109TH CONGRESS
1ST SESSION

S. _____

To prevent and mitigate identity theft; to ensure privacy; and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

IN THE SENATE OF THE UNITED STATES

Mr. SPECTER (for himself and Mr. LEAHY) introduced the following bill; which was read twice and referred to the Committee on

---

A BILL

To prevent and mitigate identity theft; to ensure privacy; and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

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 ''Personal Data Privacy and Security Act of 2005''.

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

Sec. 1. Short title; table of contents.
Sec. 2. Findings.
Sec. 3. Definitions.

TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY

Sec. 101. Fraud and related criminal activity in connection with unauthorized access to personally identifiable information.
Sec. 102. Organized criminal activity in connection with unauthorized access to personally identifiable information.
Sec. 103. Concealment of security breaches involving personally identifiable information.
Sec. 104. Aggravated fraud in connection with computers.
Sec. 105. Review and amendment of Federal sentencing guidelines related to fraudulent access to or misuse of digitized or electronic personally identifiable information.

TITLE II—ASSISTANCE FOR STATE AND LOCAL LAW ENFORCEMENT COMBATING CRIMES RELATED TO FRAUDULENT, UNAUTHORIZED, OR OTHER CRIMINAL USE OF PERSONALLY IDENTIFIABLE INFORMATION

Sec. 201. Grants for State and local enforcement.
Sec. 202. Authorization of appropriations.

TITLE III—DATA BROKERS

Sec. 301. Transparency and accuracy of data collection.
Sec. 302. Enforcement.
Sec. 303. Relation to State laws.
Sec. 304. Effective date.

TITLE IV—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

Subtitle A—Data Privacy and Security Program

Sec. 401. Purpose and applicability of data privacy and security program.
Sec. 402. Requirements for a personal data privacy and security program.
Sec. 403. Enforcement.
Sec. 404. Relation to State laws.

Subtitle B—Security Breach Notification

Sec. 421. Right to notice of security breach.
Sec. 422. Notice procedures.
Sec. 423. Content of notice.
Sec. 424. Risk assessment and fraud prevention notice exemptions.
Sec. 425. Victim protection assistance.
Sec. 426. Enforcement.
Sec. 427. Relation to State laws.
Sec. 428. Study on securing personally identifiable information in the digital era.
Sec. 429. Authorization of appropriations.
Sec. 430. Effective date.

TITLE V—PROTECTION OF SOCIAL SECURITY NUMBERS

Sec. 501. Social Security number protection.
Sec. 502. Limits on personal disclosure of social security numbers for commercial transactions and accounts.
Sec. 503. Public records.
Sec. 504. Treatment of social security numbers on government checks and prohibition of inmate access.
Sec. 505. Study and report.
Sec. 506. Enforcement.
Sec. 507. Relation to State laws.

TITLE VI—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL DATA

Sec. 601. General Services Administration review of contracts.
Sec. 602. Requirement to audit information security practices of contractors and third party business entities.
Sec. 603. Privacy impact assessment of government use of commercial information services containing personally identifiable information.
Sec. 604. Implementation of Chief Privacy Officer requirements.

SEC. 2. FINDINGS.

Congress finds that—

(1) databases of personal identifiable information are increasingly prime targets of hackers, identity thieves, rogue employees, and other criminals, including organized and sophisticated criminal operations;

(2) identity theft is a serious threat to the nation's economic stability, homeland security, the development of e-commerce, and the privacy rights of Americans;

(3) over 9,300,000 individuals were victims of identity theft in America last year;

(4) security breaches are a serious threat to consumer confidence, homeland security, e-commerce, and economic stability;

(5) it is important for business entities that own, use, or license personally identifiable information to adopt reasonable procedures to ensure the security, privacy, and confidentially of that personally identifiable information;

(6) individuals whose personal information has been compromised or who have been victims of identity theft should receive the necessary information and assistance to mitigate their damages and to restore the integrity of their personal information and identities;

(7) data brokers have assumed a significant role in providing identification, authentication, and screening services, and related data collection and analyses for commercial, nonprofit, and government operations;

(8) data misuse and use of inaccurate data have the potential to cause serious or irreparable harm to an individual's livelihood, privacy, and liberty and undermine efficient and effective business and government operations;

(9) there is a need to insure that data brokers conduct their operations in a manner that prioritizes fairness, transparency, accuracy, and respect for the privacy of consumers;

(10) government access to commercial data can potentially improve safety, law enforcement, and national security; and

(11) because government misuse of commercial data endangers privacy, security, and liberty, there is a need for Congress to exercise oversight over government use of commercial data.

SEC. 3. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ''agency'' has the same meaning given such term in section 551 of title 5, United States Code.

(2) AFFILIATE.—The term ''affiliate'' means persons related by common ownership or affiliated by corporate control.

(3) BUSINESS ENTITY.—The term ''business entity'' means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, venture established to make a profit, or nonprofit, and any contractor, subcontractor, affiliate, or licensee thereof engaged in interstate commerce.

(4) IDENTITY THEFT.—The term ''identity theft'' means a violation of section 1028 of title 18,

United States Code, or any other similar provision of applicable State law.

(5) DATA BROKER.—The term ''data broker'' means a business entity which for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of collecting, transmitting, or otherwise providing personally identifiable information on a nationwide basis on more than 5,000 individuals who are not the customers or employees of the business entity or affiliate.

(6) DATA FURNISHER.—The term ''data furnisher'' means any agency, governmental entity, organization, corporation, trust, partnership, sole proprietorship, unincorporated association, venture established to make a profit, or nonprofit, and any contractor, subcontractor, affiliate, or licensee thereof, that serves as a source of information for a data broker.

(7) PERSONAL ELECTRONIC RECORD.—The term ''personal electronic record'' means the compilation of personally identifiable information of an individual (including information associated with that personally identifiable information) in a data-

base, networked or integrated databases, or other data system.

(8) PERSONALLY IDENTIFIABLE INFORMATION.—The term ''personally identifiable information'' means any information, or compilation of information, in electronic or digital form serving as a means of identification, as defined by section 1028(d)(7) of title 18, United State Code.

(9) PUBLIC RECORD.—The term ''public record'' means any item, collection, or grouping of information about an individual that is maintained by an agency, including—

(A) education, financial transactions, medical history, and criminal or employment history containing the name of an individual; and

(B) the identifying number, symbol, or other identifying particular assigned to an individual, such as—

(i) a fingerprint;

(ii) a voice print; or

(iii) a photograph.

(10) SECURITY BREACH.—

(A) IN GENERAL.—The term ''security breach'' means compromise of the security, confidentiality, or integrity of computerized data

through misrepresentation or actions that result in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to sensitive personally identifiable information.

(B) EXCLUSION.—The term ''security breach'' does not include a good faith acquisition of sensitive personally identifiable information if the sensitive personally identifiable information is not subject to further unauthorized disclosure.

(11) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term ''sensitive personally identifiable information'' means any name or number used in conjunction with any other information to identify a specific individual, including any—

(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) unique biometric data, such as—

(i) a fingerprint;

(ii) a voice print;

(iii) a retina or iris image; or

(iv) any other unique physical representation;

(C) unique electronic identification number, address, or routing code; or

(D) telecommunication identifying information or access device (as defined in section 1029(e) of title 18, United States Code).

TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY

SEC. 101. FRAUD AND RELATED CRIMINAL ACTIVITY IN CONNECTION WITH UNAUTHORIZED ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION.

Section 1030(a)(2) of title 18, United States Code, is amended—

(1) in subparagraph (B), by striking ''or'' after the semicolon;

(2) in subparagraph (C), by inserting ''or'' after the semicolon; and

(3) by adding at the end the following:

''(D) information contained in the databases or systems of a data broker, or in other

personal electronic records, as such terms are defined in section 3 of the Personal Data Privacy and Security Act of 2005;''.

SEC. 102. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION WITH UNAUTHORIZED ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION.

Section 1961(1) of title 18, United States Code, is amended by inserting ''section 1030(a)(2)(D)(relating to fraud and related activity in connection with unauthorized access to personally identifiable information,'' before ''section 1084''.

SEC. 103. CONCEALMENT OF SECURITY BREACHES INVOLVING PERSONALLY IDENTIFIABLE INFORMATION.

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

''§ 1039. Concealment of security breaches involving personally identifiable information

''Whoever, having knowledge of a security breach requiring notice to individuals under title IV of the Personal Data Privacy and Security Act of 2005, intentionally and willfully conceals the fact of, or information related to, such security breach, shall be fined under this title or imprisoned not more than 5 years, or both.''.

(b) 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:

"1039. Concealment of security breaches involving personally identifiable information.".

SEC. 104. AGGRAVATED FRAUD IN CONNECTION WITH COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding after section 1030 the following:

"§ 1030A. Aggravated fraud in connection with computers

"(a) IN GENERAL.—Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly obtains, accesses, or transmits, without lawful authority, a means of identification of another person may, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of up to 2 years.

"(b) CONSECUTIVE SENTENCES.—Notwithstanding any other provision of law, should a court in its discretion impose an additional sentence under subsection (a)—

"(1) no term of imprisonment imposed on a person under this section shall run concurrently, ex-

cept as provided in paragraph (3), with any other term of imprisonment imposed on such person under any other provision of law, including any term of imprisonment imposed for the felony during which the means of identifications was obtained, accessed, or transmitted;

''(2) in determining any term of imprisonment to be imposed for the felony during which the means of identification was obtained, accessed, or transmitted, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(3) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section.

''(c) DEFINITION.—For purposes of this section, the term 'felony violation enumerated in subsection (c)' means any offense that is a felony violation of paragraphs (2) through (7) of section 1030(a).''.

(b) CONFORMING AND TECHNICAL AMENDMENTS.—The table of sections for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following new item:

"1030A. Aggravated fraud in connection with computers.".

SEC. 105. REVIEW AND AMENDMENT OF FEDERAL SENTENCING GUIDELINES RELATED TO FRAUDULENT ACCESS TO OR MISUSE OF DIGITIZED OR ELECTRONIC PERSONALLY IDENTIFIABLE INFORMATION.

(a) REVIEW AND AMENDMENT.—Not later than 180 days after the date of enactment of this Act, the United States Sentencing Commission, pursuant to its authority under section 994 of title 28, United States Code, and in accordance with this section, shall review and, if appropriate, amend the Federal sentencing guidelines (including its policy statements) applicable to persons convicted of using fraud to access, or misuse of, digitized or electronic personally identifiable information, including identity theft or any offense under—

(1) sections 1028, 1028A, 1030, 1030A, 2511, and 2701 of title 18, United States Code; or

(2) any other relevant provision.

(b) REQUIREMENTS.—In carrying out the requirements of this section, the United States Sentencing Commission shall—

(1) ensure that the Federal sentencing guidelines (including its policy statements) reflect—

(A) the serious nature of the offenses and penalties referred to in this Act;

(B) the growing incidences of theft and misuse of digitized or electronic personally identifiable information, including identity theft; and

(C) the need to deter, prevent, and punish such offenses;

(2) consider the extent to which the Federal sentencing guidelines (including its policy statements) adequately address violations of the sections amended by this Act to—

(A) sufficiently deter and punish such offenses; and

(B) adequately reflect the enhanced penalties established under this Act;

(3) maintain reasonable consistency with other relevant directives and sentencing guidelines;

(4) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(5) consider whether to provide a sentencing enhancement for those convicted of the offenses described in subsection (a), if the conduct involves—

(A) the online sale of fraudulently obtained or stolen personally identifiable information;

(B) the sale of fraudulently obtained or stolen personally identifiable information to an individual who is engaged in terrorist activity or aiding other individuals engaged in terrorist activity; or

(C) the sale of fraudulently obtained or stolen personally identifiable information to finance terrorist activity or other criminal activities;

(6) make any necessary conforming changes to the Federal sentencing guidelines to ensure that such guidelines (including its policy statements) as described in subsection (a) are sufficiently stringent to deter, and adequately reflect crimes related to fraudulent access to, or misuse of, personally identifiable information; and

(7) ensure that the Federal sentencing guidelines adequately meet the purposes of sentencing under section 3553(a)(2) of title 18, United States Code.

(c) EMERGENCY AUTHORITY TO SENTENCING COMMISSION.—The United States Sentencing Commission may, as soon as practicable, promulgate amendments under this section in accordance with procedures established in section 21(a) of the Sentencing Act of 1987 (28 U.S.C. 994 note) as though the authority under that Act had not expired.

TITLE II—ASSISTANCE FOR STATE AND LOCAL LAW ENFORCEMENT COMBATING CRIMES RELATED TO FRAUDULENT, UNAUTHORIZED, OR OTHER CRIMINAL USE OF PERSONALLY IDENTIFIABLE INFORMATION

SEC. 201. GRANTS FOR STATE AND LOCAL ENFORCEMENT.

(a) IN GENERAL.—Subject to the availability of amounts provided in advance in appropriations Acts, the Assistant Attorney General for the Office of Justice Programs of the Department of Justice may award a grant to a State to establish and develop programs to increase

and enhance enforcement against crimes related to fraudulent, unauthorized, or other criminal use of personally identifiable information.

(b) APPLICATION.—A State seeking a grant under subsection (a) shall submit an application to the Assistant Attorney General for the Office of Justice Programs of the Department of Justice at such time, in such manner, and containing such information as the Assistant Attorney General may require.

(c) USE OF GRANT AMOUNTS.—A grant awarded to a State under subsection (a) shall be used by a State, in conjunction with units of local government within that State, State and local courts, other States, or combinations thereof, to establish and develop programs to—

(1) assist State and local law enforcement agencies in enforcing State and local criminal laws relating to crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information;

(2) assist State and local law enforcement agencies in educating the public to prevent and identify crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information;

(3) educate and train State and local law enforcement officers and prosecutors to conduct investigations and forensic analyses of evidence and prosecutions of crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information;

(4) assist State and local law enforcement officers and prosecutors in acquiring computer and other equipment to conduct investigations and forensic analysis of evidence of crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information; and

(5) facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information with State and local law enforcement officers and prosecutors, including the use of multi-jurisdictional task forces.

(d) ASSURANCES AND ELIGIBILITY.—To be eligible to receive a grant under subsection (a), a State shall provide assurances to the Attorney General that the State—

(1) has in effect laws that penalize crimes involving the fraudulent, unauthorized, or other crimi-

nal use of personally identifiable information, such as penal laws prohibiting—

(A) fraudulent schemes executed to obtain personally identifiable information;

(B) schemes executed to sell or use fraudulently obtained personally identifiable information; and

(C) online sales of personally identifiable information obtained fraudulently or by other illegal means;

(2) will provide an assessment of the resource needs of the State and units of local government within that State, including criminal justice resources being devoted to the investigation and enforcement of laws related to crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information; and

(3) will develop a plan for coordinating the programs funded under this section with other federally funded technical assistant and training programs, including directly funded local programs such as the Local Law Enforcement Block Grant program (described under the heading ''Violent Crime Reduction Programs, State and Local Law Enforcement Assistance'' of the Departments of Commerce, Justice,

and State, the Judiciary, and Related Agencies Appropriations Act, 1998 (Public Law 105–119)).

(e) MATCHING FUNDS.—The Federal share of a grant received under this section may not exceed 90 percent of the total cost of a program or proposal funded under this section unless the Attorney General waives, wholly or in part, the requirements of this subsection.

SEC. 202. AUTHORIZATION OF APPROPRIATIONS.

(a) IN GENERAL.—There is authorized to be appropriated to carry out this title $25,000,000 for each of fiscal years 2006 through 2009.

(b) LIMITATIONS.—Of the amount made available to carry out this title in any fiscal year not more than 3 percent may be used by the Attorney General for salaries and administrative expenses.

(c) MINIMUM AMOUNT.—Unless all eligible applications submitted by a State or units of local government within a State for a grant under this title have been funded, the State, together with grantees within the State (other than Indian tribes), shall be allocated in each fiscal year under this title not less than 0.75 percent of the total amount appropriated in the fiscal year for grants pursuant to this title, except that the United States Virgin Islands, American Samoa, Guam, and the Northern Mariana Islands each shall be allocated 0.25 percent.

(d) GRANTS TO INDIAN TRIBES.—Notwithstanding any other provision of this title, the Attorney General may use amounts made available under this title to make grants to Indian tribes for use in accordance with this title.

TITLE III—DATA BROKERS

SEC. 301. TRANSPARENCY AND ACCURACY OF DATA COLLECTION.

(a) IN GENERAL.—Data brokers engaging in interstate commerce are subject to the requirements of this title for any offered product or service offered to third parties that allows access, use, compilation, distribution, processing, analyzing, or evaluating personally identifiable information, unless that product or service is currently subject to similar protections under subsections (b) and (g) of this section, the Fair Credit Reporting Act (Public Law 91–508), or the Gramm-Leach Bliley Act (Public Law 106–102), and implementing regulations.

(b) DISCLOSURES TO INDIVIDUALS.—

(1) IN GENERAL.—A data broker shall, upon the request of an individual, clearly and accurately disclose to such individual for a reasonable fee all personal electronic records pertaining to that individual maintained for disclosure to third parties in

the databases or systems of the data broker at the time of the request.

(2) INFORMATION ON HOW TO CORRECT INACCURACIES.—The disclosures required under paragraph (1) shall also include guidance to individuals on the processes and procedures for demonstrating and correcting any inaccuracies.

(c) CREATION OF AN ACCURACY RESOLUTION PROCESS.—A data broker shall develop and publish on its website timely and fair processes and procedures for responding to claims of inaccuracies, including procedures for correcting inaccurate information in the personal electronic records it maintains on individuals.

(d) ACCURACY RESOLUTION PROCESS.—

(1) PUBLIC RECORD INFORMATION.—

(A) IN GENERAL.—If an individual notifies a data broker of a dispute as to the completeness or accuracy of information, and the data broker determines that such information is derived from a public record source, the data broker shall determine within 30 days whether the information in its system accurately and completely records the information offered by the public record source.

(B) DATA BROKER ACTIONS.—If a data broker determines under subparagraph (A) that the information in its systems—

(i) does not accurately and completely record the information offered by a public record source, the data broker shall correct any inaccuracies or incompleteness, and provide to such individual written notice of such changes; and

(ii) does accurately and completely record the information offered by a public record source, the data broker shall—

(I) provide such individual with the name, address, and telephone contact information of the public record source; and

(II) notify such individual of the right to add to the personal electronic record of the individual maintained by the data broker a statement disputing the accuracy or completeness of the information for a period of 90 days under subsection (e).

(2) INVESTIGATION OF DISPUTED NON-PUBLIC RECORD INFORMATION.—If the completeness or ac-

curacy of any non-public record information disclosed to an individual under subsection (b) is disputed by the individual and such individual notifies the data broker directly of such dispute, the data broker shall, before the end of the 30-day period beginning on the date on which the data broker receives the notice of the dispute—

(A) investigate free of charge and record the current status of the disputed information; or

(B) delete the item from the individuals data file in accordance with paragraph (8).

(3) EXTENSION OF PERIOD TO INVESTIGATE.—Except as provided in paragraph (4), the 30-day period described in paragraph (1) may be extended for not more than 15 additional days if a data broker receives information from the individual during that 30-day period that is relevant to the investigation.

(4) LIMITATIONS ON EXTENSION OF PERIOD TO INVESTIGATE.—Paragraph (3) shall not apply to any investigation in which, during the 30-day period described in paragraph (1), the information that is the subject of the investigation is found to be inaccurate or incomplete or a data broker determines that the information cannot be verified.

(5) NOTICE IDENTIFYING THE DATA FURNISHER.—If the completeness or accuracy of any information disclosed to an individual under subsection (b) is disputed by the individual, a data broker shall provide upon the request of the individual, the name, business address, and telephone contact information of any data furnisher who provided an item of information in dispute.

(6) DETERMINATION THAT DISPUTE IS FRIVOLOUS OR IRRELEVANT.—

(A) IN GENERAL.—Notwithstanding paragraphs (1) through (4), a data broker may decline to investigate or terminate an investigation of information disputed by an individual under those paragraphs if the data broker reasonably determines that the dispute by the individual is frivolous or irrelevant, including by reason of a failure by the individual to provide sufficient information to investigate the disputed information.

(B) NOTICE.—Not later than 5 business days after making any determination in accordance with subparagraph (A) that a dispute is frivolous or irrelevant, a data broker shall notify the individual of such determination by

mail, or if authorized by the individual, by any other means available to the data broker.

(C) CONTENTS OF NOTICE.—A notice under subparagraph (B) shall include—

(i) the reasons for the determination under subparagraph (A); and

(ii) identification of any information required to investigate the disputed information, which may consist of a standardized form describing the general nature of such information.

(7) CONSIDERATION OF INDIVIDUAL INFORMATION.—In conducting any investigation with respect to disputed information in the personal electronic record of any individual, a data broker shall review and consider all relevant information submitted by the individual in the period described in paragraph (2) with respect to such disputed information.

(8) TREATMENT OF INACCURATE OR UNVERIFIABLE INFORMATION.—

(A) IN GENERAL.—If, after any review of public record information under paragraph (1) or any investigation of any information disputed by an individual under paragraphs (2) through (4), an item of information is found to be inac-

curate or incomplete or cannot be verified, a data broker shall promptly delete that item of information from the individual's personal electronic record or modify that item of information, as appropriate, based on the results of the investigation.

(B) NOTICE TO INDIVIDUALS OF REINSERTION OF PREVIOUSLY DELETED INFORMATION.—If any information that has been deleted from an individual's personal electronic record pursuant to subparagraph (A) is reinserted in the personal electronic record of the individual, a data broker shall, not later than 5 days after reinsertion, notify the individual of the reinsertion and identify any data furnisher not previously disclosed in writing, or if authorized by the individual for that purpose, by any other means available to the data broker, unless such notification has been previously given under this subsection.

(C) NOTICE OF RESULTS OF INVESTIGATION OF DISPUTED NON-PUBLIC RECORD.—

(i) IN GENERAL.—Not later than 5 business days after the completion of an investigation under paragraph (2), a data

broker shall provide written notice to an individual of the results of the investigation, by mail or, if authorized by the individual for that purpose, by other means available to the data broker.

(ii) ADDITIONAL REQUIREMENT.—Before the expiration of the 5-day period, as part of, or in addition to such notice, a data broker shall, in writing, provide to an individual—

(I) a statement that the investigation is completed;

(II) a report that is based upon the personal electronic record of such individual as that personal electronic record is revised as a result of the investigation;

(III) a notice that, if requested by the individual, a description of the procedures used to determine the accuracy and completeness of the information shall be provided to the individual by the data broker, including the business name, address, and telephone number of any data furnisher

of information contacted in connection with such information; and

(IV) a notice that the individual has the right to request notifications under subsection (g).

(D) DESCRIPTION OF INVESTIGATION PROCEDURES.—Not later than 15 days after receiving a request from an individual for a description referred to in subparagraph (C)(ii)(III), a data broker shall provide to the individual such a description.

(E) EXPEDITED DISPUTE RESOLUTION.—If by no later than 3 business days after the date on which a data broker receives notice of a dispute from an individual of information in the personal electronic record of such individual in accordance with paragraph (2), a data broker resolves such dispute in accordance with subparagraph (A) by the deletion of the disputed information, then the data broker shall not be required to comply with subsections (e) and (f) with respect to that dispute if the data broker provides—

(i) to the individual, by telephone, prompt notice of the deletion; and

(ii) to the individual a right to request that the data broker furnish notifications under subsection (g).

(e) STATEMENT OF DISPUTE.—

(1) IN GENERAL.—If the completeness or accuracy of any information disclosed to an individual under subsection (b) is disputed, an individual may file a brief statement setting forth the nature of the dispute.

(2) CONTENTS OF STATEMENT.—A data broker may limit the statements made pursuant to paragraph (1) to not more than 100 words if it provides an individual with assistance in writing a clear summary of the dispute or until the dispute is resolved, whichever is earlier.

(f) NOTIFICATION OF DISPUTE IN SUBSEQUENT REPORTS.—Whenever a statement of a dispute is filed under subsection (e), unless there is a reasonable grounds to believe that it is frivolous or irrelevant, a data broker shall, in any subsequent report, product, or service containing the information in question, clearly note that it is disputed by an individual and provide either the statement of such individual or a clear and accurate codification or summary thereof for a period of 90 days after the data broker first posts the statement of dispute.

(g) NOTIFICATION OF DELETION OF DISPUTED INFORMATION.—Following any deletion of information which is found to be inaccurate or whose accuracy can no longer be verified, a data broker shall, at the request of an individual, furnish notification that the item has been deleted or the statement, codification, or summary pursuant to subsection (e) or (f) to any user or customer of the products or services of the data broker who has within 90 days received a report with the deleted or disputed information or has electronically accessed the deleted or disputed information.

SEC. 302. ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) PENALTIES.—Any data broker that violates the provisions of section 301 shall be subject to civil penalties of not more than $1,000 per violation per day, with a maximum of $15,000 per day, while such violations persist.

(2) INTENTIONAL OR WILLFUL VIOLATION.—A data broker that intentionally or willfully violates the provisions of section 301 shall be subject to additional penalties in the amount of $1,000 per violation per day, with a maximum of an additional $15,000 per day, while such violations persist.

(3) EQUITABLE RELIEF.—A data broker engaged in interstate commerce that violates this section may be enjoined from further violations by a court of competent jurisdiction.

(4) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this subsection are cumulative and shall not affect any other rights and remedies available under law.

(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—Whenever it appears that a data broker to which this title applies has engaged, is engaged, or is about to engage, in any act or practice constituting a violation of this title, the Attorney General may bring a civil action in an appropriate district court of the United States to—

(A) enjoin such act or practice;

(B) enforce compliance with this title;

(C) obtain damages—

(i) in the sum of actual damages, restitution, and other compensation on behalf of the affected residents of a State; and

(ii) punitive damages, if the violation is willful or intentional; and

(D) obtain such other relief as the court determines to be appropriate.

(2) OTHER INJUNCTIVE RELIEF.—Upon a proper showing in the action under paragraph (1), the court shall grant a permanent injunction or a temporary restraining order without bond.

(c) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—In any case in which the attorney general 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 an act or practice that violates this title, the State may bring a civil action on behalf of the residents of that State in a district court of the United States of appropriate jurisdiction, or any other court of competent jurisdiction, to—

(A) enjoin that act or practice;

(B) enforce compliance with this title;

(C) obtain—

(i) damages in the sum of actual damages, restitution, or other compensation on behalf of affected residents of the State; and

(ii) punitive damages, if the violation is willful or intentional; or

(D) obtain such other legal and equitable relief as the court may consider to be appropriate.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under this subsection, the attorney general of the State involved shall provide to the Attorney General—

(i) a written notice of that action; and

(ii) a copy of the complaint for that action.

(B) EXCEPTION.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general of a State determines that it is not feasible to provide the notice described in this subparagraph before the filing of the action.

(C) NOTIFICATION WHEN PRACTICABLE.—In an action described under subparagraph (B), the attorney general of a State shall provide the written notice and the copy of the complaint to the Attorney General as soon after the filing of the complaint as practicable.

(3) ATTORNEY GENERAL AUTHORITY.—Upon receiving notice under paragraph (2), the Attorney General shall have the right to—

(A) move to stay the action, pending the final disposition of a pending Federal proceeding or action as described in paragraph (4);

(B) intervene in an action brought under paragraph (1); and

(C) file petitions for appeal.

(4) PENDING PROCEEDINGS.—If the Attorney General has instituted a proceeding or action for a violation of this Act or any regulations thereunder, no attorney general of a State may, during the pendency of such proceeding or action, bring an action under this subsection against any defendant named in such criminal proceeding or civil action for any violation that is alleged in that proceeding or action.

(5) RULE OF 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 and affirmations; or

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

(6) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under this subsection may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1931 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under this subsection process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

SEC. 303. RELATION TO STATE LAWS.

(a) IN GENERAL.—Except as provided in subsection (b), this title does not annul, alter, affect, or exempt any person subject to the provisions of this title from complying with the laws of any State with respect to the access, use, compilation, distribution, processing, analysis, and evaluation of any personally identifiable information by data brokers, except to the extent that those laws are inconsistent with any provisions of this title, and then only to the extent of such inconsistency.

(b) EXCEPTIONS.—No requirement or prohibition may be imposed under the laws of any State with respect to any subject matter regulated under section 301, relating to individual access to, and correction of, personal electronic records.

SEC. 304. EFFECTIVE DATE.

This title shall take effect 180 days after the date of enactment of this Act.

TITLE IV—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

Subtitle A—Data Privacy and Security Program

SEC. 401. PURPOSE AND APPLICABILITY OF DATA PRIVACY AND SECURITY PROGRAM.

(a) PURPOSE.—The purpose of this subtitle is to ensure standards for developing and implementing administrative, technical, and physical safeguards to protect the privacy, security, confidentiality, integrity, storage, and disposal of personally identifiable information.

(b) IN GENERAL.—A business entity engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of personally identifiable information in electronic or digital form on 10,000 or more United States persons is subject to the

requirements for a data privacy and security program under section 402 for protecting personally identifiable information.

(c) LIMITATIONS.—Notwithstanding any other obligation under this subtitle, this subtitle does not apply to—

(1) financial institutions subject to—

(A) the data security requirements and implementing regulations under the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.); and

(B) examinations for compliance with the requirements of this Act by 1 or more Federal functional regulators (as defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809)); or

(2) ''covered entities'' subject to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.), including the data security requirements and implementing regulations of that Act.

SEC. 402. REQUIREMENTS FOR A PERSONAL DATA PRIVACY AND SECURITY PROGRAM.

(a) PERSONAL DATA PRIVACY AND SECURITY PROGRAM.—Unless otherwise limited under section 401(c), a business entity subject to this subtitle shall comply with

the following safeguards to protect the privacy and security of personally identifiable information:

(1) SCOPE.—A business entity shall implement a comprehensive personal data privacy and security program, written in 1 or more readily accessible parts, that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the business entity and the nature and scope of its activities.

(2) DESIGN.—The personal data privacy and security program shall be designed to—

(A) ensure the privacy, security, and confidentiality of personal electronic records;

(B) protect against any anticipated vulnerabilities to the privacy, security, or integrity of personal electronic records; and

(C) protect against unauthorized access to use of personal electronic records that could result in substantial harm or inconvenience to any individual.

(3) RISK ASSESSMENT.—A business entity shall—

(A) identify reasonably foreseeable internal and external vulnerabilities that could result in unauthorized access, disclosure, use, or alter-

ation of personally identifiable information or systems containing personally identifiable information;

(B) assess the likelihood of and potential damage from unauthorized access, disclosure, use, or alteration of personally identifiable information; and

(C) assess the sufficiency of its policies, technologies, and safeguards in place to control and minimize risks from unauthorized access, disclosure, use, or alteration of personally identifiable information.

(4) RISK MANAGEMENT AND CONTROL.—Each business entity shall—

(A) design its personal data privacy and security program to control the risks identified under paragraph (3); and

(B) adopt measures commensurate with the sensitivity of the data as well as the size, complexity, and scope of the activities of the business entity that—

(i) control access to systems and facilities containing personally identifiable information, including controls to authen-

ticate and permit access only to authorized individuals;

(ii) detect actual and attempted fraudulent, unlawful, or unauthorized access, disclosure, use, or alteration of personally identifiable information, including by employees and other individuals otherwise authorized to have access; and

(iii) protect personally identifiable information during use, transmission, storage, and disposal by encryption or other reasonable means (including as directed for disposal of records under section 628 of the Fair Credit Reporting Act (15 U.S.C. 1681w) and the implementing regulations of such Act as set forth in section 682 of title 16, Code of Federal Regulations).

(5) ACCOUNTABILITY.—Each business entity required to establish a data security program under section 401 shall publish on its website or make otherwise available the terms of such program to the extent that such terms do not reveal information that compromise data security or privacy.

(b) TRAINING.—Each business entity subject to this subtitle shall take steps to ensure employee training and

supervision for implementation of the data security program of the business entity.

(c) VULNERABILITY TESTING.—

(1) IN GENERAL.—Each business entity subject to this subtitle shall take steps to ensure regular testing of key controls, systems, and procedures of the personal data privacy and security program to detect, prevent, and respond to attacks or intrusions, or other system failures.

(2) FREQUENCY.—The frequency and nature of the tests required under paragraph (1) shall be determined by the risk assessment of the business entity under subsection (a)(3).

(d) RELATIONSHIP TO SERVICE PROVIDERS.—In the event a business entity subject to this subtitle engages service providers not subject to this subtitle, such business entity shall—

(1) exercise appropriate due diligence in selecting those service providers for responsibilities related to personally identifiable information, and take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the security, privacy, and integrity of the personally identifiable information at issue; and

(2) require those service providers by contract to implement and maintain appropriate measures designed to meet the objectives and requirements governing entities subject to this section, section 401, and subtitle B.

(e) PERIODIC ASSESSMENT AND PERSONAL DATA PRIVACY AND SECURITY MODERNIZATION.—Each business entity subject to this subtitle shall on a regular basis monitor, evaluate, and adjust, as appropriate its data privacy and security program in light of any relevant changes in—

(1) technology;

(2) the sensitivity of personally identifiable information;

(3) internal or external threats to personally identifiable information; and

(4) the changing business arrangements of the business entity, such as—

(A) mergers and acquisitions;

(B) alliances and joint ventures;

(C) outsourcing arrangements;

(D) bankruptcy; and

(E) changes to personally identifiable information systems.

(f) IMPLEMENTATION TIME LINE.—Not later than 1 year after the date of enactment of this Act, a business entity subject to the provisions of this subtitle shall implement a data privacy and security program pursuant to this subtitle.

SEC. 403. ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) IN GENERAL.—Any business entity that violates the provisions of sections 401 or 402 shall be subject to civil penalties of not more than $5,000 per violation per day, with a maximum of $35,000 per day, while such violations persist.

(2) INTENTIONAL OR WILLFUL VIOLATION.—A business entity that intentionally or willfully violates the provisions of sections 401 or 402 shall be subject to additional penalties in the amount of $5,000 per violation per day, with a maximum of an additional $35,000 per day, while such violations persist.

(3) EQUITABLE RELIEF.—A business entity engaged in interstate commerce that violates this section may be enjoined from further violations by a court of competent jurisdiction.

(4) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this section are

cumulative and shall not affect any other rights and remedies available under law

(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—Whenever it appears that a business entity or agency to which this subtitle applies has engaged, is engaged, or is about to engage, in any act or practice constituting a violation of this subtitle, the Attorney General may bring a civil action in an appropriate district court of the United States to—

(A) enjoin such act or practice;

(B) enforce compliance with this subtitle; and

(C) obtain damages—

(i) in the sum of actual damages, restitution, and other compensation on behalf of the affected residents of a State; and

(ii) punitive damages, if the violation is willful or intentional; and

(D) obtain such other relief as the court determines to be appropriate.

(2) OTHER INJUNCTIVE RELIEF.—Upon a proper showing in the action under paragraph (1),

the court shall grant a permanent injunction or a temporary restraining order without bond.

(c) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—In any case in which the attorney general 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 an act or practice that violates this subtitle, the State may bring a civil action on behalf of the residents of that State in a district court of the United States of appropriate jurisdiction, or any other court of competent jurisdiction, to—

(A) enjoin that act or practice;

(B) enforce compliance with this subtitle;

(C) obtain—

(i) damages in the sum of actual damages, restitution, or other compensation on behalf of affected residents of the State; and

(ii) punitive damages, if the violation is willful or intentional; or

(D) obtain such other legal and equitable relief as the court may consider to be appropriate.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under this subsection, the attorney general of the State involved shall provide to the Attorney General—

(i) a written notice of that action; and

(ii) a copy of the complaint for that action.

(B) EXCEPTION.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general of a State determines that it is not feasible to provide the notice described in this subparagraph before the filing of the action.

(C) NOTIFICATION WHEN PRACTICABLE.—In an action described under subparagraph (B), the attorney general of a State shall provide the written notice and the copy of the complaint to the Attorney General as soon after the filing of the complaint as practicable.

(3) ATTORNEY GENERAL AUTHORITY.—Upon receiving notice under paragraph (2), the Attorney General shall have the right to—

(A) move to stay the action, pending the final disposition of a pending Federal proceeding or action as described in paragraph (4);

(B) intervene in an action brought under paragraph (1); and

(C) file petitions for appeal.

(4) PENDING PROCEEDINGS.—If the Attorney General has instituted a proceeding or action for a violation of this Act or any regulations thereunder, no attorney general of a State may, during the pendency of such proceeding or action, bring an action under this subsection against any defendant named in such criminal proceeding or civil action for any violation that is alleged in that proceeding or action.

(5) RULE OF 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 and affirmations; or

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

(6) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under this subsection may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1931 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under this subsection process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

SEC. 404. RELATION TO STATE LAWS.

(a) IN GENERAL.—Except as provided in subsection (b), this title does not annul, alter, affect, or exempt any person subject to the provisions of this title from complying with the laws of any State with respect to security programs for personally identifiable information, except to the extent that those laws are inconsistent with any provisions of this title, and then only to the extent of such inconsistency.

(b) EXCEPTIONS.—No requirement or prohibition may be imposed under the laws of any State with respect to any subject matter regulated under section 401(c), relating to entities exempted from compliance with subtitle A.

Subtitle B—Security Breach Notification

SEC. 421. RIGHT TO NOTICE OF SECURITY BREACH.

(a) IN GENERAL.—Unless delayed under section 422(d) or exempted under section 424, any business entity or agency engaged in interstate commerce that involves collecting, accessing, using, transmitting, storing, or disposing of personally identifiable information shall notify, following the discovery of a security breach of its systems or databases in its possession or direct control when such security breach impacts sensitive personally identifiable information—

(1) if the security breach impacts more than 10,000 individuals nationwide, impacts a database, networked or integrated databases, or other data system associated with more than 1,000,000 individuals nationwide, impacts databases owned or used by the Federal Government, or involves sensitive personally identifiable information of employees and contractors of the Federal Government—

(A) the United States Secret Service, which shall be responsible for notifying——

(i) the Federal Bureau of Investigation, if the security breach involves espionage, foreign counterintelligence, informa-

tion protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service under section 3056(a) of title 18, United States Code; and

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

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

(2) each consumer reporting agency described in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a), pursuant to subsection (b); and

(3) any resident of the United States whose sensitive personally identifiable information was subject to the security breach, pursuant to sections 422 and 423, but in the event a business entity or agency is unable to identify the specific residents of the United States whose sensitive personally identifiable information was impacted by a security breach, the business entity or agency shall consult with the

United States Secret Service to determine the scope of individuals who there is a reasonable basis to conclude have been impacted by such breach and should receive notice.

(b) CONSUMER REPORTING AGENCIES.—Any business entity or agency obligated to provide notice of a security breach to more than 1,000 residents of the United States under subsection (a)(3) shall inform consumer reporting agencies of the fact and scope of such notices for the purpose of facilitating and managing potential increases in consumer inquiries and mitigating identity theft or other negative consequences of the breach.

SEC. 422. NOTICE PROCEDURES.

(a) TIMELINESS OF NOTICE.—

(1) IN GENERAL.—Except as provided in subsection (c), all notices required under section 421 shall be issued expeditiously and without unreasonable delay after discovery of the events requiring notice.

(2) 14-DAY RULE.—The notices to Federal law enforcement and the attorney general of each State affected by a security breach required under section 421(a) shall be delivered not later than 14 days after discovery of the events requiring notice.

(3) REQUIRED DISCLOSURE.—In complying with the notices required under section 421, a business entity or agency shall expeditiously and without unreasonable delay take reasonable measures which are necessary to—

(A) determine the scope and assess the impact of a breach under section 421; and

(B) restore the reasonable integrity of the data system.

(b) METHOD.—Any business entity or agency obligated to provide notice under section 421 shall be in compliance with that section if they provide notice as follows:

(1) WRITTEN NOTIFICATION.—By written notification to the last known home address of the individual whose sensitive personally identifiable information was breached, or if unknown, notification via telephone call to the last known home telephone number.

(2) INTERNET POSTING.—If more than 1,000 residents of the United States require notice under section 421 and if the business entity or agency maintains an Internet site, conspicuous posting of the notice on the Internet site of the business entity or agency.

(3) MEDIA NOTICE.—If more than 5,000 residents of a State or jurisdiction are impacted, notice to major media outlets serving that State or jurisdiction.

(c) DELAY OF NOTIFICATION FOR LAW ENFORCEMENT PURPOSES.—

(1) IN GENERAL.—If Federal law enforcement or the attorney general of a State determines that the notices required under section 421(a) would impede a criminal investigation, such notices may be delayed until such law enforcement agency determines that the notices will no longer compromise such investigation.

(2) EXTENDED DELAY OF NOTIFICATION FOR LAW ENFORCEMENT PURPOSES.—If a business entity or agency has delayed the notices required under paragraphs (2) and (3) of section 421(a) as described in paragraph (1), the business entity or agency shall give notice 30 days after the day such law enforcement delay was invoked unless Federal law enforcement provides written notification that further delay is necessary.

SEC. 423. CONTENT OF NOTICE.

(a) IN GENERAL.—A business entity or agency obligated to provide notice to residents of the United States

under section 421(a)(3) shall clearly and concisely detail the nature of the sensitive personally identifiable information impacted by the security breach.

(b) CONTENT OF NOTICE.—A notice under subsection (a) shall include—

(1) the availability of victim protection assistance pursuant to section 425;

(2) guidance on how to request that a fraud alert be placed in the file of the individual maintained by consumer reporting agencies, pursuant to section 605A of the Fair Credit Reporting Act (15 U.S.C. 1681c–1) and the implications of such actions;

(3) the availability of a summary of rights for identity theft victims from consumer reporting agencies, pursuant to section 609 of the Fair Credit Reporting Act (15 U.S.C. 1681g);

(4) if applicable, notice that the State where an individual resides has a statute that provides the individual the right to place a security freeze on their credit report; and

(5) if applicable, notice that consumer reporting agencies have been notified of the security breach.

(c) MARKETING NOT ALLOWED IN NOTICE.—A notice under subsection (a) may not include—

(1) marketing information;

(2) sales offers; or

(3) any solicitation regarding the collection of additional personally identifiable information from an individual.

SEC. 424. RISK ASSESSMENT AND FRAUD PREVENTION NOTICE EXEMPTIONS.

(a) RISK ASSESSMENT EXEMPTION.—A business entity will be exempt from the notice requirements under paragraphs (2) and (3) of section 421(a), if a risk assessment conducted in consultation with Federal law enforcement and the attorney general of each State affected by a security breach concludes that there is a de minimis risk of harm to the individuals whose sensitive personally identifiable information was at issue in the security breach.

(b) FRAUD PREVENTION EXEMPTION.—A business entity will be exempt from the notice requirement under section 421(a) if—

(1) the nature of the sensitive personally identifiable information subject to the security breach cannot be used to facilitate transactions or facilitate identity theft to further transactions with another business entity that is not the business entity subject to the security breach notification requirements of section 421;

(2) the business entity utilizes a security program reasonably designed to block the use of the sensitive personally identifiable information to initiate unauthorized transactions before they are charged to the account of the individual; and

(3) the business entity has a policy in place to provide notice and provides such notice after a breach of the security of the system has resulted in fraud or unauthorized transactions, but does not necessarily require notice in other circumstances.

SEC. 425. VICTIM PROTECTION ASSISTANCE.

Any business entity or agency obligated to provide notice to residents of the United States under section 421(a)(3) shall offer to those same residents to cover the cost of—

(1) monthly access to a credit report for a period of 1 year from the date of notice provided under section 421(a)(3); and

(2) credit-monitoring services for up to 1 year from the date of notice provided under section 421(a)(3).

SEC. 426. ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) IN GENERAL.—Any business entity that violates the provisions of sections 421 through 425

shall be subject to civil penalties of not more than $5,000 per violation per day, with a maximum of $55,000 per day, while such violations persist.

(2) INTENTIONAL OR WILLFUL VIOLATION.—A business entity that intentionally or willfully violates the provisions of sections 421 through 425 shall be subject to additional penalties in the amount of $5,000 per violation per day, with a maximum of an additional $55,000 per day, while such violations persist.

(3) EQUITABLE RELIEF.—A business entity engaged in interstate commerce that violates this section may be enjoined from further violations by a court of competent jurisdiction.

(4) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this section are cumulative and shall not affect any other rights and remedies available under law.

(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—Whenever it appears that a business entity or agency to which this subtitle applies has engaged, is engaged, or is about to engage, in any act or practice constituting a violation of this subtitle, the Attorney General may bring a civil ac-

tion in an appropriate district court of the United States to—

(A) enjoin such act or practice;

(B) enforce compliance with this subtitle; and

(C) obtain damages—

(i) in the sum of actual damages, restitution, and other compensation on behalf of the affected residents of a State; and

(ii) punitive damages, if the violation is willful or intentional; and

(D) obtain such other relief as the court determines to be appropriate.

(2) OTHER INJUNCTIVE RELIEF.—Upon a proper showing in the action under paragraph (1), the court shall grant a permanent injunction or a temporary restraining order without bond.

(c) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been, or is threatened to be, adversely affected by a violation of this subtitle, the State, as parens patriae, may bring a civil action on behalf of the residents of that State in a district court of the

United States of appropriate jurisdiction, or any other court of competent jurisdiction, to—

(A) enjoin that practice;

(B) enforce compliance with this subtitle;

(C) obtain damages—

(i) in the sum of actual damages, restitution, and other compensation on behalf of the affected residents of that State; and

(ii) punitive damages, if the violation is willful or intentional; and

(D) obtain such other equitable relief as the court may consider to be appropriate.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Attorney General—

(i) written notice of the action; and

(ii) a copy of the complaint for the action.

(B) EXCEPTION.—

(i) IN GENERAL.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney gen-

eral of a State determines that it is not feasible to provide the notice described in such subparagraph before the filing of the action.

(ii) NOTIFICATION WHEN PRACTICABLE.—In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the Attorney General at the time the attorney general of a State files the action.

(3) ATTORNEY GENERAL AUTHORITY.—Upon receiving notice under paragraph (2), the Attorney General shall have the right to—

(A) move to stay the action, pending the final disposition of a pending Federal proceeding or action as described in paragraph (4);

(B) intervene in an action brought under paragraph (1); and

(C) file petitions for appeal.

(4) PENDING PROCEEDINGS.—If the Attorney General has instituted a proceeding or action for a violation of this Act or any regulations thereunder, no attorney general of a State may, during the pendency of such proceeding or action, bring an action under this subsection against any defendant named

in such criminal proceeding or civil action for any violation that is alleged in that proceeding or action.

(5) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this subsection shall be construed to prevent an attorney general of a State from exercising the powers conferred on such 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.

(6) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under this subsection may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under this subsection process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

SEC. 427. RELATION TO STATE LAWS.

(a) IN GENERAL.—Except as provided in subsection (b), this title does not annul, alter, affect, or exempt any person subject to the provisions of this title from complying with the laws of any State with respect to protecting consumers from the risk of theft or misuse of personally identifiable information, except to the extent that those laws are inconsistent with any provisions of this title, and then only to the extent of such inconsistency.

(b) EXCEPTIONS.—No requirement or prohibition may be imposed under the laws of any State with respect to any subject matter regulated under—

(1) section 3(9), relating to the definition of ''security breach'';

(2) paragraphs (1)(A), (2), and (3) of subsection (a), and subsection (b) of section 421, relating to the right to notice of security breach;

(3) section 422, relating to notice procedures;

(4) section 423, relating to notice content, except that nothing in this section shall prevent a State from requiring notice of additional victim protection assistance by that State; and

(5) section 424, relating to risk assessment and fraud prevention notice exemptions.

SEC. 428. STUDY ON SECURING PERSONALLY IDENTIFIABLE INFORMATION IN THE DIGITAL ERA.

(a) REQUIREMENT FOR STUDY.—Not later than 120 days after the date of enactment of this Act, the Department of Justice shall enter into a contract with the National Research Council of the National Academies to conduct a study on securing personally identifiable information in the digital era.

(b) MATTERS TO BE ASSESSED IN REVIEW.—The study required under subsection (a) shall include—

(1) threats to the public posed by the unauthorized or improper disclosure of personally identifiable information, including threats to—

(A) law enforcement;

(B) homeland security;

(C) individual citizens; and

(D) commerce;

(2) an assessment of the benefits and costs of currently available strategies for securing personally identifiable information based on—

(A) technology;

(B) legislation;

(C) regulation; or

(D) public education;

(3) research needed to develop additional strategies;

(4) recommendations for congressional or other policy actions to further minimize vulnerabilities to the threats described in paragraph (1); and

(5) other relevant issues that in the discretion of the National Research Council warrant examination.

(c) TIME LINE FOR STUDY AND REQUIREMENT FOR REPORT.—Not later than 18-month period beginning upon completion of the performance of the contract described in subsection (a), the National Research Council shall conduct the study and report its findings, conclusions, and recommendations to Congress.

(d) FEDERAL DEPARTMENT AND AGENCY COMPLIANCE.—Federal departments and agencies shall comply with requests made by the National Science Foundation, National Research Council, and National Academies for information that is necessary to assist in preparing the report required by subsection (c).

(e) AUTHORIZATION OF APPROPRIATIONS.—Of the amounts authorized to be appropriated to the Department of Justice for Department-wide activities, $850,000 shall be made available to carry out the provisions of this section for fiscal year 2006.

SEC. 429. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated such sums as may be necessary to cover the costs incurred by the United States Secret Service to carry out investigations and risk assessments of security breaches as required under this subtitle.

SEC. 430. EFFECTIVE DATE.

This subtitle shall take effect 90 days after the date of enactment of this Act.

TITLE V—PROTECTION OF SOCIAL SECURITY NUMBERS

SEC. 501. SOCIAL SECURITY NUMBER PROTECTION.

(a) IN GENERAL.—No person may—

(1) display any individual's social security number to a third party without the voluntary and affirmatively expressed consent of such individual; or

(2) sell or purchase any social security number of an individual without the voluntary and affirmatively expressed consent of such individual.

(b) PREREQUISITES FOR CONSENT.—To obtain the consent of an individual under paragraphs (1) or (2) of subsection (a), the person displaying, selling, or attempting to sell, purchasing, or attempting to purchase the social security number of such individual shall—

(1) inform such individual of the general purpose for which the social security number will be

used, the types of persons to whom the social security number may be available, and the scope of transactions permitted by the consent; and

(2) obtain the affirmatively expressed consent (electronically or in writing) of such individual.

(c) HARVESTED SOCIAL SECURITY NUMBERS.—Subsection (a) shall apply to any public record of a Federal agency that contains social security numbers extracted from other public records for the purpose of displaying or selling such numbers to the general public.

(d) EXCEPTIONS.—Nothing in this section shall be construed to prohibit or limit the display, sale, or purchase of a social security number—

(1) as required, authorized, or excepted under Federal law;

(2) to the extent necessary for a public health purpose, including the protection of the health or safety of an individual in an emergency situation;

(3) to the extent necessary for a national security purpose;

(4) to the extent necessary for a law enforcement purpose, including the investigation of fraud and the enforcement of a child support obligation;

(5) to the extent necessary for research conducted for the purpose of advancing public knowl-

edge, on the condition that the researcher provides adequate assurances that—

(A) the social security numbers will not be used to harass, target, or publicly reveal information concerning any individual;

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

(C) the researcher has in place appropriate safeguards to protect the privacy and confidentiality of any information about individuals;

(6) if such a number is required to be submitted as part of the process for applying for any type of Federal, State, or local government benefit or program;

(7) when the transmission of the number is incidental to, and in the course of, the sale, lease, franchising, or merger of all or a portion of a business; or

(8) to the extent only the last 4 digits of a social security number are displayed.

SEC. 502. LIMITS ON PERSONAL DISCLOSURE OF SOCIAL SECURITY NUMBERS FOR COMMERCIAL TRANSACTIONS AND ACCOUNTS.

(a) IN GENERAL.—Part A of title XI of the Social Security Act (42 U.S.C. 1301 et seq.) is amended by adding the following:

"SEC. 1150A. LIMITS ON PERSONAL DISCLOSURE OF SOCIAL SECURITY NUMBERS FOR COMMERCIAL TRANSACTIONS AND ACCOUNTS.

"(a) ACCOUNT NUMBERS.—

"(1) IN GENERAL.—A business entity may not—

"(A) require an individual to use the social security number of such individual as an account number or account identifier when purchasing a commercial good or service; or

"(B) deny an individual goods or services for refusing to accept the use of the social security number of such individual as an account number or account identifier.

"(2) EXISTING ACCOUNT EXCEPTION.—Paragraph (1) shall not apply to any account number or account identifier established prior to the date of enactment of this Act.

"(b) SOCIAL SECURITY NUMBER PREREQUISITES FOR GOODS AND SERVICES.—A business entity may not

require an individual to provide the social security number of such individual when purchasing a commercial good or service or deny an individual goods or services for refusing to provide that number except for any purpose relating to—

''(1) obtaining a consumer report for any purpose permitted under the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

''(2) a background check of the individual conducted by a landlord, lessor, employer, or voluntary service agency;

''(3) law enforcement; or

''(4) a Federal, State, or local law requirement.

''(c) APPLICATION OF CIVIL MONEY PENALTIES.—A violation of this section shall be deemed to be a violation of section 1129(a).

''(d) APPLICATION OF CRIMINAL PENALTIES.—A violation of this section shall be deemed to be a violation of section 208(a)(8).''.

SEC. 503. PUBLIC RECORDS.

(a) IN GENERAL.—Except as provided in paragraph (2), paragraphs (a) and (b) of section 501 shall apply to all public records posted on the Internet or provided in an electronic medium by, or on behalf of, a Federal agency.

(b) EXCEPTIONS.—

(1) TRUNCATION AND PRIOR DISPLAYS.—Section 501(a) shall not apply to—

(A) a public record which displays only the last 4 digits of the social security number of an individual; and

(B) any record or a category of public records first posted on the Internet or provided in an electronic medium by, or on behalf of, a Federal agency prior to the date of enactment of this Act.

(2) LAW ENFORCEMENT.—Nothing in this subsection shall be construed to prevent an entity acting pursuant to a police investigation or regulatory power of a domestic governmental unit from accessing the full social security number of an individual.

SEC. 504. TREATMENT OF SOCIAL SECURITY NUMBERS ON GOVERNMENT CHECKS AND PROHIBITION OF INMATE ACCESS.

(a) PROHIBITION OF USE OF SOCIAL SECURITY NUMBERS ON CHECKS ISSUED FOR PAYMENT BY GOVERNMENTAL ENTITIES.—

(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:

''(x) No Federal, State, or local agency may display the social security account number of any individual, or any derivative of such number, on any check issued for any payment by the Federal, State, or local agency.''.

(2) EFFECTIVE DATE.—The amendment made under paragraph (1) shall apply with respect to checks issued after the date that is 3 years after the date of enactment of this Act.

(b) PROHIBITION ON INMATE ACCESS TO SOCIAL SECURITY 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 further amended by adding at the end the following:

''(xi)(I) No Federal, State, or local agency 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.

''(II) For purposes of this clause, the term 'prisoner' means an individual confined in a jail, prison, or other penal institution or correctional facility pursuant to conviction of such individual of a criminal offense.''.

(2) EFFECTIVE DATE.—The amendment made under paragraph (1) shall apply with respect to employment of prisoners, or entry into contract with prisoners, after the date that is 1 year after the date of enactment of this Act.

SEC. 505. STUDY AND REPORT.

(a) BY THE COMPTROLLER GENERAL.—The Comptroller General of the United States (in this section referred to as the ''Comptroller General'') shall conduct a study and prepare a report on—

(1) all of the uses of social security numbers permitted, required, authorized, or excepted under any Federal law; and

(2) the uses of social security numbers in Federal, State, and local public records.

(b) CONTENT OF REPORT.—The report required under subsection (a) shall—

(1) identify users of social security numbers under Federal law;

(2) include a detailed description of the uses allowed as of the date of enactment of this Act;

(3) describe the impact of such uses on privacy and data security;

(4) evaluate whether such uses should be continued or discontinued by appropriate legislative action;

(5) examine whether States are complying with prohibitions on the display and use of social security numbers—

(A) under the Privacy Act of 1974 (5 U.S.C. 552a et seq.); and

(B) the Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et seq.);

(6) include a review of the uses of social security numbers in Federal, State, or local public records;

(7) include a review of the manner in which public records are stored (with separate reviews for both paper records and electronic records);

(8) include a review of the advantages, utility, and disadvantages of public records that contain social security numbers, including—

(A) impact on law enforcement;

(B) threats to homeland security; and

(C) impact on personal privacy and security;

(9) include an assessment of the costs and benefits to State and local governments of truncating,

redacting, or removing social security numbers from public records, including a review of current technologies and procedures for truncating, redacting, or removing social security numbers from public records (with separate assessments for both paper and electronic records);

(10) include an assessment of the benefits and costs to businesses, non-profit organizations, and the general public of requiring truncation, redaction, or removal of social security numbers on public records (with separate assessments for both paper and electronic records);

(11) include an assessment of Federal and State requirements to truncate social security numbers, and issue recommendations on—

(A) how to harmonize those requirements; and

(B) whether to further extend truncation requirements, taking into consideration the impact on accuracy and use;

(12) include recommendations regarding whether subsection (a) should apply to any record or category of public records first posted on the Internet or provided in an electronic medium by, or on behalf

of, a Federal agency prior to the date of enactment of this Act; and

(13) include such recommendations for legislation based on criteria the Comptroller General determines to be appropriate.

(c) REQUIRED CONSULTATION.—In developing the report required under this subsection, the Comptroller General shall consult with—

(1) the Administrative Office of the United States Courts;

(2) the Conference of State Court Administrators;

(3) the Department of Justice;

(4) the Department of Homeland Security;

(5) the Social Security Administration;

(6) Sate and local governments that store, maintain, or disseminate public records; and

(7) other stakeholders, including members of the private sector who routinely use public records that contain social security numbers.

(d) TIMING OF REPORT.—Not later than 1 year after the date of enactment of this Act, the Comptroller General shall report to Congress its findings under this section.

SEC. 506. ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) IN GENERAL.—Any person that violates the provisions of sections 501 or 502 shall be subject to civil penalties of not more than $5,000 per violation per day, with a maximum of $35,000 per day, while such violations persist.

(2) INTENTIONAL OR WILLFUL VIOLATION.—Any person who intentionally or willfully violates the provisions of sections 501 or 502 shall be subject to additional penalties in the amount of $5,000 per violation per day, with a maximum of an additional $35,000 per day, while such violations persist.

(3) EQUITABLE RELIEF.—Any person who engages in interstate commerce that violates this section may be enjoined from further violations by a court of competent jurisdiction.

(4) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this section are cumulative and shall not affect any other rights and remedies available under law

(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—Whenever it appears that a person to which this title applies has engaged, is engaged, or is about to engage, in any act or practice constituting a violation of this title, the Attorney

General may bring a civil action in an appropriate district court of the United States to—

(A) enjoin such act or practice;

(B) enforce compliance with this title; and

(C) obtain damages—

(i) in the sum of actual damages, restitution, and other compensation on behalf of the affected residents of a State; and

(ii) punitive damages, if the violation is willful or intentional; and

(D) obtain such other relief as the court determines to be appropriate.

(2) OTHER INJUNCTIVE RELIEF.—Upon a proper showing in the action under paragraph (1), the court shall grant a permanent injunction or a temporary restraining order without bond.

(c) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—In any case in which the attorney general 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 an act or practice that violates this section, the State may bring a civil action on behalf of the residents of that State in a district court of the United States of ap-

propriate jurisdiction, or any other court of competent jurisdiction, to—

(A) enjoin that act or practice;

(B) enforce compliance with this Act;

(C) obtain damages, restitution, or other compensation on behalf of residents of that State; or

(D) obtain such other legal and equitable relief as the court may consider to be appropriate.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under this subsection, the attorney general of the State involved shall provide to the Attorney General—

(i) a written notice of that action; and

(ii) a copy of the complaint for that action.

(B) EXCEPTION.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general of a State determines that it is not feasible to provide the notice described in this subparagraph before the filing of the action.

(C) NOTIFICATION WHEN PRACTICABLE.—In an action described under subparagraph (B), the attorney general of a State shall provide the written notice and the copy of the complaint to the Attorney General as soon after the filing of the complaint as practicable.

(3) ATTORNEY GENERAL AUTHORITY.—Upon receiving notice under paragraph (2), the Attorney General shall have the right to—

(A) move to stay the action, pending the final disposition of a pending Federal proceeding or action as described in paragraph (4);

(B) intervene in an action brought under paragraph (1); and

(C) file petitions for appeal.

(4) PENDING PROCEEDINGS.—If the Attorney General has instituted a proceeding or action for a violation of this Act or any regulations thereunder, no attorney general of a State may, during the pendency of such proceeding or action, bring an action under this subsection against any defendant named in such criminal proceeding or civil action for any violation that is alleged in that proceeding or action.

(5) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), noth-

ing 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 and affirmations;

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

(6) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under this subsection may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under this subsection process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

SEC. 507. RELATION TO STATE LAWS.

(a) IN GENERAL.—Except as provided in subsection (b), this title does not annul, alter, affect, or exempt any person subject to the provisions of this title from complying with the laws of any State with respect to pro-

tecting and securing social security numbers, except to the extent that those laws are inconsistent with any provisions of this title, and then only to the extent of such inconsistency.

(b) EXCEPTIONS.—No requirement or prohibition may be imposed under the laws of any State with respect to any subject matter regulated under—

(1) section 501(b), relating to prerequisites for consent for the display, sale, or purchase of social security numbers;

(2) section 501(c), relating to harvesting of social security numbers; and

(3) section 504, relating to treatment of social security numbers on government checks and prohibition of inmate access.

TITLE VI—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL DATA

SEC. 601. GENERAL SERVICES ADMINISTRATION REVIEW OF CONTRACTS.

(a) IN GENERAL.—In considering contract awards entered into after the date of enactment of this Act, the Administrator of the General Services Administration shall evaluate—

(1) the program of a contractor to ensure the privacy and security of data containing personally identifiable information;

(2) the compliance of a contractor with such program;

(3) the extent to which the databases and systems containing personally identifiable information of a contractor have been compromised by security breaches; and

(4) the response by a contractor to such breaches, including the efforts of a contractor to mitigate the impact of such breaches.

(b) PENALTIES.—In awarding contracts for products or services related to access, use, compilation, distribution, processing, analyzing, or evaluating personally identifiable information, the Administrator of the General Services Administration shall include the following:

(1) Monetary or other penalties—

(A) for failure to comply with subtitles A and B of title IV of this Act;

(B) if a contractor knows or has reason to know that the personally identifiable information being provided is inaccurate, and provides such inaccurate information; or

(C) if a contractor is notified by an individual that the personally identifiable information being provided is inaccurate and it is in fact inaccurate.

(2) Accuracy update requirements that obligate a contractor to provide notice to the Federal department or agency of any changes or corrections to the personally identifiable information provided under the contract.

SEC. 602. REQUIREMENT TO AUDIT INFORMATION SECURITY PRACTICES OF CONTRACTORS AND THIRD PARTY BUSINESS ENTITIES.

Section 3544(b) of title 44, United States Code, is amended—

(1) in paragraph (7)(C)(iii), by striking ''and'' after the semicolon;

(2) in paragraph (8), by striking the period and inserting ''; and''; and

(3) by adding at the end the following:

''(9) procedures for evaluating and auditing the information security practices of contractors or third party business entities supporting the information systems or operations of the agency involving personally identifiable information, and ensuring remedial action to address any significant deficiencies.''.

SEC. 603. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT USE OF COMMERCIAL INFORMATION SERVICES CONTAINING PERSONALLY IDENTIFIABLE INFORMATION.

(a) IN GENERAL.—Section 208(b)(1) of the E-Government Act of 2002 (44 U.S.C. 3501 note) is amended—

(1) in subparagraph (A)(i), by striking ''or''; and

(2) in subparagraph (A)(ii), by striking the period and inserting ''; or''; and

(3) by inserting after clause (ii) the following:

''(iii) purchasing or subscribing for a fee to personally identifiable information from a commercial entity (other than news reporting or telephone directories).''.

(b) LIMITATION.—Notwithstanding any other provision of law, commencing 60 days after the date of enactment of this Act, no Federal department or agency may procure or access any commercially available database consisting primarily of personally identifiable information concerning United States persons (other than news reporting or telephone directories) unless the head of such department or agency—

(1) completes a privacy impact assessment under section 208 of the E-Government Act of 2002

(44 U.S.C. 3501 note), which shall include a description of—

(A) such database;

(B) the name of the commercial entity from whom it is obtained; and

(C) the amount of the contract for use;

(2) adopts regulations that specify—

(A) the personnel permitted to access, analyze, or otherwise use such databases;

(B) standards governing the access analysis, or use of such databases;

(C) any standards used to ensure that the personally identifiable information accessed, analyzed, or used is the minimum necessary to accomplish the intended legitimate purpose of the Federal department or agency;

(D) standards limiting the retention and redisclosure of personally identifiable information obtained from such databases;

(E) procedures ensuring that such data meet standards of accuracy, relevance, completeness, and timeliness;

(F) the auditing and security measures to protect against unauthorized access, analysis, use, or modification of data in such databases;

(G) applicable mechanisms by which individuals may secure timely redress for any adverse consequences wrongly incurred due to the access, analysis, or use of such databases;

(H) mechanisms, if any, for the enforcement and independent oversight of existing or planned procedures, policies, or guidelines; and

(I) an outline of enforcement mechanisms for accountability to protect individuals and the public against unlawful or illegitimate access or use of databases; and

(3) incorporates into the contract or other agreement with the commercial entity, provisions—

(A) providing for penalties—

(i) if the entity knows or has reason to know that the personally identifiable information being provided to the Federal department or agency is inaccurate, and provides such inaccurate information; or

(ii) if the entity is notified by an individual that the personally identifiable information being provided to the Federal department or agency is inaccurate and it is in fact inaccurate; and

(B) requiring commercial entities to inform Federal departments or agencies to which they sell, disclose, or provide access to personally identifiable information of any changes or corrections to the personally identifiable information.

(c) INDIVIDUAL SCREENING PROGRAMS.—Notwithstanding any other provision of law, commencing 60 days after the date of enactment of this Act, no Federal department or agency may use commercial databases to implement an individual screening program unless such program is—

(1) congressionally authorized; and

(2) subject to regulations developed by notice and comment that—

(A) establish a procedure to enable individuals, who suffer an adverse consequence because the screening system determined that they might pose a security threat, to appeal such determination and correct information contained in the system;

(B) ensure that Federal and commercial databases that will be used to establish the identity of individuals or otherwise make assessments of individuals under the system will not

produce a large number of false positives or unjustified adverse consequences;

(C) ensure the efficacy and accuracy of all of the search tools that will be used and ensure that the department or agency can make an accurate predictive assessment of those who may constitute a threat;

(D) establish an internal oversight board to oversee and monitor the manner in which the system is being implemented;

(E) establish sufficient operational safeguards to reduce the opportunities for abuse;

(F) implement substantial security measures to protect the system from unauthorized access;

(G) adopt policies establishing the effective oversight of the use and operation of the system; and

(H) ensure that there are no specific privacy concerns with the technological architecture of the system.

(d) STUDY OF GOVERNMENT USE.—

(1) SCOPE OF STUDY.—Not later than 180 days after the date of enactment of this Act, the Comptroller General of the United States shall con-

duct a study and audit and prepare a report on Federal agency use of commercial databases, including the impact on privacy and security, and the extent to which Federal contracts include sufficient provisions to ensure privacy and security protections, and penalties for failures in privacy and security practices.

(2) REPORT.—A copy of the report required under paragraph (1) shall be submitted to Congress.

SEC. 604. IMPLEMENTATION OF CHIEF PRIVACY OFFICER REQUIREMENTS.

(a) DESIGNATION OF THE CHIEF PRIVACY OFFICER.—Pursuant to the requirements under section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (Division H of Public Law 108–447; 118 Stat. 3199) that each agency designate a Chief Privacy Officer, the Department of Justice shall implement such requirements by designating a department-wide Chief Privacy Officer, whose primary role shall be to fulfill the duties and responsibilities of Chief Privacy Officer and who shall report directly to the Deputy Attorney General.

(b) DUTIES AND RESPONSIBILITIES OF CHIEF PRIVACY OFFICER.—In addition to the duties and responsibilities outlined under section 522 of the Transportation,

Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (Division H of Public Law 108–447; 118 Stat. 3199), the Department of Justice Chief Privacy Officer shall—

(1) oversee the Department of Justice's implementation of the requirements under section 603 to conduct privacy impact assessments of the use of commercial data containing personally identifiable information by the Department;

(2) promote the use of law enforcement technologies that sustain, rather than erode, privacy protections, and assure that the implementation of such technologies relating to the use, collection, and disclosure of personally identifiable information preserve the privacy and security of such information; and

(3) coordinate with the Privacy and Civil Liberties Oversight Board, established in the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458), in implementing paragraphs (1) and (2) of this subsection.