITY.

''(a) NATIONAL CYBERSECURITY OFFICE.—There shall be in the Directorate for Information Analysis and Infrastructure Protection a National Cybersecurity Office headed by an Assistant Secretary for Cybersecurity (in this section referred to as the 'Assistant Secretary'), who shall assist the Secretary in promoting cybersecurity for the United States.

''(b) GENERAL AUTHORITY.—The Assistant Secretary, subject to the direction and control of the Secretary, shall have primary authority within the Department for all cybersecurity-related critical infrastructure protection programs of the Department, including with respect to policy formulation and program management.

''(c) RESPONSIBILITIES.—The responsibilities of the Assistant Secretary shall include the following:

''(1) To establish and manage—

''(A) a national cybersecurity response system that includes the ability to—

''(i) analyze the effect of cybersecurity threat information on national critical infrastructure; and

''(ii) aid in the detection and warning of attacks on, and in the restoration of, cybersecurity infrastructure in the aftermath of such attacks;

''(B) a national cybersecurity threat and vulnerability reduction program that identifies cybersecurity vulnerabilities that would have a national effect on critical infrastructure, performs vulnerability assessments on information technologies, and coordinates the mitigation of such vulnerabilities;

''(C) a national cybersecurity awareness and training program that promotes cybersecurity awareness among the public and the private sectors and promotes cybersecurity training and education programs;

''(D) a government cybersecurity program to coordinate and consult with Federal, State, and local governments to enhance their cybersecurity programs; and

''(E) a national security and international cybersecurity cooperation program to help foster Federal efforts to enhance international cybersecurity awareness and cooperation.

''(2) To coordinate with the private sector on the program under paragraph (1) as appropriate, and to promote cybersecurity information sharing, vulnerability assessment, and threat warning regarding critical infrastructure.

''(3) To coordinate with other directorates and offices within the Department on the cybersecurity aspects of their missions.

''(4) To coordinate with the Under Secretary for Emergency Preparedness and Response to ensure that the National Response Plan developed pursuant to section 502(6) includes appropriate measures for the recovery of the cybersecurity elements of critical infrastructure.

''(5) To develop processes for information sharing with the private sector, consistent with section 214, that—

''(A) promote voluntary cybersecurity best practices, standards, and benchmarks that are responsive to rapid technology changes and to the security needs of critical infrastructure; and

''(B) consider roles of Federal, State, local, and foreign governments and the private sector, including the insurance industry and auditors.

''(6) To coordinate with the Chief Information Officer of the Department in establishing a secure information sharing architecture and information sharing processes, including with respect to the Department's operation centers.

''(7) To consult with the Electronic Crimes Task Force of the United States Secret Service on private sector outreach and information activities.

''(8) To consult with the Office for Domestic Preparedness to ensure that realistic cybersecurity scenarios are incorporated into tabletop and recovery exercises.

''(9) To consult and coordinate, as appropriate, with other Federal agencies on cybersecurity-related programs, policies, and operations.

''(10) To consult and coordinate within the Department and, where appropriate, with other relevant Federal agencies, on security of digital control systems, such as Supervisory Control and Data Acquisition (SCADA) systems.

''(d) AUTHORITY OVER THE NATIONAL COMMUNICATIONS SYSTEM.—The Assistant Secretary shall have primary authority within the Department over the National Communications System.''.

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 note) is amended by adding at the end of the items relating to subtitle A of title II the following:

''Sec. 203. Assistance secretary for cybersecurity.''.

(c) CYBERSECURITY DEFINED.—Section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101) is amended by adding at the end the following:

''(17) CYBERSECURITY.—

''(A) IN GENERAL.—The term 'cybersecurity' means the prevention of damage to, the protection of, and the restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

''(B) OTHER TERMS.—In this paragraph—

''(i) each of the terms 'damage' and 'computer' have the meanings given such terms in section 1030 of title 18, United States Code; and

''(ii) each of the terms 'electronic communications system', 'electronic communication service', 'wire communication', and 'electronic communication' have the meanings given such terms in section 2510 of title 18, United States Code.''.

SEC. 12. PROHIBITION OF POSTING ACCOUNT NUMBERS AND INDIVIDUALS' NAMES.

A covered person shall not post in a document that is publically accessible online an individual financial account number of an individual in combination with such individual's name.

SEC. 13. ONLINE INFORMATION SECURITY WORKING GROUP.

(a) ONLINE INFORMATION SECURITY WORKING GROUP.—The Chairman of the Federal Trade Commission shall establish an Online Information Security Working Group (referred to in this section as the ''Working Group'') to develop best practices to protect sensitive personal information stored and transferred online. The Working Group shall be composed of industry participants, consumer groups, and other interested parties.

(b) REPORT.—Not later than 12 months after the date on which the Working Group is established under subsection (a), the Working Group shall submit to Congress a report on their findings.

SEC. 14. STUDY TO EXAMINE THE USE OF SOCIAL SECURITY NUMBERS BY THE GOVERNMENT.

(a) IN GENERAL.—Not later than 9 months after the date of enactment of this Act, the Chairman of the Federal Trade Commission shall submit to Congress a report that contains the results of the study conducted under

subsection (b) concerning the use and publication of social security numbers by Federal, State, and local governments and recommendations for the modification by Federal, State, and local governments of their policies for the use of social security numbers in such a way that would prevent or reduce identity theft.

(b) STUDY.—The Chairman of the Federal Trade Commission shall conduct a study to examine—

(1) where and when Federal, State, and local governments publish social security numbers;

(2) the reasons that social security numbers are published by Federal, State, and local governments;

(3) the individuals and entities that have access to such social security numbers; and

(4) the risk for identity theft as a result of the current policies on the publication of such social security numbers.

(c) RECOMMENDATIONS.—The recommendation contained in the report under subsection (a) shall be provided to all relevant State and local governments.

SEC. 15. ANNUAL IDENTITY THEFT REPORT.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Director of the Office of Identity Theft of the Federal

Trade Commission shall submit to Congress a report on identity theft.

(b) CONTENTS OF REPORT.—The report submitted under subsection (a) shall include—

(1) a description of the current trends in identity theft for residents of the United States;

(2) the total number of identity-theft enforcement actions opened or continued by the Federal Trade Commission in the year for which the report is prepared;

(3) a description of the current status and disposition of the enforcement actions described in paragraph (2);

(4) a description of the procedures utilized by the Office of Identity Theft to assist victims of identity theft in re-establishing their identity;

(5) with respect to the year for which the report is prepared, data concerning—

(A) the number of certifications of identity theft applied for under section 4;

(B) the number of such certifications issued; and

(C) the common trends with respect to such certification approvals and disapprovals; and

(6) a description of the products and services used by identity theft victims to help such victims reestablish their identities.

(c) PROVISION OF REPORT.—The report submitted under subsection (a) shall be provided to—

(1) the Committee on Banking, Housing, and Urban Affairs of the Senate;

(2) the Committee on the Judiciary of the Senate;

(3) the Committee on Commerce, Science, and Transportation of the Senate;

(4) the Committee on Finance of the Senate;

(5) the Committee on Financial Services of the House of Representatives;

(6) the Committee on the Judiciary of the House of Representatives;

(7) the Committee on Energy and Commerce of the House of Representatives; and

(8) the Committee on Ways and Means of the House of Representatives.

(d) INTERNATIONAL REPORT.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the international directorate of the Office of Identity Theft shall submit a report detailing emerging issues in international identity theft, including what action

and initiatives have been taken to fight identity theft on a global level. The report shall also spotlight the most successful steps other countries are taking to fight identity theft and shall rank the top few countries that have the worst record regarding identity theft against victims in the United States.

SEC. 16. PREEMPTION OF STATE LAW.

This Act shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this Act, and then only to the extent of the inconsistency. A State statute, regulation, order, or interpretation is not inconsistent with the provisions of this Act if the protection such statute, regulation, order, or interpretation affords any resident of the United States is greater than the protection provided under this Act.

SEC. 17. NONINTERFERENCE WITH THE FAIR CREDIT REPORTING ACT.

Nothing in this Act shall be construed to affect, alter, or supersede the applicability of the Fair Credit Reporting Act (15 U.S.C. 1601 et seq.) with respect to transactions covered under the Fair Credit Reporting Act.

○