Calendar No. 182

112TH CONGRESS
1ST SESSION

S. 1535

To protect consumers by mitigating the vulnerability of personally identifiable information to theft through a security breach, providing notice and remedies to consumers in the wake of such a breach, holding companies accountable for preventable breaches, facilitating the sharing of post-breach technical information between companies, and enhancing criminal and civil penalties and other protections against the unauthorized collection or use of personally identifiable information.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 8, 2011

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

SEPTEMBER 22, 2011

Reported by Mr. LEAHY, with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

A BILL

To protect consumers by mitigating the vulnerability of personally identifiable information to theft through a security breach, providing notice and remedies to consumers in the wake of such a breach, holding companies accountable for preventable breaches, facilitating the sharing of post-breach technical information between companies, and enhancing criminal and civil penalties and other

protections against the unauthorized collection or use 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 Protection and Breach Accountability Act of 2011''.

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

SEC. 2. FINDINGS.

Congress finds that—

(1) databases of personally 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 confidentiality 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 ensure 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;

(11) because government use of commercial data containing personal information potentially affects individual privacy, and law enforcement and national security operations, there is a need for Congress to exercise oversight over government use of commercial data;

(12) over 22,960,000 cases of data breaches involving personally identifiable information were reported through July of 2011, and in 2009 through 2010, over 230,900,000 cases of personal data breaches were reported;

(13) facilitating information sharing among business entities and across sectors in the event of a breach can assist in remediating the breach and preventing similar breaches in the future;

(14) because the Federal Government has limited resources, consumers themselves play a vital and complementary role in facilitating prompt notification and protecting against future breaches of security;

(15) in addition to the immediate damages caused by security breaches, the lack of basic remedial requirements often forces individuals whose sensitive personally identifiable information is compromised as a result of a security breach to incur the economic costs of litigation to seek remedies, and the economic costs of fees required in many States to freeze compromised accounts; and

(16) victims of personal data breaches may suffer debilitating emotional and physical effects and become depressed or anxious, especially in cases of repeated or unresolved instances of data breaches.

SEC. 3. DEFINITIONS.

In this Act, the following definitions shall apply:

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

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

(3) BUSINESS ENTITY.—The term ''business entity'' means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture established to make a profit, or nonprofit.

(4) CREDIT RATING AGENCY.—The term ''credit rating agency'' has the meaning given such term in section 3(a)(61) of the Securities Exchange Act of 1934 (12 U.S.C. 78c(a)(61)).

(5) CREDIT REPORT.—The term ''credit report'' means a consumer report, as that term is defined in section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a).

(6) DATA BROKER.—The term ''data broker'' means a business entity which for monetary fees or dues regularly engages in the practice of collecting, transmitting, or providing access to sensitive personally identifiable information on more than 5,000 individuals who are not the customers or employees of that business entity or affiliate primarily for the purposes of providing such information to nonaffiliated third parties on an interstate basis.

(7) DATA FURNISHER.—The term ''data furnisher'' means any agency, organization, corporation, trust, partnership, sole proprietorship, unincor-

porated association, or nonprofit that serves as a source of information for a data broker.

(8) ENCRYPTION.—The term ''encryption''—

(A) means the protection of data in electronic form, in storage or in transit, using an encryption technology that has been adopted by a widely accepted standards setting body or, has been widely accepted as an effective industry practice which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and

(B) includes appropriate management and safeguards of such cryptographic keys so as to protect the integrity of the encryption.

(9) IDENTITY THEFT.—The term ''identity theft'' means a violation of section 1028(a)(7) of title 18, United States Code.

(10) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' includes the following:

(A) The Office of the Director of National Intelligence.

(B) The Central Intelligence Agency.

(C) The National Security Agency.

(D) The Defense Intelligence Agency.

(E) The National Geospatial-Intelligence Agency.

(F) The National Reconnaissance Office.

(G) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs.

(H) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, and the Department of Energy.

(I) The Bureau of Intelligence and Research of the Department of State.

(J) The Office of Intelligence and Analysis of the Department of the Treasury.

(K) The elements of the Department of Homeland Security concerned with the analysis of intelligence information, including the Office of Intelligence of the Coast Guard.

(L) Such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

(11) PERSONAL ELECTRONIC RECORD.—

(A) IN GENERAL.—The term ''personal electronic record'' means data associated with an individual contained in a database, networked or integrated databases, or other data system that is provided by a data broker to nonaffiliated third parties and includes personally identifiable information about that individual.

(B) EXCLUSIONS.—The term ''personal electronic record'' does not include—

(i) any data related to an individual's past purchases of consumer goods; or

(ii) any proprietary assessment or evaluation of an individual or any proprietary assessment or evaluation of information about an individual.

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

(13) PREDISPUTE ARBITRATION AGREEMENT.—The term ''predispute arbitration agreement'' means any agreement to arbitrate a dispute that had not

yet arisen at the time of the making of the agreement.

(14) PUBLIC RECORD SOURCE.—The term ''public record source'' means the Congress, any agency, any State or local government agency, the government of the District of Columbia and governments of the territories or possessions of the United States, and Federal, State or local courts, courts martial and military commissions, that maintain personally identifiable information in records available to the public.

(15) SECURITY BREACH.—

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

(i) that result in, or that there is a reasonable basis to conclude has resulted in—

(I) the unauthorized acquisition of sensitive personally identifiable information; or

(II) access to sensitive personally identifiable information that is for an

unauthorized purpose, or in excess of authorization; and

(ii) which present a significant risk of harm or fraud to any individual.

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

(i) a good faith acquisition of sensitive personally identifiable information by a business entity or agency, or an employee or agent of a business entity or agency, if the sensitive personally identifiable information is not subject to further unauthorized disclosure;

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

(iii) any lawfully authorized criminal investigation or authorized investigative, protective, or intelligence activities that are carried out by or on behalf of any element of the intelligence community and conducted in accordance with the United States laws, authorities, and regulations governing such intelligence activities.

(16) SECURITY FREEZE.—The term ''security freeze'' means a notice, at the request of the consumer and subject to exceptions in section 215(b), that prohibits the consumer reporting agency from releasing all or any part of the consumer's credit report or any information derived from it without the express authorization of the consumer.

(17) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term ''sensitive personally identifiable information'' means any information or compilation of information, in electronic or digital form that includes—

(A) an individual's first and last name or first initial and last name in combination with any 1 of the following data elements:

(i) A nontruncated social security number, driver's license number, passport number, or alien registration number.

(ii) Any 2 of the following:

(I) Home address.

(II) Telephone number.

(III) Mother's maiden name.

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

(iii) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation.

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

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

(C) any other combination of data elements that could allow unauthorized access to or acquisition of the information described in subparagraph (A) or (B), including—

(i) a unique account identifier;

(ii) an electronic identification number;

(iii) a user name;

(iv) a routing code; or

(v) any associated security code, access code, or password or any associated security questions and answers that could allow unauthorized access to the account.

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

SEC. 101. 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 (relating to fraud and related activity in connection with computers) if the act is a felony,'' before ''section 1084''.

SEC. 102. CONCEALMENT OF SECURITY BREACHES INVOLVING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.

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

"§ 1041. Concealment of security breaches involving sensitive personally identifiable information

''(a) Whoever, having knowledge of a security breach and having the obligation to provide notice of such breach to individuals under the Personal Data Protection and Breach Accountability Act of 2011, and having not otherwise qualified for an exemption from providing notice under section 212 of the Personal Data Protection and Breach Accountability Act of 2011, intentionally or willfully conceals the fact of such security breach and which breach causes economic damage or substantial emotional distress to 1 or more persons, shall be fined under this title or imprisoned not more than 5 years, or both.

''(b) For purposes of subsection (a), the term 'person' has the same meaning as in section 1030(e)(12) of title 18, United States Code.

''(c) Any person seeking an exemption under section 212(b) of the Personal Data Protection and Breach Accountability Act of 2011 shall be immune from prosecution under this section if the United States Secret Service does not indicate, in writing, that such notice be given under section 212(b)(3) of the Personal Data Protection and Breach Accountability Act of 2011.''.

(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:

"1041. Concealment of security breaches involving personally identifiable information.".

(c) ENFORCEMENT AUTHORITY.—

(1) IN GENERAL.—The United States Secret Service shall have the authority to investigate offenses under this section.

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

SEC. 103. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

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

(1) by inserting "or conspiracy" after "or an attempt" each place it appears, except for paragraph (4);

(2) in paragraph (2)(B)—

(A) in clause (i), by inserting ", or attempt or conspiracy or conspiracy to commit an offense," after "the offense";

(B) in clause (ii), by inserting ", or attempt or conspiracy or conspiracy to commit an offense," after "the offense"; and

(C) in clause (iii), by inserting "(or, in the case of an attempted offense, would, if completed, have obtained)" after "information obtained"; and

(3) in paragraph (4)—

(A) in subparagraph (A)—

(i) by striking clause (ii);

(ii) by striking "in the case of—" and all that follows through "an offense under subsection (a)(5)(B)" and inserting "in the case of an offense, or an attempt or conspiracy to commit an offense, under subsection (a)(5)(B)";

(iii) by inserting "or conspiracy" after "if the offense";

(iv) by redesignating subclauses (I) through (VI) as clauses (i) through (vi), respectively, and adjusting the margin accordingly; and

(v) in clause (vi), as so redesignated, by striking "; or" and inserting a semicolon;

(B) in subparagraph (B)—

(i) by striking clause (ii);

(ii) by striking ''in the case of—'' and all that follows through ''an offense under subsection (a)(5)(A)'' and inserting ''in the case of an offense, or an attempt or conspiracy to commit an offense, under subsection (a)(5)(A)'';

(iii) by inserting ''or conspiracy'' after ''if the offense''; and

(iv) by striking ''; or'' and inserting a semicolon;

(C) in subparagraph (C)—

(i) by striking clause (ii);

(ii) by striking ''in the case of—'' and all that follows through ''an offense or an attempt to commit an offense'' and inserting ''in the case of an offense, or an attempt or conspiracy to commit an offense,''; and

(iii) by striking ''; or'' and inserting a semicolon;

(D) in subparagraph (D)—

(i) by striking clause (ii);

(ii) by striking ''in the case of—'' and all that follows through ''an offense or an attempt to commit an offense'' and insert-

ing ''in the case of an offense, or an attempt or conspiracy to commit an offense,''; and

(iii) by striking ''; or'' and inserting a semicolon;

(E) in subparagraph (E), by inserting ''or conspires'' after ''offender attempts'';

(F) in subparagraph (F), by inserting ''or conspires'' after ''offender attempts''; and

(G) in subparagraph (G)(ii), by inserting ''or conspiracy'' after ''an attempt''.

SEC. 104. FALSE NOTIFICATION.

(a) IN GENERAL.—It shall be unlawful for an individual to send a notification of a breach of security that is false or intentionally misleading in order to obtain sensitive personally identifiable information in an effort to defraud an individual.

(b) PENALTY.—Any person that violates subsection (a) shall be fined not more than $1,000,000, imprisoned not more than 5 years, or both.

(c) RULE OF CONSTRUCTION.—For purposes of this section, any single action or conduct that violates subsection (a) with respect to multiple protected computers shall be construed to be a single violation.

SEC. 105. UNAUTHORIZED INSTALLATION OF PERSONAL INFORMATION COLLECTION FEATURES ON A USER'S COMPUTER.

(a) DEFINITION.—In this section, the term ''protected computer'' has the meaning given the term in section 1030(e)(2) of title 18, United States Code.

(b) IN GENERAL.—It shall be unlawful for a person that is not an authorized user of a protected computer to cause the installation on the protected computer of software that collects sensitive personally identifiable information from an authorized user, unless the person—

(1) provides a clear and conspicuous disclosure of such collection; and

(2) obtains the consent of an authorized user of the protected computer prior to any collection of sensitive personally identifiable information.

(c) COLLECTION AND USE OF PERSONAL INFORMATION IN WEB SEARCHES.—It shall be unlawful for an Internet service provider or proxy server to knowingly or intentionally—

(1) bypass the display of search engine results and redirect web searches or queries entered by an authorized user of a protected computer directly to a commercial website, counterfeit web page, or targeted advertisement and derive an economic benefit from such activity; or

~~(2) monitor, manipulate, aggregate, and market the data collected in the process of intercepting a web search or query entered by an authorized user of a protected computer and derive an economic benefit from such activity.~~

~~(d) OTHER COLLECTION OF PERSONAL INFORMATION.—~~

~~(1) IN GENERAL.—It shall be unlawful for a person who is not an authorized user of a protected computer to cause the installation on the protected computer of software that engages in any of the collection practices described in paragraph (2), unless the person—~~

~~(A) provides a clear and conspicuous disclosure of such collection; and~~

~~(B) obtains the consent of an authorized user of the protected computer prior to any such collection of information.~~

~~(2) COLLECTION PRACTICES DESCRIBED.—The collection practices described in this paragraph are—~~

~~(A) the use of a keystroke-logging function that records all or substantially all keystrokes made by an owner or operator of a computer~~

and transfers that information from the computer to another person;

(B) the collection of data in a manner that—

(i) correlates sensitive personally identifiable information with a history of—

(I) all, or substantially all, of the websites visited by an owner or operator, other than websites operated by the person providing such software; or

(II) all, or substantially all, of the web searches conducted by an owner or operator other than search data collected by a search engine; and

(ii) uses the information described in clause (i) to deliver advertising to, or display advertising on, the computer; and

(C) the extracting from the hard drive or other storage medium of the computer—

(i) the substantive contents of files, data, software, or other information knowingly saved or installed by the authorized user of a protected computer; or

(ii) the substantive contents of communications sent by an authorized user of

a protected computer to any other computer.

(e) EXCEPTION.—This section shall not restrict a person from causing the installation of software that collects information for the provider of an online service or website knowingly used or subscribed to by an authorized user if the information collected is used only to affect the experience of the user while using that online service or website.

(f) UNINSTALL FUNCTIONALITY.—

(1) IN GENERAL.—Software that performs any function described in subsection (b) or (c) shall have the capability to subsequently be uninstalled or disabled by an authorized user through a program removal function that is usual and customary with the operating system of the computer or otherwise as clearly and conspicuously disclosed to the user.

(2) AUTHORITY TO UNINSTALL.—Software that enables an authorized user of a protected computer, such as a parent, employer, or system administrator, to choose to prevent another user of the same computer from uninstalling or disabling the software shall not be considered to prevent reasonable efforts to uninstall or disable the software within the meaning of paragraph (1) if not less than 1 authorized

user retains the ability to uninstall or disable the software.

(g) LIMITATIONS ON LIABILITY.—

(1) IN GENERAL.—The restrictions imposed under this section do not apply to any monitoring of, or interaction with, a subscriber's Internet or other network connection or service, or a protected computer, by or at the direction of a telecommunications carrier, cable operator, computer hardware or software provider, financial institution or provider of information services or interactive computer service for—

(A) network or computer security purposes;

(B) diagnostics;

(C) technical support;

(D) repair;

(E) network management;

(F) authorized updates of software or system firmware;

(G) authorized remote system management;

(H) authorized provision of protection for users of the computer from objectionable content;

(I) authorized scanning for computer software used in violation of this section for removal by an authorized user; or

(J) detection or prevention of the unauthorized use of software fraudulent or other illegal activities.

(2) MANUFACTURER'S LIABILITY FOR THIRD-PARTY SOFTWARE.—A manufacturer or retailer of a computer shall not be liable under any provision of this section for causing the installation on the computer, prior to the first retail sale and delivery of the computer, of third-party branded software, unless the manufacturer or retailer knowingly allows the installation of such third-party branded software and derives a benefit from the operation of such software.

(3) EXCEPTION FOR AUTHORIZED INVESTIGATIVE AGENCIES.—Nothing in this section prohibits any lawfully authorized criminal investigation or authorized investigative, protective, or intelligence activities that are carried out by or on behalf of any element of the intelligence community and conducted in accordance with the United States laws, authorities, and regulations governing such intelligence activities, of a law enforcement agency of the United

States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(h) ENFORCEMENT BY THE ATTORNEY GENERAL.—

(1) LIABILITY AND PENALTY FOR VIOLATIONS.—Any person who engages in an activity in violation of this section shall be fined not more than $500,000, imprisoned not more than 5 years, or both.

(2) ENHANCED LIABILITY AND PENALTIES FOR PATTERN OR PRACTICE OF VIOLATIONS.—

(A) IN GENERAL.—Any person who engages in a pattern or practice of activity that violates the provisions of this section shall be fined not more than $1,000,000, imprisoned not more than 5 years, or both.

(B) TREATMENT OF SINGLE ACTION OR CONDUCT.—For purposes of subparagraph (A), any single action or conduct that violates this section with respect to multiple protected computers shall be construed as a single violation.

(3) CONSIDERATIONS.—In determining the amount of any penalty under paragraph (1) or (2), the court shall take into account—

(A) the degree of culpability of the defendant;

(B) any history of prior such conduct;

(C) the ability of the defendant to pay any fine imposed;

(D) the effect on the ability of the defendant to continue to do business; and

(E) such other matters as justice may require.

TITLE II—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

Subtitle A—A Data Privacy and Security Program

SEC. 201. 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 security of sensitive personally identifiable information.

(b) IN GENERAL.—A business entity engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive 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 pro-

gram under section 202 for protecting sensitive personally identifiable information.

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

(1) FINANCIAL INSTITUTIONS.—Financial institutions—

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

(B) subject to—

(i) examinations for compliance with the requirements of this Act by a Federal Functional Regulator or State Insurance Authority (as those terms are defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809)); or

(ii) compliance with part 314 of title 16, Code of Federal Regulations.

(2) HIPAA REGULATED ENTITIES.—

(A) COVERED ENTITIES.—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.

(B) BUSINESS ENTITIES.—A business entity shall be deemed in compliance with this Act if the business entity—

(i) is acting as a business associate, as that term is defined under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.) and is in compliance with the requirements imposed under that Act and implementing regulations promulgated under that Act; and

(ii) is subject to, and currently in compliance, with the privacy and data security requirements under sections 13401 and 13404 of division A of the American Reinvestment and Recovery Act of 2009 (42 U.S.C. 17931 and 17934) and implementing regulations promulgated under such sections.

(3) PUBLIC RECORDS.—Public records not otherwise subject to a confidentiality or nondisclosure requirement, or information obtained from a news report or periodical.

(d) RULE OF CONSTRUCTION.—Nothing in this subtitle shall be construed to modify, limit, or supersede the

operation of the provisions of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), or its implementing regulations, including such regulations adopted or enforced by the States.

SEC. 202. REQUIREMENTS FOR A PERSONAL DATA PRIVACY AND SECURITY PROGRAM.

(a) PERSONAL DATA PRIVACY AND SECURITY PROGRAM.—A business entity subject to this subtitle shall comply with the following safeguards and any other administrative, technical, or physical safeguards identified by the Federal Trade Commission in a rulemaking process pursuant to section 553 of title 5, United States Code, for the protection of sensitive personally identifiable information:

(1) SCOPE.—A business entity shall implement a comprehensive personal data privacy and security program 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 sensitive personally identifiable information;

~~(B) protect against any anticipated vulnerabilities to the privacy, security, or integrity of sensitive personally identifiable information; and~~

~~(C) protect against unauthorized access or use of sensitive personally identifiable information that could create a significant risk of harm or fraud 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 alteration of sensitive personally identifiable information or systems containing sensitive personally identifiable information;~~

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

~~(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 sensitive personally identifiable information; and~~

(D) assess the vulnerability of sensitive personally identifiable information during destruction and disposal of such information, including through the disposal or retirement of hardware.

(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 sensitive personally identifiable information, including controls to authenticate and permit access only to authorized individuals;

(ii) detect, record, and preserve information relevant to actual and attempted fraudulent, unlawful, or unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information,

including by employees and other individuals otherwise authorized to have access;

(iii) protect sensitive personally identifiable information during use, transmission, storage, and disposal by encryption, redaction, or access controls that are widely accepted as an effective industry practice or industry standard, 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);

(iv) ensure that sensitive personally identifiable information is properly destroyed and disposed of, including during the destruction of computers, diskettes, and other electronic media that contain sensitive personally identifiable information;

(v) trace access to records containing sensitive personally identifiable information so that the business entity can determine

who accessed or acquired such sensitive personally identifiable information pertaining to specific individuals;

(vi) ensure that no third party or customer of the business entity is authorized to access or acquire sensitive personally identifiable information without the business entity first performing sufficient due diligence to ascertain, with reasonable certainty, that such information is being sought for a valid legal purpose; and

(vii) minimize the amount of personal information maintained by the business entity, providing for the retention of such personal information only as reasonably needed for the business purposes of the business entity or as necessary to comply with any other provision of law.

(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 sensitive 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 sensitive 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 section 201, this section, and subtitle B.

(c) 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 sensitive personally identifiable information systems.

(f) IMPLEMENTATION TIMELINE.—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. 203. FEDERAL ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) IN GENERAL.—The Attorney General may bring a civil action in the appropriate United States district court against any business entity that engages in conduct constituting a violation of this subtitle and, upon proof of such conduct by a preponderance of the evidence, such business entity shall be subject to a civil penalty of not more than $5,000 per violation per day while such a violation exists, with a maximum of $20,000,000 per violation, unless such conduct is found to be willful or intentional.

(2) INTENTIONAL OR WILLFUL VIOLATION.—A business entity that intentionally or willfully violates the provisions of this subtitle shall be subject to additional penalties in the amount of $5,000 per violation per day while such a violation exists.

(3) CONSIDERATIONS.—In determining the amount of a civil penalty under this subsection, the court shall take into account—

(A) the degree of culpability of the business entity;

(B) any prior violations of this subtitle by the business entity;

(C) the ability of the business entity to pay a civil penalty;

(D) the effect on the ability of the business entity to continue to do business;

(E) the number of individuals whose personally identifiable information was compromised by the breach;

(F) the relative cost of compliance with this subtitle; and

(G) such other matters as justice may require.

(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—If it appears that a business entity has engaged, or is engaged, in any act or practice constituting a violation of this subtitle, the Attorney General may petition an appropriate district court of the United States for an order—

(A) enjoining such act or practice; or

(B) enforcing compliance with this subtitle.

(2) ISSUANCE OF ORDER.—A court may issue an order under paragraph (1), if the court finds that the conduct in question constitutes a violation of this subtitle.

(c) 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.

SEC. 204. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) CIVIL ACTIONS.—

(1) IN GENERAL.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the acts or practices of a business entity that violate 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; or

(C) obtain civil penalties of not more than $5,000 per violation per day while such violations persist, up to a maximum of $20,000,000 per violation.

(2) CONSIDERATIONS.—In determining the amount of a civil penalty under this subsection, the court shall take into account—

(A) the degree of culpability of the business entity;

(B) any prior violations of this subtitle by the business entity;

(C) the ability of the business entity to pay a civil penalty;

(D) the effect on the ability of the business entity to continue to do business;

(E) the number of individuals whose personally identifiable information was compromised by the breach;

(F) the relative cost of compliance with this subtitle; and

(G) such other matters as justice may require.

(3) 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) EXEMPTION.—

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

(ii) NOTIFICATION.—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 State attorney general files the action.

(b) FEDERAL PROCEEDINGS.—Upon receiving notice under subsection (a)(2), the Attorney General shall have the right to—

(1) move to stay the action, pending the final disposition of a pending Federal proceeding or action;

(2) initiate an action in the appropriate United States district court under section 217 and move to

consolidate all pending actions, including State actions, in such court;

(3) intervene in an action brought under subsection (a)(2); and

(4) file petitions for appeal.

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

(d) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this subtitle regarding notification 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—

(1) conduct investigations;

(2) administer oaths or affirmations; or

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

(e) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in—

(A) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(B) another court of competent jurisdiction.

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

(A) is an inhabitant; or

(B) may be found.

SEC. 205. SUPPLEMENTAL ENFORCEMENT BY INDIVIDUALS.

(a) IN GENERAL.—Any person aggrieved by a violation of the provisions of this subtitle by a business entity may bring a civil action in a court of appropriate jurisdiction to recover for personal injuries sustained as a result of the violation.

(b) AUTHORITY TO BRING CIVIL ACTION; JURISDICTION.—As provided in subsection (c), any person may commence a civil action on his own behalf against any business entity who is alleged to have violated the provisions of this subtitle.

(c) REMEDIES IN A CITIZEN SUIT.—

(1) DAMAGES.—Any individual harmed by a failure of a business entity to comply with the provisions of this subtitle, shall be able to collect damages of not more than $10,000 per violation per day while such violations persist, up to a maximum of $20,000,000 per violation.

(2) PUNITIVE DAMAGES.—A business entity may be liable for punitive damages if the business entity intentionally or willfully violates the provisions of this subtitle.

(3) EQUITABLE RELIEF.—A business entity that violates the provisions of this subtitle may be enjoined to comply with the provisions of those sections.

(d) 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.

(e) ACCESS TO JUSTICE.—The rights and remedies afforded by this section shall not be abridged or precluded by any predispute arbitration agreement, and any claims under this section that arise from the same security breach are presumed to meet the commonality requirement under rule 23(a)(2) of the Federal Rules of Civil Procedure.

Subtitle B—Security Breach Notification

SEC. 211. NOTICE TO INDIVIDUALS.

(a) IN GENERAL.—Any agency, or business entity engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of or collects sensitive personally identifiable information that experiences a security breach of such information, shall, following the discovery of such security breach of such information, notify any resident of the United States whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed, or acquired.

(b) OBLIGATION OF OWNER OR LICENSEE.—

(1) NOTICE TO OWNER OR LICENSEE.—Any agency, or business entity engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information that the agency or business entity does not own or license shall notify the owner or licensee of the information following the discovery of a security breach involving such information.

(2) NOTICE BY OWNER, LICENSEE OR OTHER DESIGNATED THIRD PARTY.—Nothing in this subtitle shall prevent or abrogate an agreement between an agency or business entity required to give notice

under this section and a designated third party, including an owner or licensee of the sensitive personally identifiable information subject to the security breach, to provide the notifications required under subsection (a).

(3) BUSINESS ENTITY RELIEVED FROM GIVING NOTICE.—A business entity obligated to give notice under subsection (a) shall be relieved of such obligation if an owner or licensee of the sensitive personally identifiable information subject to the security breach, or other designated third party, provides such notification.

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—All notifications required under this section shall be made without unreasonable delay following the discovery by the agency or business entity of a security breach.

(2) REASONABLE DELAY.—Reasonable delay under this subsection may include any time necessary to determine the scope of the security breach, conduct the risk assessment described in section 212(b)(1), and provide notice to law enforcement when required.

(3) BURDEN OF PRODUCTION.—The agency, business entity, owner, or licensee required to pro-

vide notice under this subtitle shall, upon the request of the Attorney General or the attorney general of a State or any State or local law enforcement agency authorized by the attorney general of the State or by State statute to prosecute violations of consumer protection law, provide records or other evidence of the notifications required under this subtitle, including to the extent applicable, the reasons for any delay of notification.

(d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT PURPOSES.—

(1) IN GENERAL.—If a Federal law enforcement agency or member of the intelligence community determines that the notification required under this section would impede any lawfully authorized criminal investigation or authorized investigative, protective, or intelligence activities that are carried out by or on behalf of any element of the intelligence community and conducted in accordance with the United States laws, authorities, and regulations governing such intelligence activities, such notification shall be delayed upon written notice from such Federal law enforcement or intelligence agency to the agency or business entity that experienced the breach.

(2) EXTENDED DELAY OF NOTIFICATION.—If the notification required under subsection (a) is delayed pursuant to paragraph (1), an agency or business entity shall give notice 30 days after the day such law enforcement delay was invoked unless a Federal law enforcement or intelligence agency provides written notification that further delay is necessary.

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

SEC. 212. EXEMPTIONS FROM NOTICE TO INDIVIDUALS.

(a) EXEMPTION FOR NATIONAL SECURITY AND LAW ENFORCEMENT.—

(1) IN GENERAL.—Section 211 shall not apply to an agency or business entity if the agency or business entity certifies, in writing, that notification of the security breach as required by section 211 reasonably could be expected to—

(A) cause damage to the national security; or

(B) hinder a law enforcement investigation or the ability of the agency to conduct law enforcement investigations.

(2) LIMITS ON CERTIFICATIONS.—An agency or business entity may not execute a certification under paragraph (1) to—

(A) conceal violations of law, inefficiency, or administrative error;

(B) prevent embarrassment to a business entity, organization, or agency;

(C) restrain competition; or

(D) delay notification under section 211 for any other reason, except where the agency or business entity reasonably believes an exemption under paragraph (1) applies.

(3) NOTICE.—In every case in which an agency or business agency issues a certification under paragraph (1), the certification, accompanied by a description of the factual basis for the certification, shall be immediately provided to the United States Secret Service and the Federal Bureau of Investigation.

(4) SECRET SERVICE AND FBI REVIEW OF CERTIFICATIONS.—

(A) IN GENERAL.—The United States Secret Service or the Federal Bureau of Investigation may review a certification provided by an agency under paragraph (3), and shall review a certification provided by a business entity under paragraph (3), to determine whether an exemption under paragraph (1) is merited. Such review shall be completed not later than 7 business days after the date of receipt of the certification, except as provided in paragraph (5)(C).

(B) NOTICE.—Upon completing a review under subparagraph (A) the United States Secret Service or the Federal Bureau of Investigation shall immediately notify the agency or business entity, in writing, of its determination of whether an exemption under paragraph (1) is merited.

(C) EXEMPTION.—The exemption under paragraph (1) shall not apply if the United States Secret Service or the Federal Bureau of Investigation determines under this paragraph that the exemption is not merited.

(5) ADDITIONAL AUTHORITY OF THE SECRET SERVICE AND FBI.—

(A) IN GENERAL.—In determining under paragraph (4) whether an exemption under paragraph (1) is merited, the United States Secret Service or the Federal Bureau of Investigation may request additional information from the agency or business entity regarding the basis for the claimed exemption, if such additional information is necessary to determine whether the exemption is merited.

(B) REQUIRED COMPLIANCE.—Any agency or business entity that receives a request for additional information under subparagraph (A) shall cooperate with any such request.

(C) TIMING.—If the United States Secret Service or the Federal Bureau of Investigation requests additional information under subparagraph (A), the United States Secret Service or the Federal Bureau of Investigation shall notify the agency or business entity not later than 7 business days after the date of receipt of the additional information whether an exemption under paragraph (1) is merited.

(b) SAFE HARBOR.—

(1) IN GENERAL.—An agency or business entity will be exempt from the notice requirements under section 211, if—

(A) a risk assessment conducted by the agency or business entity concludes that there is no significant risk that a security breach has resulted in, or will result in harm to the individuals whose sensitive personally identifiable information was subject to the security breach; and

(B) the United States Secret Service or the Federal Bureau of Investigation does not indicate within 7 business days from the receipt of written notification from an agency or business entity pursuant to subsection (b)(2), that the agency or business entity should not be exempt from the notice requirements of section 211.

(2) RISK ASSESSMENT REQUIREMENTS.—

(A) CONDUCTING A RISK ASSESSMENT.—Upon discovery of a security breach of an agency or business entity, the agency or business entity shall conduct a risk assessment to determine if there is a significant risk that the security breach resulted in, or will result in, harm to the individuals whose sensitive personally

identifiable information was subject to the security breach.

(i) PRESUMPTION OF NO SIGNIFICANT RISK.—It is presumed that there is no significant risk that the security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach, if such sensitive personally identifiable information has been rendered indecipherable through the use of best practices or methods as described by the Federal Trade Commission, such as redaction, access controls, or other such mechanisms, which are widely accepted as an effective industry practice, or an effective industry standard, or other such mechanisms establishing a presumption that no significant risk exists.

(ii) PRESUMPTION OF SIGNIFICANT RISK.—It is presumed that there is a significant risk that the security breach has resulted in, or will result in, harm to individuals whose sensitive personally identifiable information was subject to the secu-

rity breach if the agency or business entity failed to render such sensitive personally identifiable information indecipherable through the use of best practices or methods, such as redaction, access controls, or other such mechanisms which are widely accepted as an effective industry practice or an effective industry standard, or other such mechanisms establishing a presumption that a significant risk exists.

(B) WRITTEN NOTIFICATION TO LAW ENFORCEMENT.—Without unreasonable delay, but not later than 7 days after the discovery of a security breach, unless extended by the United States Secret Service or the Federal Bureau of Investigation, the agency or business entity must notify the United States Secret Service and the Federal Bureau of Investigation, in writing, of—

(i) the results of the risk assessment; and

(ii) its decision to invoke the risk assessment exemption.

(c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

(1) IN GENERAL.—A business entity shall be exempt from the notice requirement under section 211 if the business entity utilizes or participates in a security program that—

(A) is designed to block the use of the sensitive personally identifiable information to initiate unauthorized financial transactions before they are charged to the account of the individual; and

(B) provides for notice to affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

(2) LIMITATION.—Paragraph (1) does not apply to a business entity if—

(A) the information subject to the security breach includes sensitive personally identifiable information, other than a credit card or credit card security code, of any type of the sensitive personally identifiable information identified in section 3; or

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

SEC. 213. METHODS OF NOTICE TO INDIVIDUALS.

To comply with section 211, an agency or business entity shall provide the following forms of notice:

(1) INDIVIDUAL WRITTEN NOTICE.—Written notice to individuals by 1 of the following means:

(A) Individual written notification to the last known home mailing address of the individual in the records of the agency or business entity.

(B) E-mail notice, unless the individual has expressly opted not to receive such notices of security breaches or the notice is inconsistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).

(2) TELEPHONE NOTICE.—Telephone notice to the individual personally.

(3) PUBLIC NOTICE.—

(A) ELECTRONIC NOTICE.—Prominent notice via all reasonable means of electronic contact between the individual and the agency or business entity, including any website, networked devices, or other interface through which the agency or business entity regularly interacts with the consumer, if the number of

individuals whose personally identifiable information was or is reasonably believed to have been accessed or acquired by an unauthorized person exceeds 5,000.

(B) MEDIA NOTICE.—Notice to major media outlets serving a State or jurisdiction, if the number of residents of such State whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person exceeds 5,000.

SEC. 214. CONTENT OF NOTICE TO INDIVIDUALS.

(a) IN GENERAL.—Regardless of the method by which individual notice is provided to individuals under section 213(1), such notice shall include—

(1) a description of the categories of sensitive personally identifiable information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, and how the agency or business entity came into possession the sensitive personally identifiable information at issue;

(2) a toll-free number—

(A) that the individual may use to contact the agency or business entity, or the agent of the agency or business entity; and

(B) from which the individual may learn what types of sensitive personally identifiable information the agency or business entity maintained about that individual;

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

(4) the telephone numbers and websites for the relevant Federal agencies that provide information regarding identity theft prevention and protection;

(5) notice that the individual is entitled to receive, at no cost to such individual, consumer credit reports on a quarterly basis for a period of 2 years, credit monitoring or any other service that enables consumers to detect the misuse of sensitive personally identifiable information for a period of 2 years, and instructions to the individual on requesting such reports or service from the agency or business entity;

(6) notice that the individual is entitled to receive a security freeze and that the agency or business entity will be liable for any costs associated with the security freeze for 2 years and the necessary instructions for requesting a security freeze; and

(7) notice that any costs or damages incurred by an individual as a result of a security breach will be paid by the business entity or agency that experienced the security breach.

(b) TELEPHONE NOTICE.—Telephone notice described in section 213(2) shall include, to the extent possible—

(1) notification that a security breach has occurred and that the individual's sensitive personally identifiable information may have been compromised;

(2) a description of the categories of sensitive personally identifiable information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person;

(3) a toll-free number and website—

(A) that the individual may use to contact the agency or business entity, or the authorized agent of the agency or business entity; and

(B) from which the individual may learn what types of sensitive personally identifiable information the agency or business entity maintained about that individual and remedies available to that individual; and

(4) an alert to the individual that the agency or business entity is sending or has sent written notification containing additional information as required under section 213(1)(A).

(c) PUBLIC NOTICE.—Public notice described in section 213(3) shall include—

(1) electronic notice, which includes—

(A) notification that a security breach has occurred and that the individual's sensitive personally identifiable information may have been compromised;

(B) a description of the categories of sensitive personally identifiable information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person; and

(C) a toll-free number and website—

(i) that the individual may use to contact the agency or business entity, or the authorized agent of the agency or business entity; and

(ii) from which the individual may learn what types of sensitive personally identifiable information the agency or business entity maintained about that indi-

vidual and remedies available to that individual;

(2) media notice, which includes—

(A) a description of the categories of sensitive personally identifiable information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person;

(B) a toll-free number—

(i) that the individual may use to contact the agency or business entity, or the authorized agent of the agency or business entity; and

(ii) from which the individual may learn what types of sensitive personally identifiable information the agency or business entity maintained about that individual and remedies available to that individual;

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

(D) the telephone numbers and websites for the relevant Federal agencies that provide

information regarding identity theft prevention and protection;

(E) notice that the affected individuals are entitled to receive, at no cost to such individuals, consumer credit reports on a quarterly basis for a period of 2 years, credit monitoring, or any other service that enables consumers to detect the misuse of sensitive personally identifiable information for a period of 2 years;

(F) notice that the individual is entitled to receive a security freeze and that the agency or business entity will be liable for any costs associated with the security freeze for 2 years; and

(G) notice that the individual is entitled to receive compensation from the business entity or agency for any costs or damages incurred by the individual resulting from the security breach.

(d) ADDITIONAL CONTENT.—Notwithstanding section 221, a State may require that a notice under subsection (a) shall also include information regarding victim protection assistance provided for by that State.

SEC. 215. REMEDIES FOR SECURITY BREACH.

(a) CREDIT REPORTS AND CREDIT MONITORING.—An agency or business entity required to provide notifica-

~~tion under this subtitle shall, upon request of an individual whose sensitive personally identifiable information was included in the security breach, provide or arrange for the provision of, to each such individual and at no cost to such individual—~~

~~(1) consumer credit reports from not fewer than 1 of the major credit reporting agencies beginning not later than 60 days following the request of the individual and continuing on a quarterly basis for a period of 2 years thereafter; and~~

~~(2) a credit monitoring or other service that enables consumers to detect the misuse of their personal information, beginning not later than 60 days following the request of the individual and continuing for a period of 2 years.~~

~~(b) SECURITY FREEZE.—~~

~~(1) REQUEST.—Any consumer may submit a written request, by certified mail or such other secure method as authorized by a credit rating agency, to a credit rating agency to place a security freeze on the credit report of the consumer.~~

~~(2) IMPLEMENTATION OF SECURITY FREEZE.—Upon receipt of a written request under paragraph (1), a credit rating agency shall—~~

(A) not later than 5 business days after receipt of the request, place a security freeze on the credit report of the consumer; and

(B) not later than 10 business days after placing a security freeze, send a written confirmation of such security freeze to the consumer, which shall provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of the credit report of the consumer to a third party or for a specified period of time.

(3) DURATION OF SECURITY FREEZE.—Except as provided in paragraph (4), any security freeze authorized pursuant to the provisions of this section shall remain in effect until the consumer requests security freeze to be removed.

(4) DISCLOSURE OF CREDIT REPORT TO THIRD PARTY.—

(A) IN GENERAL.—If a consumer that has requested a security freeze under this subsection wishes to authorize the disclosure of the credit report of the consumer to a third party, or for a specified period of time, while such se-

curity freeze is in effect, the consumer shall contact the credit rating agency and provide—

(i) proper identification;

(ii) the unique personal identification number or password described in paragraph (2)(B); and

(iii) proper information regarding the third party who is to receive the credit report or the time period for which the credit report shall be available.

(B) REQUIREMENT.—Not later than 3 business days after receipt of a request under subparagraph (A), a credit rating agency shall lift the security freeze.

(5) PROCEDURES.—

(A) IN GENERAL.—A credit rating agency shall develop procedures to receive and process requests from consumers under paragraph (2) of this section.

(B) REQUIREMENT.—Procedures developed under subparagraph (A), at a minimum, shall include the ability of a consumer to send such temporary lift or removal request by electronic mail, letter, telephone, or facsimile.

(6) REQUESTS BY THIRD PARTY.—If a third party requests access to a credit report of a consumer that has been frozen under this subsection and the consumer has not authorized the disclosure of the credit report of the consumer to the third party, the third party may deem such credit application as incomplete.

(7) DETERMINATION BY CREDIT RATING AGENCY.—

(A) IN GENERAL.—A credit rating agency may refuse to implement or may remove a security freeze under this subsection if the agency determines, in good faith, that—

(i) the request for a security freeze was made as part of a fraud that the consumer participated in, had knowledge of, or that can be demonstrated by circumstantial evidence; or

(ii) the consumer credit report was frozen due to a material misrepresentation of fact by the consumer.

(B) NOTICE.—If a credit rating agency makes a determination under subparagraph (A) to not implement, or to remove, a security freeze under this subsection, the credit rating

agency shall notify the consumer in writing of such determination—

(i) in the case of a determination not to implement a security freeze, not later than 5 business days after the determination is made; and

(ii) in the case of a removal of a security freeze, prior to removing the freeze on the credit report of the consumer.

(8) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to prohibit disclosure of a credit report of a consumer to—

(A) a person, or the person's subsidiary, affiliate, agent or assignee with which the consumer has or, prior to assignment, had an account, contract or debtor-creditor relationship for the purpose of reviewing the account or collecting the financial obligation owing for the account, contract or debt;

(B) a subsidiary, affiliate, agent, assignee or prospective assignee of a person to whom access has been granted under paragraph (4) for the purpose of facilitating the extension of credit or other permissible use;

(C) any person acting pursuant to a court order, warrant or subpoena;

(D) any person for the purpose of using such credit information to prescreen as provided by the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(E) any person for the sole purpose of providing a credit file monitoring subscription service to which the consumer has subscribed;

(F) a credit rating agency for the sole purpose of providing a consumer with a copy of the credit report of the consumer upon the request of the consumer; or

(G) a Federal, State or local governmental entity, including a law enforcement agency, or court, or their agents or assignees pursuant to their statutory or regulatory duties. For purposes of this subsection, ''reviewing the account'' includes activities related to account maintenance, monitoring, credit line increases and account upgrades and enhancements; and

(H) any person for the sole purpose of providing a remedy requested by an individual under this section.

(9) EXCEPTIONS.—The following persons shall not be required to place a security freeze under this subsection, but shall be subject to any security freeze placed on a credit report by another credit rating agency:

(A) A check services or fraud prevention services company that reports on incidents of fraud or issues authorizations for the purpose of approving or processing negotiable instruments, electronic fund transfers or similar methods of payment.

(B) A deposit account information service company that issues reports regarding account closures due to fraud, substantial overdrafts, automated teller machine abuse, or similar information regarding a consumer to inquiring banks or other financial institutions for use only in reviewing a consumer request for a deposit account at the inquiring bank or financial institution.

(C) A credit rating agency that—

(i) acts only to resell credit information by assembling and merging information contained in a database of 1 or more credit reporting agencies; and

(ii) does not maintain a permanent database of credit information from which new credit reports are produced.

(10) FEES.—

(A) IN GENERAL.—A credit rating agency may charge reasonable fees for each security freeze, removal of such freeze or temporary lift of such freeze for a period of time, and a temporary lift of such freeze for a specific party.

(B) REQUIREMENT.—Any fees charged under subparagraph (A) shall be borne by the agency or business entity providing notice under section 214 for 2 years following the establishment of the security freeze under this subsection.

(c) COSTS RESULTING FROM A SECURITY BREACH.—

(1) IN GENERAL.—A business entity or agency that experiences a security breach and is required to provide notice under this subtitle shall pay, upon request, to any individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed or acquired as a result of such security breach, any costs or damages incurred by the individual as a result of such secu-

rity breach, including costs associated with identity theft suffered as a result of such security breach.

(2) COMPLIANCE.—A business entity or agency shall be deemed in compliance with this subsection if the business entity or agency—

(A) provides insurance to any individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed or acquired as a result of a security breach and such insurance is sufficient to compensate the consumer for not less than $25,000 of costs or damages; or

(B) pays, without unreasonable delay, any actual costs or damages incurred by an individual as a result of the security breach.

SEC. 216. NOTICE TO CREDIT REPORTING AGENCIES.

If an agency or business entity is required to provide notification to more than 5,000 individuals under section 211(a), the agency or business entity shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis (as defined in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)) of the timing and distribution of the notices. Such notice shall be given to the consumer credit reporting agencies without unreasonable delay and, if it

will not delay notice to the affected individuals, prior to the distribution of notices to the affected individuals.

SEC. 217. NOTICE TO LAW ENFORCEMENT.

(a) SECRET SERVICE AND FBI.—Any business entity or agency shall notify the United States Secret Service and the Federal Bureau of Investigation of the fact that a security breach has occurred if—

(1) the number of individuals whose sensitive personally identifying information was, or is reasonably believed to have been accessed or acquired by an unauthorized person exceeds 5,000;

(2) the security breach involves a database, networked or integrated databases, or other data system containing the sensitive personally identifiable information of more than 500,000 individuals nationwide;

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

(4) the security breach involves primarily sensitive personally identifiable information of individuals known to the agency or business entity to be employees and contractors of the Federal Government involved in national security or law enforcement.

(b) FTC REVIEW OF THRESHOLDS.—The Federal Trade Commission may alter the circumstances under which notification is required under subsection (a) in a matter consistent with the public interest.

(c) NOTICE TO OTHER LAW ENFORCEMENT AGENCIES.—The United States Secret Service and the Federal Bureau of Investigation shall be responsible for notifying—

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

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

(3) the Federal Trade Commission, if the security breach involves consumer reporting agencies subject to the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), or anticompetitive conduct.

(d) TIMING OF NOTICES.—The notices required under this section shall be delivered as follows:

(1) Notice under subsection (a) shall be delivered as promptly as possible, but not later than 10 days after discovery of the security breach.

(2) Notice under section 211 shall be delivered to individuals not later than 48 hours after the Federal Bureau of Investigation or the Secret Service

receives notice of a security breach from an agency or business entity.

SEC. 218. FEDERAL ENFORCEMENT.

(a) CIVIL ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—The Attorney General may bring a civil action in the appropriate United States district court against any business entity that engages in conduct constituting a violation of this subtitle and, upon proof of such conduct by a preponderance of the evidence, such business entity shall be subject to a civil penalty of not more than $500 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $20,000,000 per violation, unless such conduct is found to be willful or intentional.

(2) PRESUMPTION.—A violation of section 212(a)(2) shall be presumed to be willful or intentional conduct.

(b) CONSIDERATIONS.—In determining the amount of a civil penalty under this subsection, the court shall take into account—

(1) the degree of culpability of the business entity;

~~(2) any prior violations of this subtitle by the business entity;~~

~~(3) the ability of the business entity to pay a civil penalty;~~

~~(4) the effect on the ability of the business entity to continue to do business;~~

~~(5) the number of individuals whose personally identifiable information was compromised by the breach;~~

~~(6) the relative cost of compliance with this subtitle; and~~

~~(7) such other matters as justice may require.~~

~~(c) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—~~

~~(1) IN GENERAL.—If it appears that a business entity has engaged, or is engaged, in any act or practice constituting a violation of this subtitle, the Attorney General may petition an appropriate district court of the United States for an order—~~

~~(A) enjoining such act or practice; or~~

~~(B) enforcing compliance with this subtitle.~~

~~(2) ISSUANCE OF ORDER.—A court may issue an order under paragraph (1), if the court finds that the conduct in question constitutes a violation of this subtitle.~~

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

(e) FRAUD ALERT.—Section 605A(b)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681c–1(b)(1)) is amended by inserting ", or evidence that the consumer has received notice that the consumer's financial information has or may have been compromised," after "identity theft report".

SEC. 219. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) IN GENERAL.—

(1) CIVIL ACTIONS.—

(A) IN GENERAL.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of a business entity in a practice that is prohibited under this subtitle, the State or the State or local law enforcement agency on behalf of the residents of the agency's jurisdiction, may bring

a civil action on behalf of the residents of the State or jurisdiction in a district court of the United States of appropriate jurisdiction or any other court of competent jurisdiction, including a State court, to—

(i) enjoin that practice;

(ii) enforce compliance with this subtitle; or

(iii) obtain civil penalties of not more than $500 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $20,000,000 per violation, unless such conduct is found to be willful or intentional.

(B) PRESUMPTION.—A violation of section 212(a)(2) shall be presumed to be willful or intentional.

(2) CONSIDERATIONS.—In determining the amount of a civil penalty under this subsection, the court shall take into account—

(A) the degree of culpability of the business entity;

(B) any prior violations of this subtitle by the business entity;

(C) the ability of the business entity to pay a civil penalty;

(D) the effect on the ability of the business entity to continue to do business;

(E) the number of individuals whose personally identifiable information was compromised by the breach;

(F) the relative cost of compliance with this subtitle; and

(G) such other matters as justice may require.

(3) NOTICE.—

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

(i) written notice of the action; and

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

(B) EXEMPTION.—

(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 subtitle, if the State attorney general determines that it is not feasible to provide the notice described in such subparagraph before the filing of the action.

(ii) NOTIFICATION.—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 State attorney general files the action.

(b) FEDERAL PROCEEDINGS.—Upon receiving notice under subsection (a)(2), the Attorney General shall have the right to—

(1) move to stay the action, pending the final disposition of a pending Federal proceeding or action;

(2) initiate an action in the appropriate United States district court under section 217 and move to consolidate all pending actions, including State actions, in such court;

(3) intervene in an action brought under subsection (a)(2); and

(4) file petitions for appeal.

(c) PENDING PROCEEDINGS.—If the Attorney General has instituted a proceeding or action for a violation

of this subtitle or any regulations thereunder, no attorney general of a State may, during the pendency of such proceeding or action, bring an action under this subtitle against any defendant named in such criminal proceeding or civil action for any violation that is alleged in that proceeding or action.

(d) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this subtitle regarding notification 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—

(1) conduct investigations;

(2) administer oaths or affirmations; or

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

(e) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in—

(A) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(B) another court of competent jurisdiction.

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

(A) is an inhabitant; or

(B) may be found.

SEC. 220. SUPPLEMENTAL ENFORCEMENT BY INDIVIDUALS.

(a) IN GENERAL.—Any person aggrieved by a violation of the provisions of section 211, 213, 214, 215, or 216 by a business entity may bring a civil action in a court of appropriate jurisdiction to recover for personal injuries sustained as a result of the violation.

(b) REMEDIES IN A CITIZEN SUIT.—

(1) DAMAGES.—Any individual harmed by a failure of a business entity to comply with the provisions of section 211, 213, 214, 215, or 216, shall be able to collect damages of not more than $500 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $20,000,000 per violation.

(2) PUNITIVE DAMAGES.—A business entity may be liable for punitive damages if it—

(A) intentionally or willfully violates the provisions of section 211, 213, 214, 215, or 216; or

(B) failed to comply with the requirements of subsections (a) through (d) of section 202.

(3) EQUITABLE RELIEF.—A business entity that violates the provisions of section 211, 213, 214, 215, or 216 may be enjoined to provide required remedies under section 215 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.

(c) ACCESS TO JUSTICE.—The rights and remedies afforded by this section shall not be abridged or precluded by any predispute arbitration agreement, and any claims under this section that arise from the same security breach are presumed to meet the commonality requirement under rule 23(a)(2) of the Federal Rules of Civil Procedure.

SEC. 221. RELATION TO OTHER LAWS.

(a) IN GENERAL.—The provisions of this subtitle shall supersede any other provision of Federal law or any provision of law of any State relating to notification by

a business entity engaged in interstate commerce or an agency of a security breach, except as provided in section 214(c).

(b) RULE OF CONSTRUCTION.—Nothing in this subtitle shall be construed to exempt any entity from liability under common law, including through the operation of ordinary preemption principles, for damages caused by the failure to notify an individual following a security breach.

(c) PRESUMPTION OF PER SE NEGLIGENCE.—If a business entity fails to comply with the requirements in section 211, 212, 213, 214, 215, or 216, there shall be a presumption that the entity was per se negligent.

SEC. 222. AUTHORIZATION OF APPROPRIATIONS.

There are 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. 223. REPORTING ON RISK ASSESSMENT EXEMPTIONS.

The United States Secret Service and the Federal Bureau of Investigation shall report to Congress not later than 18 months after the date of enactment of this Act, and upon the request by Congress thereafter, on—

(1) the number and nature of the security breaches described in the notices filed by those busi-

ness entities invoking the risk assessment exemption under section 212(b) and the response of the United States Secret Service and the Federal Bureau of Investigation to such notices; and

(2) the number and nature of security breaches subject to the national security and law enforcement exemptions under section 212(a), provided that such report may not disclose the contents of any risk assessment provided to the United States Secret Service and the Federal Bureau of Investigation pursuant to this subtitle.

Subtitle C—Post-Breach Technical Information Clearinghouse

SEC. 230. CLEARINGHOUSE INFORMATION COLLECTION, MAINTENANCE, AND ACCESS.

(a) IN GENERAL.—The Attorney General shall maintain a clearinghouse of technical information concerning system vulnerabilities identified in the wake of security breaches, which shall—

(1) contain information disclosed by agencies or business entities under subsection (b); and

(2) be accessible to certified entities under subsection (c).

(b) POST-BREACH TECHNICAL NOTIFICATION.—In any instance where an agency or business entity is re-

quired to notify the United States Secret Service and the Federal Bureau of Investigation under section 217, the agency or business entity shall also provide the Attorney General with technical information concerning the nature of the security breach, including—

(1) technical information regarding any system vulnerabilities of the agency or business entity revealed by or identified as a consequence of the security breach;

(2) technical information regarding any system vulnerabilities of the agency or business entity actually exploited during the security breach; and

(3) any other technical information concerning the nature of the security breach deemed appropriate for collection by the Attorney General in furtherance of this subtitle.

(c) ACCESS TO CLEARINGHOUSE.—Any entity certified under subsection (d) may review information maintained by the technical information clearinghouse for the purpose of preventing security breaches that threaten the security of sensitive personally identifiable information.

(d) CERTIFICATION FOR ACCESS.—The Attorney General shall issue and revoke certifications to agencies and business entities wishing to review information maintained by the technical information clearinghouse and

shall establish conditions for obtaining and maintaining such certifications, including agreement that any information obtained directly or derived indirectly from the review of information maintained by the technical information clearinghouse—

(1) shall only be used to improve the security and reduce the vulnerability of networks that use personally identifiable information;

(2) may not be used for any competitive commercial purpose; and

(3) may not be shared with any third party, including other parties certified for access to the information clearinghouse, without the express written consent of the Attorney General.

(c) RULEMAKING.—In consultation with the private sector, appropriate representatives of State and local governments, and other appropriate Federal agencies, the Attorney General shall promulgate any regulations pursuant to section 553 of title 5, United States Code, necessary to carry out the provisions of this section.

SEC. 231. PROTECTIONS FOR CLEARINGHOUSE PARTICIPANTS.

(a) PROTECTION OF PROPRIETARY INFORMATION.—To the extent feasible, the Attorney General shall ensure that any technical information disclosed to the Attorney

~~General under this subtitle shall be stored in a format designed to protect proprietary business information from inadvertent disclosure.~~

~~(b) ANONYMOUS DATA RELEASE.—To the extent feasible, the Attorney General shall ensure that all information stored in the technical information clearinghouse and accessed by certified parties is presented in a form that minimizes the potential for such information to be traced to a particular network, company, or security breach incident.~~

~~(c) PROTECTION FROM PUBLIC DISCLOSURE.—Except as otherwise provided in this subtitle—~~

~~(1) security and vulnerability information collected under this section and provided to the Federal Government, including aggregated analysis and data, shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and~~

~~(2) under section 230(c), security and vulnerability-related information provided to the Federal Government under this section, including aggregated analysis and data, shall be protected from public disclosure, except that this paragraph—~~

~~(A) does not prohibit the sharing of such information, as the Attorney General determines to be appropriate, in order to mitigate~~

cybersecurity threats or further the official functions of a government agency; and

(B) does not authorized such information to be withheld from a committee of Congress authorized to request the information.

(d) PROTECTION OF CLASSIFIED INFORMATION.—Nothing in this subtitle permits the unauthorized disclosure of classified information.

SEC. 232. EFFECTIVE DATE.

This subtitle shall take effect on the expiration of the date which is 90 days after the date of enactment of this Act.

TITLE III—ACCESS TO AND USE OF COMMERCIAL DATA

SEC. 301. GENERAL SERVICES ADMINISTRATION REVIEW OF CONTRACTS.

(a) IN GENERAL.—In considering contract awards totaling more than $500,000 and entered into after the date of enactment of this Act with data brokers, the Administrator of the General Services Administration shall evaluate—

(1) the data privacy and security program of a data broker to ensure the privacy and security of data containing personally identifiable information, including whether such program adequately address-

es privacy and security threats created by malicious software or code, or the use of peer-to-peer file sharing software;

(2) the compliance of a data broker with such program;

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

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

(b) COMPLIANCE SAFE HARBOR.—The data privacy and security program of a data broker shall be deemed sufficient for the purposes of subsection (a), if the data broker complies with or provides protection equal to industry standards, as identified by the Federal Trade Commission, that are applicable to the type of personally identifiable information involved in the ordinary course of business of such data broker.

(c) PENALTIES.—In awarding contracts with data brokers 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—

(1) include monetary or other penalties—

(A) for failure to comply with subtitles A and B of title III; or

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

(2) require a data broker that engages service providers not subject to subtitle A of title III for responsibilities related to sensitive personally identifiable information to—

(A) exercise appropriate due diligence in selecting those service providers for responsibilities related to personally identifiable information;

(B) 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

(C) require such service providers, by contract, to implement and maintain appropriate measures designed to meet the objectives and requirements in title III.

(d) LIMITATION.—The penalties under subsection (c) shall not apply to a data broker providing information that is accurately and completely recorded from a public record source or licensor.

SEC. 302. 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 (as that term is defined in section 3 of the Personal Data Protection and Breach Accountability Act of 2011) and ensuring remedial action to address any significant deficiencies.".

SEC. 303. 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'';

(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 data broker (as such terms are defined in section 3 of the Personal Data Protection and Breach Accountability Act of 2011).''.

(b) LIMITATION.—Notwithstanding any other provision of law, commencing 1 year after the date of enactment of this Act, no Federal agency may enter into a contract with a data broker to access for a fee any 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 subject to the provision in that Act pertaining to sensitive information, include a description of—

(A) such database;

(B) the name of the data broker 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 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 totaling more than $500,000, provisions—

(A) providing for penalties—

(i) for failure to comply with title III of this Act; or

(ii) 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; and

(B) requiring a data broker that engages service providers not subject to subtitle A of title III for responsibilities related to sensitive personally identifiable information to—

(i) exercise appropriate due diligence in selecting those service providers for responsibilities related to personally identifiable information;

(ii) 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

(iii) require such service providers, by contract, to implement and maintain appropriate measures designed to meet the objectives and requirements in title III.

(c) LIMITATION ON PENALTIES.—The penalties under subsection (b)(3)(A) shall not apply to a data broker providing information that is accurately and completely recorded from a public record source.

(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 conduct a study and audit and prepare a report on Federal agency actions to address the recommendations in the Government Accountability Office's April 2006 report on agency adherence to key privacy principles in using data brokers or commercial databases containing personally identifiable information.

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

SEC. 304. FBI REPORT ON REPORTED BREACHES AND COMPLIANCE.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, and each year thereafter, the Federal Bureau of Investigation, in coordination with the Secret Service, shall submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a report regarding any reported breaches at agencies or business entities during the preceding year.

(b) REPORT CONTENT.—Such reporting shall include—

(1) the total instances of breaches of security in the previous year;

(2) the percentage of breaches described in subsection (a) that occurred at an agency or business

entity that did not comply with the personal data privacy and security program under section 202; and

(3) recommendations, if any, for modifying or amending this Act to increase its effectiveness.

SEC. 305. DEPARTMENT OF JUSTICE REPORT ON ENFORCEMENT ACTIONS.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, and each year thereafter, the Attorney General shall submit to Congress a report on the enforcement actions taken in the previous year in cases of violations of any sections of this Act.

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

(1) statistics on Federal enforcement actions, State attorneys general enforcement actions, and private enforcement actions related to the provisions of this Act; and

(2) recommendations, if any, for modifying of amending this Act to increase the effectiveness of such enforcement actions.

SEC. 306. DEPARTMENT OF JUSTICE REPORT ON ENFORCEMENT ACTIONS.

Section 529 of title 28, United States Code, is amended by adding at the end the following:

''(c) Not later than 1 year after the date of enactment of the Personal Data Protection and Breach Accountability Act of 2011, and every fiscal year thereafter, the Attorney General shall submit to Congress a report on the efforts of the Federal Government to enforce the Personal Data Protection and Breach Accountability Act of 2011 that shall include a description of the best practices for enforcement of such Act.''.

SEC. 307. FBI REPORT ON NOTIFICATION EFFECTIVENESS.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, and each year thereafter, the Federal Bureau of Investigation, in coordination with the Secret Service, shall submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a report regarding the effectiveness of post-breach notification practices by agencies and business entities.

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

(1) in each instance of a breach of security, the amount of time between the instance of the breach and the discovery of the breach by the affected business entity;

(2) in each instance of a breach of security, the amount of time between the discovery of the breach

~~by the affected business entity and the notification to the FBI and Secret Service; and~~

~~(3) in each instance of a breach of security, the amount of time between the discovery of the breach by the affected business entity and the notification to individuals whose sensitive personally identifiable information was compromised.~~

~~TITLE IV—COMPLIANCE WITH STATUTORY PAY-AS-YOU-GO ACT~~

~~SEC. 401. BUDGET COMPLIANCE.~~

~~The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement titled "Budgetary Effects of PAYGO Legislation" for this Act, submitted for printing in the Congressional Record by the Chairman of the Senate Budget Committee, provided that such statement has been submitted prior to the vote on passage.~~

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Personal Data Protection and Breach Accountability Act of 2011".

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

SEC. 2. FINDINGS.

Congress finds that—

(1) databases of personally 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 confidentiality 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 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;

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

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

(10) because government use of commercial data containing personal information potentially affects individual privacy, and law enforcement and national security operations, there is a need for Congress to exercise oversight over government use of commercial data;

(11) over 22,960,000 cases of data breaches involving personally identifiable information were reported through July of 2011, and in 2009 through 2010, over 230,900,000 cases of personal data breaches were reported;

(12) facilitating information sharing among business entities and across sectors in the event of a breach can assist in remediating the breach and preventing similar breaches in the future;

(13) because the Federal Government has limited resources, consumers themselves play a vital and complementary role in facilitating prompt notification and protecting against future breaches of security;

(14) in addition to the immediate damages caused by security breaches, the lack of basic remedial requirements often forces individuals whose sensitive personally identifiable information is compromised as a result of a security breach to incur the economic costs of litigation to seek remedies, and the economic costs of fees required in many States to freeze compromised accounts; and

(15) victims of personal data breaches may suffer debilitating emotional and physical effects and become depressed or anxious, especially in cases of repeated or unresolved instances of data breaches.

SEC. 3. DEFINITIONS.

(a) IN GENERAL.—In this Act, the following definitions shall apply:

(1) AFFILIATE.—The term "affiliate" means persons related by common ownership or by corporate control.

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

(3) BUSINESS ENTITY.—The term "business entity" means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture established to make a profit, or nonprofit.

(4) CREDIT RATING AGENCY.—The term "credit rating agency" has the meaning given such term in section 3(a)(61) of the Securities Exchange Act of 1934 (12 U.S.C. 78c(a)(61)).

(5) CREDIT REPORT.—The term "credit report" means a consumer report, as that term is defined in section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a).

(6) DATA BROKER.—The term "data broker" means a business entity which for monetary fees or dues regularly engages in the practice of collecting, transmitting, or providing access to sensitive personally identifiable information on more than 5,000 individuals who are not the customers or employees of

that business entity or affiliate primarily for the purposes of providing such information to nonaffiliated third parties on an interstate basis.

(7) DESIGNATED ENTITY.—The term "designated entity" means the Federal Government entity designated under section 217(a).

(8) ENCRYPTION.—The term "encryption"—

(A) means the protection of data in electronic form, in storage or in transit, using an encryption technology that has been generally accepted by experts in the field of information security that renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and

(B) includes appropriate management and safeguards of such cryptographic keys so as to protect the integrity of the encryption.

(9) IDENTITY THEFT.—The term "identity theft" means a violation of section 1028(a)(7) of title 18, United States Code.

(10) INTELLIGENCE COMMUNITY.—The term "intelligence community" includes the following:

(A) The Office of the Director of National Intelligence.

(B) The Central Intelligence Agency.

(C) The National Security Agency.

(D) The Defense Intelligence Agency.

(E) The National Geospatial-Intelligence Agency.

(F) The National Reconnaissance Office.

(G) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs.

(H) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, and the Department of Energy.

(I) The Bureau of Intelligence and Research of the Department of State.

(J) The Office of Intelligence and Analysis of the Department of the Treasury.

(K) The elements of the Department of Homeland Security concerned with the analysis of intelligence information, including the Office of Intelligence of the Coast Guard.

(L) Such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the de-

partment or agency concerned, as an element of the intelligence community.

(11) PREDISPUTE ARBITRATION AGREEMENT.—The term "predispute arbitration agreement" means any agreement to arbitrate a dispute that had not yet arisen at the time of the making of the agreement.

(12) PUBLIC RECORD SOURCE.—The term "public record source" means the Congress, any agency, any State or local government agency, the government of the District of Columbia and governments of the territories or possessions of the United States, and Federal, State or local courts, courts martial and military commissions, that maintain personally identifiable information in records available to the public.

(13) SECURITY BREACH.—

(A) IN GENERAL.—The term "security breach" means compromise of the security, confidentiality, or integrity of, or the loss of, computerized data through misrepresentation or actions that result in, or that there is a reasonable basis to conclude has resulted in—

(i) the unauthorized acquisition of sensitive personally identifiable information; or

(ii) access to sensitive personally identifiable information that is for an unauthorized purpose, or in excess of authorization.

(B) EXCLUSION.—The term "security breach" does not include—

(i) a good faith acquisition of sensitive personally identifiable information by a business entity or agency, or an employee or agent of a business entity or agency, if the sensitive personally identifiable information is not subject to further unauthorized disclosure;

(ii) the release of a public record not otherwise subject to confidentiality or nondisclosure requirements or the release of information obtained from a public record; or

(iii) any lawfully authorized criminal investigation or authorized investigative, protective, or intelligence activities that are carried out by or on behalf of any element of the intelligence community and conducted in accordance with the United States laws, authorities, and regulations governing such intelligence activities.

(14) SECURITY FREEZE.—The term "security freeze" means a notice, at the request of the consumer and subject to exceptions in section 215(b), that prohibits the consumer reporting agency from releasing all or any part of the consumer's credit report or any information derived from it without the express authorization of the consumer.

(15) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term "sensitive personally identifiable information" means any information or compilation of information, in electronic or digital form that includes the following:

(A) An individual's first and last name or first initial and last name in combination with any 2 of the following data elements:

(i) Home address.

(ii) Telephone number of the individual.

(iii) Mother's maiden name.

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

(B) A non-truncated social security number, driver's license number, passport number, or alien registration number or other government-issued unique identification number.

(C) Information about an individual's geographic location that is in whole or in part generated by or derived from that individual's use of a wireless communication device or other electronic device, excluding telephone and instrument numbers and network or Internet Protocol addresses.

(D) Unique biometric data such as a finger print, voice print, face print, a retina or iris image, or any other unique physical representation.

(E) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, health insurance policy or subscriber identification number, or routing code.

(F) Not less than 2 of the following data elements:

(i) An individual's first and last name or first initial and last name.

(ii) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.

(iii) Any security code, access code, or password, or source code that could be used to generate such codes and passwords.

(iv) Information regarding an individual's medical history, mental or physical medical condition, or medical treatment or diagnosis by a health care professional.

(G) Any other combination of data elements that could allow unauthorized access to or acquisition of the information described in subparagraph (A), (B), (C), (D), (E), or (F), including—

(i) a unique account identifier;

(ii) an electronic identification number;

(iii) a user name;

(iv) a routing code; or

(v) any associated security code, access code, or password or any associated security questions and answers that could allow unauthorized access to the account.

(16) SERVICE PROVIDER.—

(A) IN GENERAL.—The term "service provider" means a business entity that—

(i) provides electronic data transmission, routing, intermediate and transient storage, or connections to the system or network of the business entity;

(ii) is not the sender or the intended recipient of the data;

(iii) is not ordinarily expected to select or modify the content of the electronic data; and

(iv) transmits, routes, stores, or provides connections for personal information in a manner that personal information is undifferentiated from other types of data that such business entity transmits, routes, stores, or provides connections.

(B) SAVINGS CLAUSE.—Any such business entity shall be treated as a service provider under this Act only to the extent that the business entity is engaged in the provision of the transmission, routing, intermediate and transient storage or connections described in subparagraph (A).

(b) MODIFIED DEFINITION BY RULEMAKING.—The Federal Trade Commission may, by rule promulgated under section 553 of title 5, United States Code, modify

the definition of "sensitive personally identifiable information" in a manner consistent with the purposes of this Act and to the extent that such modification will not unreasonably impede interstate commerce.

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

SEC. 101. CONCEALMENT OF SECURITY BREACHES INVOLVING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.

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

"§ 1041. Concealment of security breaches involving sensitive personally identifiable information

"(a) Whoever, having knowledge of a security breach and of the fact that notice of such security breach is required under title II of the Personal Data Protection and Breach Accountability Act of 2011, intentionally or willfully conceals the fact of such security breach and which breach, shall, in the event that such security breach results in economic harm or substantial emotional distress to 1 or more persons, shall be fined under this title or imprisoned not more than 5 years, or both.

"(b) For purposes of subsection (a), the term 'person' has the same meaning as in section 1030(e)(12) of title 18, United States Code.

"(c) Any person seeking an exemption under section 212(b) of the Personal Data Protection and Breach Accountability Act of 2011 shall be immune from prosecution under this section if the United States Secret Service does not indicate, in writing, that such notice be given under section 212(b)(1)(B) of the Personal Data Protection and Breach Accountability Act of 2011.".

(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:

"1041. Concealment of security breaches involving sensitive personally identifiable information.".

(c) ENFORCEMENT AUTHORITY.—

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

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

SEC. 102. UNAUTHORIZED MANIPULATION OF INTERNET TRAFFIC ON A USER'S COMPUTER.

(a) DEFINITION.—In this section, the term "protected computer" has the meaning given the term in section 1030(e)(2) of title 18, United States Code.

(b) PROHIBITION.—

(1) IN GENERAL.—Unless a service provider provides a clear and conspicuous disclosure of data collected in the process of intercepting a web search or query entered by an authorized user of a protected computer, and obtains the consent of an authorized user of the protected computer prior to any such action, it shall be unlawful for a service provider to knowingly or intentionally—

(A) bypass the display of search engine results and redirect web searches or queries entered by an authorized user of a protected computer directly to a commercial website, counterfeit web page, or targeted advertisement and derive an economic benefit from such activity; or

(B) monitor, manipulate, aggregate, and market the data collected in the process of intercepting a web search or query entered by an authorized user of a protected computer and derive an economic benefit from such activity.

(2) CONSENT.—A service provider may not require consent to perform the collection of data described in paragraph (1) as a condition of providing service to an authorized user of the protected computer.

(c) LIMITATIONS ON LIABILITY.—The restrictions imposed under this section do not apply to any monitoring of, or interaction with, a subscriber's Internet or other network connection or service, or a protected computer, by or at the direction of a telecommunications carrier, cable operator, computer hardware or software provider, financial institution or provider of information services or interactive computer service for—

(1) network or computer security purposes;

(2) diagnostics;

(3) technical support;

(4) repair;

(5) network management;

(6) authorized updates of software or system firmware;

(7) authorized remote system management;

(8) authorized provision of protection for users of the computer from objectionable content;

(9) authorized scanning for computer software used in violation of this section for removal by an authorized user; or

(10) detection or prevention of fraud.

(d) ENFORCEMENT BY THE ATTORNEY GENERAL.—

(1) LIABILITY AND PENALTY FOR VIOLATIONS.—Any person who engages in an activity in violation of this section shall be fined not more than $500,000.

(2) ENHANCED LIABILITY AND PENALTIES FOR PATTERN OR PRACTICE OF VIOLATIONS.—

(A) IN GENERAL.—Any person who engages in a pattern or practice of activity that violates the provisions of this section shall be fined not more than $1,000,000.

(B) TREATMENT OF SINGLE ACTION OR CONDUCT.—For purposes of subparagraph (A), any single action or conduct that violates this section with respect to multiple protected computers shall be construed as a single violation.

(3) CONSIDERATIONS.—In determining the amount of any penalty under paragraph (1) or (2), the court shall take into account—

(A) the degree of culpability of the defendant;

(B) any history of prior such conduct;

(C) the ability of the defendant to pay any fine imposed;

(D) the effect on the ability of the defendant to continue to do business; and

(E) such other matters as justice may require.

TITLE II—PRIVACY AND SECURITY OF SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION

Subtitle A—A Data Privacy and Security Program

SEC. 201. 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 security of sensitive personally identifiable information.

(b) IN GENERAL.—A business entity engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive 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 pro-

gram under section 202 for protecting sensitive personally identifiable information.

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

(1) FINANCIAL INSTITUTIONS.—A financial institution subject to the data security requirements and standards under 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) and subject to the jurisdiction of an agency or authority described in section 505(a) of the Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)), if the Federal functional regulator (as defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809)) with jurisdiction over that financial institution has issued a regulation under title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) that requires financial institutions within its jurisdiction to provide notification to individuals following a breach of security.

(2) HIPAA REGULATED ENTITIES.—

(A) COVERED ENTITIES.—A business entity 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.

(B) COMPLIANCE.—A business entity that—

(i) is acting as a business associate, as that term is defined under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.) and is in compliance with the requirements imposed under that Act and implementing regulations promulgated under that Act; and

(ii) is subject to, and currently in compliance, with the privacy and data security requirements under sections 13401 and 13404 of division A of the American Reinvestment and Recovery Act of 2009 (42 U.S.C. 17931 and 17934) and implementing regulations promulgated under such sections.

(3) SERVICE PROVIDERS.—A service provider for any electronic communication by a third-party, to the extent that the service provider is exclusively engaged in the transmission, routing, or temporary, intermediate, or transient storage of that communication.

(4) PUBLIC RECORDS.—Public records not otherwise subject to a confidentiality or nondisclosure requirement, or information obtained from a public

record, including information obtained from a news report or periodical.

(d) RULE OF CONSTRUCTION.—Nothing in this subtitle shall be construed to modify, limit, or supersede the operation of the provisions of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), or its implementing regulations, including such regulations adopted or enforced by the States.

SEC. 202. REQUIREMENTS FOR A PERSONAL DATA PRIVACY AND SECURITY PROGRAM.

(a) PERSONAL DATA PRIVACY AND SECURITY PROGRAM.—A business entity subject to this subtitle shall comply with the following safeguards and any other administrative, technical, or physical safeguards identified by the Federal Trade Commission in a rulemaking process pursuant to section 553 of title 5, United States Code, for the protection of sensitive personally identifiable information:

(1) SCOPE.—A business entity shall implement a comprehensive personal data privacy and security program 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 sensitive personally identifiable information;

(B) protect against any anticipated vulnerabilities to the privacy, security, or integrity of sensitive personally identifiable information; and

(C) protect against unauthorized access to or use of sensitive personally identifiable information that could create a significant risk of harm 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 alteration of sensitive personally identifiable information or systems containing sensitive personally identifiable information;

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

(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 sensitive personally identifiable information; and

(D) assess the vulnerability of sensitive personally identifiable information during destruction and disposal of such information, including through the disposal or retirement of hardware.

(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 sensitive personally identifiable information, including controls to authenticate and permit access only to authorized individuals;

(ii) detect, record, and preserve information relevant to actual and attempted fraudulent, unlawful, or unauthorized access, disclosure, use, or alteration of sen-

sitive personally identifiable information, including by employees and other individuals otherwise authorized to have access;

(iii) protect sensitive personally identifiable information during use, transmission, storage, and disposal by encryption, redaction, or access controls that are widely accepted as an effective industry practice or industry standard, 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);

(iv) ensure that sensitive personally identifiable information is properly destroyed and disposed of, including during the destruction of computers, diskettes, and other electronic media that contain sensitive personally identifiable information;

(v) trace access to records containing sensitive personally identifiable information so that the business entity can determine who accessed or acquired such sensitive per-

sonally identifiable information pertaining to specific individuals;

(vi) ensure that no third party or customer of the business entity is authorized to access or acquire sensitive personally identifiable information without the business entity first performing sufficient due diligence to ascertain, with reasonable certainty, that such information is being sought for a valid legal purpose; and

(vii) minimize the amount of personal information maintained by the business entity, providing for the retention of such personal information only as reasonably needed for the business purposes of the business entity or as necessary to comply with any other provision of law.

(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) CERTAIN RELATIONSHIP TO PROVIDERS OF SERVICES.—In the event a business entity subject to this subtitle engages a person or entity not subject to this subtitle (other than a service provider) to receive sensitive personally identifiable information in performing services or functions (other than the services or functions provided by a service provider) on behalf of and under the instruction of such business entity, such business entity shall—

(1) exercise appropriate due diligence in selecting the person or entity for responsibilities related to sensitive personally identifiable information, and take reasonable steps to select and retain a person or entity that is capable of maintaining appropriate safeguards for the security, privacy, and integrity of the sensitive personally identifiable information at issue; and

(2) require the person or entity by contract to implement and maintain appropriate measures de-

signed to meet the objectives and requirements governing entities subject to section 201, this section, 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 sensitive personally identifiable information;

(3) internal or external threats to sensitive 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 sensitive personally identifiable information systems.

(f) IMPLEMENTATION TIMELINE.—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. 203. FEDERAL ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) IN GENERAL.—The Attorney General may bring a civil action in the appropriate United States district court against any business entity that engages in conduct constituting a violation of this subtitle and, upon proof of such conduct by a preponderance of the evidence, such business entity shall be subject to a civil penalty of not more than $5,000 per violation per day while such a violation exists, with a maximum of $20,000,000 per violation, unless such conduct is found to be willful or intentional.

(2) INTENTIONAL OR WILLFUL VIOLATION.—A business entity that intentionally or willfully violates the provisions of this subtitle shall be subject to additional penalties in the amount of $5,000 per violation per day while such a violation exists.

(3) CONSIDERATIONS.—In determining the amount of a civil penalty under this subsection, the court shall take into account—

(A) the degree of culpability of the business entity;

(B) any prior violations of this subtitle by the business entity;

(C) the ability of the business entity to pay a civil penalty;

(D) the effect on the ability of the business entity to continue to do business;

(E) the number of individuals whose sensitive personally identifiable information was compromised by the breach;

(F) the relative cost of compliance with this subtitle; and

(G) such other matters as justice may require.

(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—If it appears that a business entity has engaged, or is engaged, in any act or practice constituting a violation of this subtitle, the Attorney General may petition an appropriate district court of the United States for an order—

(A) enjoining such act or practice; or

(B) enforcing compliance with this subtitle.

(2) ISSUANCE OF ORDER.—A court may issue an order under paragraph (1), if the court finds that the

conduct in question constitutes a violation of this subtitle.

(c) 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.

SEC. 204. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) CIVIL ACTIONS.—

(1) IN GENERAL.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the acts or practices of a business entity that violate 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; or

(C) obtain civil penalties of not more than $5,000 per violation per day while such viola-

tions persist, up to a maximum of $20,000,000 per violation.

(2) CONSIDERATIONS.—In determining the amount of a civil penalty under this subsection, the court shall take into account—

(A) the degree of culpability of the business entity;

(B) any prior violations of this subtitle by the business entity;

(C) the ability of the business entity to pay a civil penalty;

(D) the effect on the ability of the business entity to continue to do business;

(E) the number of individuals whose sensitive personally identifiable information was compromised by the breach;

(F) the relative cost of compliance with this subtitle; and

(G) such other matters as justice may require.

(3) 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 in subparagraph (B), the attorney general of a State shall provide the written notice and a copy of the complaint to the Attorney General as soon after the filing of the complaint as practicable.

(b) FEDERAL PROCEEDINGS.—Upon receiving notice under subsection (a)(3), the Attorney General shall have the right to—

(1) move to stay the action, pending the final disposition of a pending Federal proceeding or action described in subsection (c);

(2) initiate an action in the appropriate United States district court under section 218 and move to

consolidate all pending actions, including State actions, in such court;

(3) intervene in an action brought under subsection (a)(2); and

(4) file petitions for appeal.

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

(d) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this section 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—

(1) conduct investigations;

(2) administer oaths or affirmations; or

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

(e) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in—

(A) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(B) another court of competent jurisdiction.

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

(A) is an inhabitant; or

(B) may be found.

SEC. 205. SUPPLEMENTAL ENFORCEMENT BY INDIVIDUALS.

(a) IN GENERAL.—Any person aggrieved by a violation of the provisions of this subtitle by a business entity may bring a civil action in a court of appropriate jurisdiction to recover for personal injuries sustained as a result of the violation.

(b) AUTHORITY TO BRING CIVIL ACTION; JURISDICTION.—As provided in subsection (c), any person may commence a civil action on his own behalf against any business entity who is alleged to have violated the provisions of this subtitle.

(c) REMEDIES IN A CITIZEN SUIT.—

(1) DAMAGES.—Any individual harmed by a failure of a business entity to comply with the provisions of this subtitle, shall be able to collect damages

of not more than $10,000 per violation per day while such violations persist, up to a maximum of $20,000,000 per violation.

(2) PUNITIVE DAMAGES.—A business entity may be liable for punitive damages if the business entity intentionally or willfully violates the provisions of this subtitle.

(3) EQUITABLE RELIEF.—A business entity that violates the provisions of this subtitle may be enjoined to comply with the provisions of those sections.

(d) 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.

(e) NONENFORCEABILITY OF CERTAIN PROVISIONS WAIVING RIGHTS AND REMEDIES OR REQUIRING ARBITRATION OF DISPUTES.—

(1) WAIVER OF RIGHTS AND REMEDIES.—The rights and remedies provided for in this section may not be waived by any agreement, policy form, or condition of employment including by a predispute arbitration agreement.

(2) PREDISPUTE ARBITRATION AGREEMENTS.—No predispute arbitration agreement shall be valid or

enforceable, if the agreement requires arbitration of a dispute arising under this section.

(f) CONSIDERATIONS.—In determining the amount of a civil penalty under this subsection, the court shall take into account—

(1) the degree of culpability of the business entity;

(2) any prior violations of this subtitle by the business entity;

(3) the ability of the business entity to pay a civil penalty;

(4) the effect on the ability of the business entity to continue to do business;

(5) the number of individuals whose sensitive personally identifiable information was compromised by the breach;

(6) the relative cost of compliance with this subtitle; and

(7) such other matters as justice may require.

Subtitle B—Security Breach Notification

SEC. 211. NOTICE TO INDIVIDUALS.

(a) IN GENERAL.—Any agency, or business entity engaged in interstate commerce other than a service provider, that uses, accesses, transmits, stores, disposes of or collects

sensitive personally identifiable information that experiences a security breach of such information, shall, following the discovery of such security breach of such information, notify any resident of the United States whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed, or acquired.

(b) OBLIGATION OF OWNER OR LICENSEE.—

(1) NOTICE TO OWNER OR LICENSEE.—Any agency, or business entity engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information that the agency or business entity does not own or license shall notify the owner or licensee of the information following the discovery of a security breach involving such information.

(2) NOTICE BY OWNER, LICENSEE OR OTHER DESIGNATED THIRD PARTY.—Nothing in this subtitle shall prevent or abrogate an agreement between an agency or business entity required to give notice under this section and a designated third party, including an owner or licensee of the sensitive personally identifiable information subject to the security breach, to provide the notifications required under subsection (a).

(3) BUSINESS ENTITY RELIEVED FROM GIVING NOTICE.—A business entity obligated to give notice under subsection (a) shall be relieved of such obligation if an owner or licensee of the sensitive personally identifiable information subject to the security breach, or other designated third party, provides such notification.

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

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—All notifications required under this section shall be made without unreasonable

delay following the discovery by the agency or business entity of a security breach.

(2) REASONABLE DELAY.—Reasonable delay under this subsection may include any time necessary to determine the scope of the security breach, conduct the risk assessment described in section 212(b)(1), and provide notice to law enforcement when required.

(3) BURDEN OF PRODUCTION.—The agency, business entity, owner, or licensee required to provide notice under this subtitle shall, upon the request of the Attorney General, the Federal Trade Commission, or the attorney general of a State or any State or local law enforcement agency authorized by the attorney general of the State or by State statute to prosecute violations of consumer protection law, provide records or other evidence of the notifications required under this subtitle, including to the extent applicable, the reasons for any delay of notification.

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

(1) IN GENERAL.—If a Federal law enforcement agency or member of the intelligence community determines that the notification required under this section would impede any lawfully authorized criminal investigation or authorized investigative, protective,

or intelligence activities that are carried out by or on behalf of any element of the intelligence community and conducted in accordance with the United States laws, authorities, and regulations governing such intelligence activities, such notification shall be delayed upon written notice from such Federal law enforcement agency or member of the intelligence community to the agency or business entity that experienced the breach. The notification shall specify in writing the period of delay required.

(2) EXTENDED DELAY OF NOTIFICATION.—If the notification required under subsection (a) is delayed pursuant to paragraph (1), an agency or business entity shall give notice 30 days after the day such law enforcement delay was invoked unless a Federal law enforcement or member of the intelligence community provides written notification that further delay is necessary.

(3) LAW ENFORCEMENT IMMUNITY.—No non-constitutional cause of action shall lie in any court against an agency for acts relating to the delay of notification for law enforcement or intelligence purposes under this subtitle.

SEC. 212. EXEMPTIONS FROM NOTICE TO INDIVIDUALS.

(a) EXEMPTION FOR NATIONAL SECURITY AND LAW ENFORCEMENT.—

(1) IN GENERAL.—Section 211 shall not apply to an agency or business entity if—

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

(B) the Federal Bureau of Investigation determines that notification of the security breach could be expected to cause damage to national security.

(2) IMMUNITY.—No non-constitutional cause of action shall lie in any court against any Federal agency for acts relating to the exemption from notification under this subtitle.

(b) SAFE HARBOR.—

(1) IN GENERAL.—An agency or business entity shall be exempt from the notice requirements under section 211, if—

(A) a risk assessment conducted by the agency or business entity, in consultation with the Federal Trade Commission, concludes that

there is no significant risk that a security breach has resulted in, or will result in harm to the individuals whose sensitive personally identifiable information was subject to the security breach; and

(B) the Federal Trade Commission or designated entity does not indicate within 7 business days from the receipt of written notification from an agency or business entity pursuant to subsection 212 (b)(2), that the agency or business entity should not be exempt from the notice requirements of section 211.

(2) RISK ASSESSMENT REQUIREMENTS.—

(A) CONDUCTING A RISK ASSESSMENT.—Upon discovery of a security breach of an agency or business entity, the agency or business entity shall conduct a risk assessment to determine if there is a significant risk that the security breach resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach.

(i) PRESUMPTION OF NO SIGNIFICANT RISK.—It is presumed that there is no significant risk that the security breach has re-

sulted in, or will result in, harm to the individuals whose sensitive personally identifiable data was subject to the security breach, if the sensitive personally identifiable information has been rendered unusable, unreadable, or indecipherable through a security technology or methodology (if the technology or methodology is generally accepted by experts in the information security field). Any such presumption may be rebutted by facts demonstrating that the security technologies or methodologies in a specific case, have been or are reasonably likely to be compromised.

(ii) PRESUMPTION OF SIGNIFICANT RISK.—It is presumed that there is a significant risk that the security breach has resulted in, or will result in, harm to individuals whose sensitive personally identifiable information was subject to the security breach if the agency or business entity failed to render such sensitive personally identifiable information indecipherable through a security technology or methodology (if the technology or methodology is

generally accepted by experts in the information security field).

(iii) METHODOLOGIES OR TECHNOLOGIES.—

(I) REQUIRED RULEMAKING.—Not later than 1 year after the date of the enactment of this Act, and biannually thereafter, the Federal Trade Commission, after consultation with the National Institute of Standards and Technology, shall issue rules (pursuant to section 553 of title 5, United States Code) or guidance to identify security methodologies or technologies, such as encryption, which render sensitive personally identifiable information unusable, unreadable, or indecipherable, that shall, if applied to such sensitive personally identifiable information, establish a presumption that no significant risk of harm exists to individuals whose sensitive personally identifiable information was subject to a security breach. Any such presumption may be rebutted by facts demonstrating that

any such methodology or technology in a specific case has been or is reasonably likely to be compromised.

(II) REQUIRED CONSULTATION.—In issuing rules or guidance under subclause (II), the Commission shall also consult with relevant industries, consumer organizations, and data security and identity theft prevention experts and established standards setting bodies.

(iv) FTC GUIDANCE.—Not later than 1 year after the date of the enactment of this Act, the Federal Trade Commission, after consultation with the National Institute of Standards and Technology, shall issue guidance regarding the application of the exemption in clause (i).

(B) WRITTEN NOTIFICATION.—Without unreasonable delay, but not later than 7 days after the discovery of a security breach, unless extended by the United States Secret Service or the Federal Bureau of Investigation, the agency or business entity must notify the Federal Trade

Commission and designated entity, in writing, of—

(i) the results of the risk assessment; and

(ii) its decision to invoke the risk assessment exemption.

(C) VIOLATIONS.—It shall be a violation of this section to—

(i) fail to conduct a risk assessment in a reasonable manner, or according to standards generally accepted by experts in the field of information security; or

(ii) submit results of a risk assessment that—

(I) conceal violations of law, inefficiency, or administrative error;

(II) prevent embarrassment to a business entity, organization, or agency;

(III) restrain competition;

(IV) contain fraudulent or deliberately misleading information; or

(V) delay notification under section 211 for any other reason, except where the agency or business entity

reasonably believes that the risk assessment exception may apply.

(c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

(1) IN GENERAL.—A business entity shall be exempt from the notice requirements of this subtitle if the business entity utilizes or participates in a security program that—

(A) effectively blocks the use of the sensitive personally identifiable information to initiate unauthorized financial transactions before they are charged to the account of the individual; and

(B) provides for notice to affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

(2) LIMITATION.—Paragraph (1) shall not apply to a business entity if the information subject to the security breach includes an individual's first and last name, or any other type of sensitive personally identifiable information, other than a credit card or credit card security code identified in section 3, unless that information is only a credit card number or a credit card security code.

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

(1) FINANCIAL INSTITUTIONS.—A financial institution subject to the data security requirements and standards under 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), and subject to the jurisdiction of an agency or authority described in section 505(a) of the Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)), if the Federal functional regulator (as defined by section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809)) with jurisdiction over that financial institution has issued a regulation under title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) that requires financial institutions within its jurisdiction to provide notification to individuals following a breach of security.

(2) HIPAA REGULATED ENTITIES EXEMPTION.—

(A) IN GENERAL.—A business entity shall be exempt from the notice requirement under section 211 if the business entity is one of the following:

(i) COVERED ENTITIES.—A business entity subject to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.), including the data breach notification requirements and implementing regulations of that Act.

(ii) BUSINESS ENTITIES.—A business entity that—

(I) is acting as a business associate, as that term is defined under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.) and is in compliance with the requirements imposed under that Act and implementing regulations promulgated under that Act; and

(II) is subject to, and currently in compliance with, the data breach notification requirements under section 13402 or 13407 of the American Reinvestment and Recovery Act of 2009 (42 U.S.C. 17932 and 17937) and implementing regulations promulgated under such sections.

(B) LIMITATION.—Paragraph (1) shall not apply to a business entity if the information subject to the security breach includes an individual's first and last name, or any other type of sensitive personally identifiable information other than a health insurance policy or subscriber identification number or information re-

garding an individual's medical history, mental or physical medical condition, or medical treatment or diagnosis by a health care professional as identified in section 3 unless that information is only a health insurance policy or subscriber identification number or information regarding an individual's medical history, mental or physical medical condition, or medical treatment or diagnosis by a health care professional.

SEC. 213. METHODS OF NOTICE TO INDIVIDUALS.

To comply with section 211, an agency or business entity shall provide the following forms of notice:

(1) INDIVIDUAL WRITTEN NOTICE.—Written notice to individuals by 1 of the following means:

(A) Individual written notification to the last known home mailing address of the individual in the records of the agency or business entity.

(B) E-mail notice, unless the individual has expressly opted not to receive such notices of security breaches or the notice is inconsistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).

(2) TELEPHONE NOTICE.—Telephone notice to the individual personally.

(3) PUBLIC NOTICE.—

(A) ELECTRONIC NOTICE.—Prominent notice via all reasonable means of electronic contact between the individual and the agency or business entity, including any website, networked devices, or other interface through which the agency or business entity regularly interacts with the consumer, if the number of individuals whose sensitive personally identifiable information was or is reasonably believed to have been accessed or acquired by an unauthorized person exceeds 5,000.

(B) MEDIA NOTICE.—Notice to major media outlets serving a State or jurisdiction, if the number of residents of such State whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person exceeds 5,000.

SEC. 214. CONTENT OF NOTICE TO INDIVIDUALS.

(a) IN GENERAL.—Regardless of the method by which individual notice is provided to individuals under section 213(1), such notice shall include—

(1) a description of the categories of sensitive personally identifiable information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, and how the agency or business entity came into possession of the sensitive personally identifiable information at issue;

(2) a toll-free number—

(A) that the individual may use to contact the agency or business entity, or the agent of the agency or business entity; and

(B) from which the individual may learn what types of sensitive personally identifiable information the agency or business entity maintained about that individual;

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

(4) the telephone numbers and websites for the relevant Federal agencies that provide information regarding identity theft prevention and protection;

(5) notice that the individual is entitled to receive, at no cost to such individual, consumer credit reports on a quarterly basis for a period of 2 years, credit monitoring or any other service that enables consumers to detect the misuse of sensitive personally

identifiable information for a period of 2 years, and instructions to the individual on requesting such reports or service from the agency or business entity;

(6) notice that the individual is entitled to receive a security freeze and that the agency or business entity will be liable for any costs associated with the security freeze for 2 years and the necessary instructions for requesting a security freeze; and

(7) notice that any costs or damages incurred by an individual as a result of a security breach will be paid by the business entity or agency that experienced the security breach.

(b) TELEPHONE NOTICE.—Telephone notice described in section 213(2) shall include, to the extent possible—

(1) notification that a security breach has occurred and that the individual's sensitive personally identifiable information may have been compromised;

(2) a description of the categories of sensitive personally identifiable information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person;

(3) a toll-free number and website—

(A) that the individual may use to contact the agency or business entity, or the authorized agent of the agency or business entity; and

(B) from which the individual may learn what types of sensitive personally identifiable information the agency or business entity maintained about that individual and remedies available to that individual; and

(4) an alert to the individual that the agency or business entity is sending or has sent written notification containing additional information as required under section 213(1)(A).

(c) PUBLIC NOTICE.—Public notice described in section 213(3) shall include—

(1) electronic notice, which includes—

(A) notification that a security breach has occurred and that the individual's sensitive personally identifiable information may have been compromised;

(B) a description of the categories of sensitive personally identifiable information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person; and

(C) a toll-free number and website—

(i) that the individual may use to contact the agency or business entity, or the

authorized agent of the agency or business entity; and

(ii) from which the individual may learn what types of sensitive personally identifiable information the agency or business entity maintained about that individual and remedies available to that individual;

(2) media notice, which includes—

(A) a description of the categories of sensitive personally identifiable information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person;

(B) a toll-free number—

(i) that the individual may use to contact the agency or business entity, or the authorized agent of the agency or business entity; and

(ii) from which the individual may learn what types of sensitive personally identifiable information the agency or business entity maintained about that individual and remedies available to that individual;

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

(D) the telephone numbers and websites for the relevant Federal agencies that provide information regarding identity theft prevention and protection;

(E) notice that the affected individuals are entitled to receive, at no cost to such individuals, consumer credit reports on a quarterly basis for a period of 2 years, credit monitoring, or any other service that enables consumers to detect the misuse of sensitive personally identifiable information for a period of 2 years;

(F) notice that the individual is entitled to receive a security freeze and that the agency or business entity will be liable for any costs associated with the security freeze for 2 years; and

(G) notice that the individual is entitled to receive compensation from the business entity or agency for any costs or damages incurred by the individual resulting from the security breach.

(d) ADDITIONAL CONTENT.—Notwithstanding section 221, a State may require that a notice under subsection

(a) shall also include information regarding victim protection assistance provided for by that State.

(e) DIRECT BUSINESS RELATIONSHIP.—Regardless of whether a business entity, agency, or a designated third party provides the notice required pursuant to section 211(b), such notice shall include the name of the business entity or agency that has a direct relationship with the individual being notified.

SEC. 215. REMEDIES FOR SECURITY BREACH.

(a) CREDIT REPORTS AND CREDIT MONITORING.—An agency or business entity required to provide notification under this subtitle shall, upon request of an individual whose sensitive personally identifiable information was included in the security breach, provide or arrange for the provision of, to each such individual and at no cost to such individual—

(1) consumer credit reports from not fewer than 1 of the major credit reporting agencies beginning not later than 60 days following the request of the individual and continuing on a quarterly basis for a period of 2 years thereafter; and

(2) a credit monitoring or other service that enables consumers to detect the misuse of their personal information, beginning not later than 60 days fol-

lowing the request of the individual and continuing for a period of 2 years.

(b) SECURITY FREEZE.—

(1) REQUEST.—Any consumer may submit a written request, by certified mail or such other secure method as authorized by a credit rating agency, to a credit rating agency to place a security freeze on the credit report of the consumer.

(2) IMPLEMENTATION OF SECURITY FREEZE.—Upon receipt of a written request under paragraph (1), a credit rating agency shall—

(A) not later than 5 business days after receipt of the request, place a security freeze on the credit report of the consumer; and

(B) not later than 10 business days after placing a security freeze, send a written confirmation of such security freeze to the consumer, which shall provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of the credit report of the consumer to a third party or for a specified period of time.

(3) DURATION OF SECURITY FREEZE.—Except as provided in paragraph (4), any security freeze au-

thorized pursuant to the provisions of this section shall remain in effect until the consumer requests security freeze to be removed.

(4) DISCLOSURE OF CREDIT REPORT TO THIRD PARTY.—

(A) IN GENERAL.—If a consumer that has requested a security freeze under this subsection wishes to authorize the disclosure of the credit report of the consumer to a third party, or for a specified period of time, while such security freeze is in effect, the consumer shall contact the credit rating agency and provide—

(i) proper identification;

(ii) the unique personal identification number or password described in paragraph (2)(B); and

(iii) proper information regarding the third party who is to receive the credit report or the time period for which the credit report shall be available.

(B) REQUIREMENT.—Not later than 3 business days after receipt of a request under subparagraph (A), a credit rating agency shall lift the security freeze.

(5) PROCEDURES.—

(A) IN GENERAL.—A credit rating agency shall develop procedures to receive and process requests from consumers under paragraph (2) of this section.

(B) REQUIREMENT.—Procedures developed under subparagraph (A), at a minimum, shall include the ability of a consumer to send such temporary lift or removal request by electronic mail, letter, telephone, or facsimile.

(6) REQUESTS BY THIRD PARTY.—If a third party requests access to a credit report of a consumer that has been frozen under this subsection and the consumer has not authorized the disclosure of the credit report of the consumer to the third party, the third party may deem such credit application as incomplete.

(7) DETERMINATION BY CREDIT RATING AGENCY.—

(A) IN GENERAL.—A credit rating agency may refuse to implement or may remove a security freeze under this subsection if the agency determines, in good faith, that—

(i) the request for a security freeze was made as part of a fraud that the consumer participated in, had knowledge of, or that

can be demonstrated by circumstantial evidence; or

(ii) the consumer credit report was frozen due to a material misrepresentation of fact by the consumer.

(B) NOTICE.—If a credit rating agency makes a determination under subparagraph (A) to not implement, or to remove, a security freeze under this subsection, the credit rating agency shall notify the consumer in writing of such determination—

(i) in the case of a determination not to implement a security freeze, not later than 5 business days after the determination is made; and

(ii) in the case of a removal of a security freeze, prior to removing the freeze on the credit report of the consumer.

(8) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to prohibit disclosure of a credit report of a consumer to—

(A) a person, or the person's subsidiary, affiliate, agent or assignee with which the consumer has or, prior to assignment, had an account, contract or debtor-creditor relationship for

the purpose of reviewing the account or collecting the financial obligation owing for the account, contract or debt;

(B) a subsidiary, affiliate, agent, assignee or prospective assignee of a person to whom access has been granted under paragraph (4) for the purpose of facilitating the extension of credit or other permissible use;

(C) any person acting pursuant to a court order, warrant or subpoena;

(D) any person for the purpose of using such credit information to prescreen as provided by the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(E) any person for the sole purpose of providing a credit file monitoring subscription service to which the consumer has subscribed;

(F) a credit rating agency for the sole purpose of providing a consumer with a copy of the credit report of the consumer upon the request of the consumer; or

(G) a Federal, State or local governmental entity, including a law enforcement agency, or court, or their agents or assignees pursuant to their statutory or regulatory duties. For purposes

of this subsection, "reviewing the account" includes activities related to account maintenance, monitoring, credit line increases and account upgrades and enhancements; and

(H) any person for the sole purpose of providing a remedy requested by an individual under this section.

(9) EXCEPTIONS.—The following persons shall not be required to place a security freeze under this subsection, but shall be subject to any security freeze placed on a credit report by another credit rating agency:

(A) A check services or fraud prevention services company that reports on incidents of fraud or issues authorizations for the purpose of approving or processing negotiable instruments, electronic fund transfers or similar methods of payment.

(B) A deposit account information service company that issues reports regarding account closures due to fraud, substantial overdrafts, automated teller machine abuse, or similar information regarding a consumer to inquiring banks or other financial institutions for use only in re-

viewing a consumer request for a deposit account at the inquiring bank or financial institution.

(C) A credit rating agency that—

(i) acts only to resell credit information by assembling and merging information contained in a database of 1 or more credit reporting agencies; and

(ii) does not maintain a permanent database of credit information from which new credit reports are produced.

(10) FEES.—

(A) IN GENERAL.—A credit rating agency may charge reasonable fees for each security freeze, removal of such freeze or temporary lift of such freeze for a period of time, and a temporary lift of such freeze for a specific party.

(B) REQUIREMENT.—Any fees charged under subparagraph (A) shall be borne by the agency or business entity providing notice under section 214 for 2 years following the establishment of the security freeze under this subsection.

(c) COSTS RESULTING FROM A SECURITY BREACH.—

(1) IN GENERAL.—A business entity or agency that experiences a security breach and is required to provide notice under this subtitle shall pay, upon re-

quest, to any individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed or acquired as a result of such security breach, any costs or damages incurred by the individual as a result of such security breach, including costs associated with identity theft suffered as a result of such security breach.

(2) COMPLIANCE.—A business entity or agency shall be deemed in compliance with this subsection if the business entity or agency—

(A) provides insurance to any individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed or acquired as a result of a security breach and such insurance is sufficient to compensate the consumer for not less than $25,000 of costs or damages; or

(B) pays, without unreasonable delay, any actual costs or damages incurred by an individual as a result of the security breach.

SEC. 216. NOTICE TO CREDIT REPORTING AGENCIES.

If an agency or business entity is required to provide notification to more than 5,000 individuals under section 211(a), the agency or business entity shall also notify all consumer reporting agencies that compile and maintain

files on consumers on a nationwide basis (as defined in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)) of the timing and distribution of the notices. Such notice shall be given to the consumer credit reporting agencies without unreasonable delay and, if it will not delay notice to the affected individuals, prior to the distribution of notices to the affected individuals.

SEC. 217. NOTICE TO LAW ENFORCEMENT.

(a) DESIGNATION OF A GOVERNMENT ENTITY TO RECEIVE NOTICE.—

(1) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, the Secretary of Homeland Security, in consultation with the Attorney General, shall designate a Federal Government entity to receive the information required to be submitted under this subtitle, and any other reports and information about information security incidents, threats, and vulnerabilities.

(2) RESPONSIBILITIES OF THE DESIGNATED ENTITY.—The designated entity shall—

(A) be responsible for promptly providing the information it receives to the United States Secret Service and the Federal Bureau of Investigation, and to the Federal Trade Commission for civil law enforcement purposes; and

(B) provide the information described in subparagraph (A) as appropriate to other Federal agencies for law enforcement, national security, or data security purposes.

(b) NOTICE.—Any business entity or agency shall notify the designated entity of the fact that a security breach has occurred if—

(1) the number of individuals whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person exceeds 5,000;

(2) the security breach involves a database, networked or integrated databases, or other data system containing the sensitive personally identifiable information of more than 500,000 individuals nationwide;

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

(4) the security breach involves primarily sensitive personally identifiable information of individuals known to the agency or business entity to be employees and contractors of the Federal Government involved in national security or law enforcement.

(c) FTC REVIEW OF THRESHOLDS.—

(1) REVIEW.—Not later than 1 year after the date of enactment of this Act, the Federal Trade Commission, in consultation with the Attorney General and the Secretary of Homeland Security, shall promulgate regulations regarding the reports required under subsection (a).

(2) RULEMAKING.—The Federal Trade Commission, in consultation with the Attorney General and the Secretary of Homeland Security, after notice and the opportunity for public comment, and in a manner consistent with this section, shall promulgate regulations, as necessary, under section 553 of title 5, United States Code, to adjust the thresholds for notice to law enforcement and national security authorities under subsection (a) and to facilitate the purposes of this section.

(d) TIMING OF NOTICES.—The notices required under this section shall be delivered as follows:

(1) Notice under subsection (a) shall be delivered as promptly as possible, but not later than 10 days after discovery of the security breach.

(2) Notice under section 211 shall be delivered to individuals not later than 48 hours after the Federal Bureau of Investigation or the Secret Service receives

notice of a security breach from an agency or business entity.

SEC. 218. FEDERAL ENFORCEMENT.

(a) CIVIL ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—The Attorney General may bring a civil action in the appropriate United States district court against any business entity that engages in conduct constituting a violation of this subtitle and, upon proof of such conduct by a preponderance of the evidence, such business entity shall be subject to a civil penalty of not more than $500 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $20,000,000 per violation, unless such conduct is found to be willful or intentional.

(2) PRESUMPTION.—A violation of section 212(b)(2)(C) shall be presumed to be willful or intentional conduct.

(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—If it appears that a business entity has engaged, or is engaged, in any act or practice constituting a violation of this subtitle, the Attor-

ney General may petition an appropriate district court of the United States for an order—

(A) enjoining such act or practice; or

(B) enforcing compliance with this subtitle.

(2) ISSUANCE OF ORDER.—A court may issue an order under paragraph (1), if the court finds that the conduct in question constitutes a violation of this subtitle.

(c) CIVIL ACTIONS BY THE FEDERAL TRADE COMMISSION.—

(1) IN GENERAL.—Compliance with the requirements imposed under this subtitle may be enforced under the Federal Trade Commission Act (15 U.S.C. 41 et seq.) by the Federal Trade Commission with respect to business entities subject to this Act. All of the functions and powers of the Federal Trade Commission under the Federal Trade Commission Act are available to the Commission to enforce compliance by any person with the requirements imposed under this title.

(2) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—For the purpose of the exercise by the Federal Trade Commission of its functions and powers under the Federal Trade Commission Act, a violation of any requirement or prohibition imposed under this title

shall constitute an unfair or deceptive act or practice in commerce in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(I)(B)) regarding unfair or deceptive acts or practices and shall be subject to enforcement by the Federal Trade Commission under that Act with respect to any business entity, irrespective of whether that business entity is engaged in commerce or meets any other jurisdictional tests in the Federal Trade Commission.

(d) CONSIDERATIONS.—In determining the amount of a civil penalty under this subsection, the court shall take into account—

(1) the degree of culpability of the business entity;

(2) any prior violations of this subtitle by the business entity;

(3) the ability of the business entity to pay a civil penalty;

(4) the effect on the ability of the business entity to continue to do business;

(5) the number of individuals whose sensitive personally identifiable information was compromised by the breach;

(6) the relative cost of compliance with this subtitle; and

(7) such other matters as justice may require.

(e) COORDINATION OF ENFORCEMENT.—

(1) IN GENERAL.—Before opening an investigation, the Federal Trade Commission shall consult with the Attorney General.

(2) LIMITATION.—The Federal Trade Commission may initiate investigations under this subsection unless the Attorney General determines that such an investigation would impede an ongoing criminal investigation or national security activity.

(3) COORDINATION AGREEMENT.—

(A) IN GENERAL.—In order to avoid conflicts and promote consistency regarding the enforcement and litigation of matters under this Act, not later than 180 days after the enactment of this Act, the Attorney General and the Commission shall enter into an agreement for coordination regarding the enforcement of this Act.

(B) REQUIREMENT.—The coordination agreement entered into under subparagraph (A) shall include provisions to ensure that parallel investigations and proceedings under this section are conducted in a manner that avoids conflicts

and does not impede the ability of the Attorney General to prosecute violations of Federal criminal laws.

(4) COORDINATION WITH THE FCC.—If an enforcement action under this Act relates to customer proprietary network information, the Federal Trade Commission shall coordinate the enforcement action with the Federal Communications Commission.

(f) RULEMAKING.—The Federal Trade Commission may, in consultation with the Attorney General, issue such other regulations as it determines to be necessary to carry out this subtitle. All regulations promulgated under this Act shall be issued in accordance with section 553 of title 5, United States Code. Where regulations relate to customer proprietary network information, the promulgation of such regulations will be coordinated with the Federal Communications Commission.

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

(h) FRAUD ALERT.—Section 605A(b)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681c–1(b)(1)) is amended by inserting ", or evidence that the consumer has received

notice that the consumer's financial information has or may have been compromised," after "identity theft report".

SEC. 219. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) IN GENERAL.—

(1) CIVIL ACTIONS.—

(A) IN GENERAL.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of a business entity in a practice that is prohibited under this subtitle, the State or the State or local law enforcement agency on behalf of the residents of the agency's jurisdiction, may bring a civil action on behalf of the residents of the State or jurisdiction in a district court of the United States of appropriate jurisdiction or any other court of competent jurisdiction, including a State court, to—

(i) enjoin that practice;

(ii) enforce compliance with this subtitle; or

(iii) obtain civil penalties of not more than $500 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $20,000,000 per violation, unless such conduct is found to be willful or intentional.

(B) PRESUMPTION.—A violation of section 212(b)(2)(C) shall be presumed to be willful or intentional.

(2) CONSIDERATIONS.—In determining the amount of a civil penalty under this subsection, the court shall take into account—

(A) the degree of culpability of the business entity;

(B) any prior violations of this subtitle by the business entity;

(C) the ability of the business entity to pay a civil penalty;

(D) the effect on the ability of the business entity to continue to do business;

(E) the number of individuals whose sensitive personally identifiable information was compromised by the breach;

(F) the relative cost of compliance with this subtitle; and

(G) such other matters as justice may require.

(3) NOTICE.—

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

(i) written notice of the action; and

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

(B) EXEMPTION.—

(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 subtitle, if the State attorney general determines that it is not feasible to provide the notice described in such subparagraph before the filing of the action.

(ii) NOTIFICATION.—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 State attorney general files the action.

(b) FEDERAL PROCEEDINGS.—Upon receiving notice under subsection (a)(2), the Attorney General shall have the right to—

(1) move to stay the action, pending the final disposition of a pending Federal proceeding or action;

(2) initiate an action in the appropriate United States district court under section 218 and move to consolidate all pending actions, including State actions, in such court;

(3) intervene in an action brought under subsection (a)(2); and

(4) file petitions for appeal.

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

(d) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this subtitle regarding notification shall be construed to prevent an at-

torney general of a State from exercising the powers conferred on such attorney general by the laws of that State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

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

(e) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in—

(A) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(B) another court of competent jurisdiction.

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

(A) is an inhabitant; or

(B) may be found.

SEC. 220. SUPPLEMENTAL ENFORCEMENT BY INDIVIDUALS.

(a) IN GENERAL.—Any person aggrieved by a violation of the provisions of section 211, 213, 214, 215, or 216 by a business entity may bring a civil action in a court

of appropriate jurisdiction to recover for personal injuries sustained as a result of the violation.

(b) AUTHORITY TO BRING CIVIL ACTION; JURISDICTION.—As provided in subsection (c), an individual may commence a civil action on his own behalf against any business entity who is alleged to have violated the provisions of this subtitle.

(c) REMEDIES IN A CITIZEN SUIT.—

(1) DAMAGES.—Any individual harmed by a failure of a business entity to comply with the provisions of section 211, 213, 214, 215, or 216, shall be able to collect damages of not more than $500 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $20,000,000 per violation

(2) PUNITIVE DAMAGES.—A business entity may be liable for punitive damages if it—

(A) intentionally or willfully violates the provisions of section 211, 213, 214, 215, or 216; or

(B) failed to comply with the requirements of subsections (a) through (d) of section 202.

(3) EQUITABLE RELIEF.—A business entity that violates the provisions of section 211, 213, 214, 215,

or 216 may be enjoined to provide required remedies under section 215 by a court of competent jurisdiction.

(d) 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.

(e) NONENFORCEABILITY OF CERTAIN PROVISIONS WAIVING RIGHTS AND REMEDIES OR REQUIRING ARBITRATION OF DISPUTES.—

(1) WAIVER OF RIGHTS AND REMEDIES.—The rights and remedies provided for in this section may not be waived by any agreement, policy form, or condition of employment including by a predispute arbitration agreement.

(2) PREDISPUTE ARBITRATION AGREEMENTS.—No predispute arbitration agreement shall be valid or enforceable, if the agreement requires arbitration of a dispute arising under this section.

(f) CONSIDERATIONS.—In determining the amount of a civil penalty under this subsection, the court shall take into account—

(1) the degree of culpability of the business entity;

(2) any prior violations of this subtitle by the business entity;

(3) the ability of the business entity to pay a civil penalty;

(4) the effect on the ability of the business entity to continue to do business;

(5) the number of individuals whose sensitive personally identifiable information was compromised by the breach;

(6) the relative cost of compliance with this subtitle; and

(7) such other matters as justice may require.

SEC. 221. RELATION TO OTHER LAWS.

(a) IN GENERAL.—The provisions of this subtitle shall supersede any other provision of Federal law or any provision of law of any State relating to notification by a business entity engaged in interstate commerce or an agency of a security breach, except as provided in this subsection.

(b) LIMITATIONS.—

(1) STATE COMMON LAW.—Nothing in this subtitle shall be construed to exempt any entity from liability under common law, including through the operation of ordinary preemption principles, and including liability through state trespass, contract, or

tort law, for damages caused by the failure to notify an individual following a security breach.

(2) GRAMM-LEACH-BLILEY ACT.—Nothing in this Act shall supersede the data security requirements of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), or implementing regulations based on that Act.

(3) HEALTH PRIVACY.—

(A) To the extent that a business entity acts as a covered entity or a business associate under the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17932), and has the obligation to provide breach notification under that Act or its implementing regulations, the requirements of this Act shall not apply.

(B) To the extent that a business entity acts as a vendor of personal health records, a third party service provider, or other entity subject to the Health Information Technology for Economical and Clinical Health Act (42 U.S.C. 17937), and has the obligation to provide breach notification under that Act or its implementing regulations, the requirements of this Act shall not apply.

SEC. 222. AUTHORIZATION OF APPROPRIATIONS.

There are 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. 223. REPORTING ON RISK ASSESSMENT EXEMPTIONS.

The United States Secret Service and the Federal Bureau of Investigation shall report to Congress not later than 18 months after the date of enactment of this Act, and upon the request by Congress thereafter, on—

(1) the number and nature of the security breaches described in the notices filed by those business entities invoking the risk assessment exemption under section 212(b) and the response of the United States Secret Service and the Federal Bureau of Investigation to such notices; and

(2) the number and nature of security breaches subject to the national security and law enforcement exemptions under section 212(a), provided that such report may not disclose the contents of any risk assessment provided to the United States Secret Service and the Federal Bureau of Investigation pursuant to this subtitle.

Subtitle C—Post-Breach Technical Information Clearinghouse

SEC. 230. CLEARINGHOUSE INFORMATION COLLECTION, MAINTENANCE, AND ACCESS.

(a) IN GENERAL.—The designated entity shall maintain a clearinghouse of technical information concerning system vulnerabilities identified in the wake of security breaches, which shall—

(1) contain information disclosed by agencies or business entities under subsection (b); and

(2) be accessible to certified entities under subsection (c).

(b) POST-BREACH TECHNICAL NOTIFICATION.—In any instance where an agency or business entity is required to notify the designated entity under section 217, the agency or business entity shall also provide the designated entity with technical information concerning the nature of the security breach, including—

(1) technical information regarding any system vulnerabilities of the agency or business entity revealed by or identified as a consequence of the security breach;

(2) technical information regarding any system vulnerabilities of the agency or business entity actually exploited during the security breach; and

(3) any other technical information concerning the nature of the security breach deemed appropriate for collection by the designated entity in furtherance of this subtitle.

(c) ACCESS TO CLEARINGHOUSE.—Any entity certified under subsection (d) may review information maintained by the technical information clearinghouse for the purpose of preventing security breaches that threaten the security of sensitive personally identifiable information.

(d) CERTIFICATION FOR ACCESS.—The designated entity shall issue and revoke certifications to agencies and business entities wishing to review information maintained by the technical information clearinghouse and shall establish conditions for obtaining and maintaining such certifications, including agreement that any information obtained directly or derived indirectly from the review of information maintained by the technical information clearinghouse—

(1) shall only be used to improve the security and reduce the vulnerability of networks that collect, access, transmit, use, store, or dispose of sensitive personally identifiable information;

(2) may not be used for any competitive commercial purpose; and

(3) may not be shared with any third party, including other parties certified for access to the infor-

mation clearinghouse, without the express written consent of the designated entity.

(e) RULEMAKING.—In consultation with the private sector, appropriate representatives of State and local governments, and other appropriate Federal agencies, the designated entity may issue such regulations as it determines to be necessary to carry out this subtitle. All regulations promulgated under this Act shall be issued in accordance with section 553 of title 5, United States Code.

SEC. 231. PROTECTIONS FOR CLEARINGHOUSE PARTICIPANTS.

(a) PROTECTION OF PROPRIETARY INFORMATION.—To the extent feasible, the designated entity shall ensure that any technical information disclosed to the designated entity under this subtitle shall be stored in a format designed to protect proprietary business information from inadvertent disclosure.

(b) ANONYMOUS DATA RELEASE.—To the extent feasible, the designated entity shall ensure that all information stored in the technical information clearinghouse and accessed by certified parties is presented in a form that minimizes the potential for such information to be traced to a particular network, company, or security breach incident.

(c) PROTECTION FROM PUBLIC DISCLOSURE.—Except as otherwise provided in this subtitle—

(1) security and vulnerability information collected under this section and provided to the Federal Government, including aggregated analysis and data, shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and

(2) under section 230(e), security and vulnerability-related information provided to the Federal Government under this section, including aggregated analysis and data, shall be protected from public disclosure, except that this paragraph—

(A) does not prohibit the sharing of such information, as the designated entity determines to be appropriate, in order to mitigate cybersecurity threats or further the official functions of a government agency; and

(B) does not authorized such information to be withheld from a committee of Congress authorized to request the information.

(d) PROTECTION OF CLASSIFIED INFORMATION.—Nothing in this subtitle permits the unauthorized disclosure of classified information.

SEC. 232. EFFECTIVE DATE.

This subtitle shall take effect on the expiration of the date which is 90 days after the date of enactment of this Act.

TITLE III—ACCESS TO AND USE OF COMMERCIAL DATA

SEC. 301. GENERAL SERVICES ADMINISTRATION REVIEW OF CONTRACTS.

(a) IN GENERAL.—In considering contract awards totaling more than $500,000 and entered into after the date of enactment of this Act with data brokers, the Administrator of the General Services Administration shall evaluate—

(1) the data privacy and security program of a data broker to ensure the privacy and security of data containing sensitive personally identifiable information, including whether such program adequately addresses privacy and security threats created by malicious software or code, or the use of peer-to-peer file sharing software;

(2) the compliance of a data broker with such program;

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

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

(b) COMPLIANCE SAFE HARBOR.—The data privacy and security program of a data broker shall be deemed sufficient for the purposes of subsection (a), if the data broker complies with or provides protection equal to industry standards, as identified by the Federal Trade Commission, that are applicable to the type of sensitive personally identifiable information involved in the ordinary course of business of such data broker.

(c) PENALTIES.—In awarding contracts with data brokers for products or services related to access, use, compilation, distribution, processing, analyzing, or evaluating sensitive personally identifiable information, the Administrator of the General Services Administration shall—

(1) include monetary or other penalties—

(A) for failure to comply with subtitles A and B of title II; or

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

(2) require a data broker that engages service providers not subject to subtitle A of title II for re-

sponsibilities related to sensitive personally identifiable information to—

(A) exercise appropriate due diligence in selecting those service providers for responsibilities related to sensitive personally identifiable information;

(B) take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the security, privacy, and integrity of the sensitive personally identifiable information at issue; and

(C) require such service providers, by contract, to implement and maintain appropriate measures designed to meet the objectives and requirements in title II.

(d) LIMITATION.—The penalties under subsection (c) shall not apply to a data broker providing information that is accurately and completely recorded from a public record source or licensor.

SEC. 302. 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 sensitive personally identifiable information (as that term is defined in section 3 of the Personal Data Protection and Breach Accountability Act of 2011) and ensuring remedial action to address any significant deficiencies.".

SEC. 303. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT USE OF COMMERCIAL INFORMATION SERVICES CONTAINING SENSITIVE 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";

(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 sensitive personally identifiable information from a data broker (as such terms are defined in section 3 of the Personal Data Protection and Breach Accountability Act of 2011).".

(b) LIMITATION.—Notwithstanding any other provision of law, commencing 1 year after the date of enactment of this Act, no Federal agency may enter into a contract with a data broker to access for a fee any database consisting primarily of sensitive 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 subject to the provision in that Act pertaining to sensitive information, include a description of—

(A) such database;

(B) the name of the data broker 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 sensitive personally identifiable information accessed, analyzed, or used is the minimum necessary to accomplish the intended legitimate purpose of the Federal agency;

(D) standards limiting the retention and redisclosure of sensitive 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 totaling more than $500,000, provisions—

(A) providing for penalties—

(i) for failure to comply with title II of this Act; or

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

(B) requiring a data broker that engages service providers not subject to subtitle A of title II for responsibilities related to sensitive personally identifiable information to—

(i) exercise appropriate due diligence in selecting those service providers for responsibilities related to sensitive personally identifiable information;

(ii) take reasonable steps to select and retain service providers that are capable of

maintaining appropriate safeguards for the security, privacy, and integrity of the sensitive personally identifiable information at issue; and

(iii) require such service providers, by contract, to implement and maintain appropriate measures designed to meet the objectives and requirements in title II.

(c) LIMITATION ON PENALTIES.—The penalties under subsection (b)(3)(A) shall not apply to a data broker providing information that is accurately and completely recorded from a public record source.

(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 conduct a study and audit and prepare a report on Federal agency actions to address the recommendations in the Government Accountability Office's April 2006 report on agency adherence to key privacy principles in using data brokers or commercial databases containing sensitive personally identifiable information.

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

SEC. 304. FBI REPORT ON REPORTED BREACHES AND COMPLIANCE.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, and each year thereafter, the Federal Bureau of Investigation, in coordination with the Secret Service, shall submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a report regarding any reported breaches at agencies or business entities during the preceding year.

(b) REPORT CONTENT.—Such reporting shall include—

(1) the total instances of breaches of security in the previous year;

(2) the percentage of breaches described in subsection (a) that occurred at an agency or business entity that did not comply with the personal data privacy and security program under section 202; and

(3) recommendations, if any, for modifying or amending this Act to increase its effectiveness.

SEC. 305. DEPARTMENT OF JUSTICE REPORT ON ENFORCEMENT ACTIONS.

Section 529 of title 28, United States Code, is amended by adding at the end the following:

"(c) Not later than 1 year after the date of enactment of the Personal Data Protection and Breach Accountability

Act of 2011, and every fiscal year thereafter, the Attorney General shall submit to Congress a report on Federal enforcement actions, State attorneys general enforcement actions, and private enforcement actions, undertaken pursuant to the Personal Data Protection and Breach Accountability Act of 2011 that shall include a description of the best practices for enforcement of such Act as well as recommendations, if any, for modifying or amending this Act to increase the effectiveness of such enforcement actions.".

SEC. 306. REPORT ON NOTIFICATION EFFECTIVENESS.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, and each year thereafter, the designated entity, in coordination with the Attorney General and the Federal Trade Commission, shall submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a report regarding the effectiveness of post-breach notification practices by agencies and business entities.

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

(1) in each instance of a breach of security, the amount of time between the instance of the breach and the discovery of the breach by the affected business entity;

(2) in each instance of a breach of security, the amount of time between the discovery of the breach by the affected business entity and the notification to the FBI and Secret Service; and

(3) in each instance of a breach of security, the amount of time between the discovery of the breach by the affected business entity and the notification to individuals whose sensitive personally identifiable information was compromised.

TITLE IV—COMPLIANCE WITH STATUTORY PAY-AS-YOU-GO ACT

SEC. 401. BUDGET COMPLIANCE.

The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement titled "Budgetary Effects of PAYGO Legislation" for this Act, submitted for printing in the Congressional Record by the Chairman of the Senate Budget Committee, provided that such statement has been submitted prior to the vote on passage.

Calendar No. 182

112TH CONGRESS
1ST SESSION

S. 1535

A BILL

To protect consumers by mitigating the vulnerability of personally identifiable information to theft through a security breach, providing notice and remedies to consumers in the wake of such a breach, holding companies accountable for preventable breaches, facilitating the sharing of post-breach technical information between companies, and enhancing criminal and civil penalties and other protections against the unauthorized collection or use of personally identifiable information.

SEPTEMBER 22, 2011

Reported with an amendment