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

IN THE SENATE OF THE UNITED STATES

Mr. LEAHY introduced the following bill; which was read twice and referred to the Committee on ____________________

A BILL

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the “Personal Data Privacy and Security Act of 2011”.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:
Sec. 1. Short title; table of contents.
Sec. 2. Findings.
Sec. 3. Definitions.

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

Sec. 101. Organized criminal activity in connection with unauthorized access to personally identifiable information.
Sec. 102. Concealment of security breaches involving sensitive personally identifiable information.
Sec. 103. Penalties for fraud and related activity in connection with computers.

TITLE II—DATA BROKERS

Sec. 201. Transparency and accuracy of data collection.
Sec. 203. Relation to State laws.
Sec. 204. Effective date.

TITLE III—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

Subtitle A—A Data Privacy and Security Program

Sec. 301. Purpose and applicability of data privacy and security program.
Sec. 302. Requirements for a personal data privacy and security program.
Sec. 303. Enforcement.
Sec. 304. Relation to other laws.

Subtitle B—Security Breach Notification

Sec. 311. Notice to individuals.
Sec. 312. Exemptions.
Sec. 313. Methods of notice.
Sec. 314. Content of notification.
Sec. 315. Coordination of notification with credit reporting agencies.
Sec. 316. Notice to law enforcement.
Sec. 317. Enforcement.
Sec. 318. Enforcement by State attorneys general.
Sec. 319. Effect on Federal and State law.
Sec. 320. Authorization of appropriations.
Sec. 321. Reporting on risk assessment exemptions.
Sec. 322. Effective date.

TITLE IV—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL DATA

Sec. 401. General services administration review of contracts.
Sec. 402. Requirement to audit information security practices of contractors and third party business entities.
Sec. 403. Privacy impact assessment of government use of commercial information services containing personally identifiable information.

TITLE V—COMPLIANCE WITH STATUTORY PAY-AS-YOU-GO ACT

Sec. 501. Budget compliance.
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 re-
store 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; and

(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.
SEC. 3. DEFINITIONS.

In this Act, the following definitions shall apply:

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

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

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

(5) 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 non-affiliated third parties on an interstate basis.
(6) DATA FURNISHER.—The term “data furnisher” means any agency, organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or nonprofit that serves as a source of information for a data broker.

(7) 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.

(8) 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 per-
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.

(9) 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 by section 1028(d)(7) of title 18, United State Code.

(10) 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.
(11) 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; and

(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 infor-
mation is not subject to further unauthorized disclosure;

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

(iii) any lawfully authorized investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the United States.

(12) 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 non-truncated social security number, driver’s license number, passport number, or alien registration number.

(ii) Any 2 of the following:

(I) Home address or telephone number.

(II) Mother’s maiden name.
(III) Month, day, and year of birth.

(iii) Unique biometric data such as a fingerprint, 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; or

(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.
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 title III of the Personal Data Privacy and Security Act of 2011, and having not otherwise qualif-
fied for an exemption from providing notice under section 312 of such Act, intentionally and willfully conceals the fact of such security breach and which breach causes economic damage 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 312(b) of the Personal Data Privacy and Security 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 312(b)(3) of such Act.”.

(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);
(i) 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 con-
sspiracy to commit an offense, under sub-
section (a)(5)(B)”;

(ii) by inserting “or conspiracy” after
“if the offense”; and

(iii) by redesignating subclauses (I)
through (VI) as clauses (i) through (vi),
respectively, and adjusting the margin ac-
cordingly; and

(iv) in clause (vi), as so redesignated,
by striking “; or” and inserting a semi-
colon;

(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 con-
sspiracy to commit an offense, under sub-
section (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 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;

(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”.

**TITLE II—DATA BROKERS**

**SEC. 201. TRANSPARENCY AND ACCURACY OF DATA COLLECTION.**

(a) In General.—Data brokers engaging in interstate commerce are subject to the requirements of this title for any product or service offered to third parties that allows access or use of personally identifiable information.

(b) Limitation.—Notwithstanding any other provision of this section, this section shall not apply to—

(1) any product or service offered by a data broker engaging in interstate commerce where such product or service is currently subject to, and in compliance with, access and accuracy protections similar to those under subsections (c) through (e) of this section under the Fair Credit Reporting Act (Public Law 91–508);

(2) any data broker that is subject to regulation under the Gramm-Leach-Bliley Act (Public Law 106–102);

(3) any data broker currently subject to and in compliance with the data security requirements for
such entities under the Health Insurance Portability and Accountability Act (Public Law 104–191), and its implementing regulations;

(4) any data broker subject to, and 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;

(5) information in a personal electronic record that—

(A) the data broker has identified as inaccurate, but maintains for the purpose of aiding the data broker in preventing inaccurate information from entering an individual’s personal electronic record; and

(B) is not maintained primarily for the purpose of transmitting or otherwise providing that information, or assessments based on that information, to nonaffiliated third parties;

(6) information concerning proprietary methodologies, techniques, scores, or algorithms relating to fraud prevention not normally provided to third parties in the ordinary course of business; and
(7) information that is used for legitimate governmental or fraud prevention purposes that would be compromised by disclosure to the individual.

(e) DISCLOSURES TO INDIVIDUALS.—

(1) IN GENERAL.—A data broker shall, upon the request of an individual, disclose to such individual for a reasonable fee all personal electronic records pertaining to that individual maintained or accessed by the data broker specifically for disclosure to third parties that request information on that individual in the ordinary course of business in the databases or systems of the data broker at the time of such request.

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

(d) DISCLOSURE TO INDIVIDUALS OF ADVERSE ACTIONS TAKEN BY THIRD PARTIES.—

(1) IN GENERAL.—If a person takes any adverse action with respect to any individual that is based, in whole or in part, on any information contained in a personal electronic record, the person, at no cost to the affected individual, shall provide—
(A) written or electronic notice of the adverse action to the individual;

(B) to the individual, in writing or electronically, the name, address, and telephone number of the data broker (including a toll-free telephone number established by the data broker, if the data broker complies and maintains data on individuals on a nationwide basis) that furnished the information to the person;

(C) a copy of the information such person obtained from the data broker; and

(D) information to the individual on the procedures for correcting any inaccuracies in such information.

(2) Accepted Methods of Notice.—A person shall be in compliance with the notice requirements under paragraph (1) if such person provides written or electronic notice in the same manner and using the same methods as are required under section 313(1) of this Act.

(e) Accuracy Resolution Process.—

(1) Information from a Public Record or Licensor.—

(A) In general.—If an individual notifies a data broker of a dispute as to the complete—
ness or accuracy of information disclosed to such individual under subsection (c) that is obtained from a public record source or a license agreement, such data broker shall determine within 30 days whether the information in its system accurately and completely records the information available from the licensor or public record source.

(B) DATA BROKER ACTIONS.—If a data broker determines under subparagraph (A) that the information in its systems does not accurately and completely record the information available from a public record source or licensor, the data broker shall—

(i) correct any inaccuracies or incompleteness, and provide to such individual written notice of such changes; and

(ii) provide such individual with the contact information of the public record or licensor.

(2) INFORMATION NOT FROM A PUBLIC RECORD SOURCE OR LICENSOR.—If an individual notifies a data broker of a dispute as to the completeness or accuracy of information not from a public record or licensor that was disclosed to the individual under
subsection (c), the data broker shall, within 30 days
of receiving notice of such dispute—

(A) review and consider free of charge any
information submitted by such individual that is
relevant to the completeness or accuracy of the
disputed information; and

(B) correct any information found to be in-
complete or inaccurate and provide notice to
such individual of whether and what informa-
tion was corrected, if any.

(3) Extension of review period.—The 30-
day period described in paragraph (1) may be ex-
tended for not more than 30 additional days if a
data broker receives information from the individual
during the initial 30-day period that is relevant to
the completeness or accuracy of any disputed infor-
mation.

(4) Notice identifying the data fur-
nisher.—If the completeness or accuracy of any in-
formation not from a public record source or licensor
that was disclosed to an individual under subsection
(c) is disputed by such individual, the data broker
shall provide, upon the request of such individual,
the contact information of any data furnisher that
provided the disputed information.
(5) Determination that dispute is frivolous or irrelevant.—

(A) In general.—Notwithstanding paragraphs (1) through (3), a data broker may decline to investigate or terminate a review of information disputed by an individual under those paragraphs if the data broker reasonably determines that the dispute by the individual is frivolous or intended to perpetrate fraud.

(B) Notice.—A data broker shall notify an individual of a determination under subparagraph (A) within a reasonable time by any means available to such data broker.

SEC. 202. ENFORCEMENT.

(a) Civil Penalties.—

(1) Penalties.—Any data broker that violates the provisions of section 201 shall be subject to civil penalties of not more than $1,000 per violation per day while such violations persist, up to a maximum of $250,000 per violation.

(2) Intentional or willful violation.—A data broker that intentionally or willfully violates the provisions of section 201 shall be subject to additional penalties in the amount of $1,000 per viola-
tion per day, to a maximum of an additional $250,000 per violation, while such violations persist.

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

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

(b) FEDERAL TRADE COMMISSION AUTHORITY.—Any data broker shall have the provisions of this title enforced against it by the Federal Trade Commission.

(e) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—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 data broker that violate this title, the State may bring a civil action on behalf of the residents of that State in a district court of the United
States of appropriate jurisdiction, or any other court of competent jurisdiction, to—

(A) enjoin that act or practice;

(B) enforce compliance with this title; or

(C) obtain civil penalties of not more than $1,000 per violation per day while such violations persist, up to a maximum of $250,000 per violation.

(2) NOTICE.—

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

(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 subparagraph (A) before the filing of the action.

(C) NOTIFICATION WHEN PRACTICABLE.—

In an action described under subparagraph (B),
the attorney general of a State shall provide the
written notice and the copy of the complaint to
the Federal Trade Commission as soon after
the filing of the complaint as practicable.

(3) Federal Trade Commission Author-
ity.—Upon receiving notice under paragraph (2),
the Federal Trade Commission shall have the right
to—

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

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

(C) file petitions for appeal.

(4) Pending Proceedings.—If the Federal
Trade Commission has instituted a proceeding or
civil action for a violation of this title, no attorney
general of a State may, during the pendency of such
proceeding or civil action, bring an action under this
subsection against any defendant named in such civil
action for any violation that is alleged in that civil
action.

(5) Rule of Construction.—For purposes of
bringing any civil action under paragraph (1), noth-
ing in this title shall be construed to prevent an at-
torney general of a State from exercising the powers
conferred on the attorney general by the laws of that
State to—

(A) conduct investigations;
(B) administer oaths and affirmations; or
(C) compel the attendance of witnesses or
the production of documentary and other evi-
dence.

(6) VENUE; SERVICE OF PROCESS.—

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

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

(i) is an inhabitant; or

(ii) may be found.

(d) NO PRIVATE CAUSE OF ACTION.—Nothing in
this title establishes a private cause of action against a
data broker for violation of any provision of this title.

SEC. 203. RELATION TO STATE LAWS.

No requirement or prohibition may be imposed under
the laws of any State with respect to any subject matter
regulated under section 201, relating to individual access
to, and correction of, personal electronic records held by
data brokers.

SEC. 204. EFFECTIVE DATE.

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

TITLE III—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

Subtitle A—A Data Privacy and Security Program

SEC. 301. PURPOSE AND APPLICABILITY OF DATA PRIVACY
AND SECURITY PROGRAM.

(a) PURPOSE.—The purpose of this subtitle is to en-
sure standards for developing and implementing adminis-
trative, 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 per-
sonally 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 302 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


(2) HIPPA 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) Safe Harbors.—
(1) In general.—A business entity shall be deemed in compliance with the privacy and security program requirements under section 302 if the business entity complies with or provides protection equal to industry standards or standards widely accepted as an effective industry practice, 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 business entity.

(2) Limitation.—Nothing in this subsection shall be construed to permit, and nothing does permit, the Federal Trade Commission to issue regulations requiring, or according greater legal status to, the implementation of or application of a specific technology or technological specifications for meeting the requirements of this title.

SEC. 302. 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 identifying information;

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

   (C) protect against unauthorized access to use of sensitive personally identifying 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 fa-
cilities containing sensitive personally iden-
tifiable information, including controls to
authenticate and permit access only to au-
thorized individuals;

(ii) detect, record, and preserve infor-
mation relevant to actual and attempted
fraudulent, unlawful, or unauthorized ac-
cess, disclosure, use, or alteration of sen-
sitive personally identifiable information,
including by employees and other individ-
uals otherwise authorized to have access;

(iii) protect sensitive personally identi-
ifiable information during use, trans-
mission, storage, and disposal by
encryption, redaction, or access controls
that are widely accepted as an effective in-
dustry practice or industry standard, or
other reasonable means (including as di-
rected for disposal of records under section
628 of the Fair Credit Reporting Act (15
U.S.C. 1681w) and the implementing regu-
lations 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; and

(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.

(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 301, 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 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. 303. Enforcement.**

(a) **Civil Penalties.**—

(1) **In General.**—Any business entity that violates the provisions of sections 301 or 302 shall be subject to civil penalties of not more than $5,000 per violation per day while such a violation exists, with a maximum of $500,000 per violation.

(2) **Intentional or Willful Violation.**—A business entity that intentionally or willfully violates the provisions of sections 301 or 302 shall be subject to additional penalties in the amount of $5,000 per violation per day while such a violation exists, with a maximum of an additional $500,000 per violation.

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

(4) **Other Rights and Remedies.**—The rights and remedies available under this section are
cumulative and shall not affect any other rights and remedies available under law.

(b) **Federal Trade Commission Authority.**— Any business entity shall have the provisions of this subtitle enforced against it by the Federal Trade Commission.

(c) **State Enforcement.**—

(1) **Civil Actions.**—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 $500,000 per violation.
(2) NOTICE.—

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

(i) a written notice of that action; and

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

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

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

(3) FEDERAL TRADE COMMISSION AUTHORITY.—Upon receiving notice under paragraph (2), the Federal Trade Commission shall have the right to—
(A) move to stay the action, pending the
final disposition of a pending Federal pro-
ceeding or action as described in paragraph (4);
(B) intervene in an action brought under
paragraph (1); and
(C) file petitions for appeal.

(4) PENDING PROCEEDINGS.—If the Federal
Trade Commission has instituted a proceeding or ac-
tion for a violation of this subtitle or any regulations
thereunder, no attorney general of a State may, dur-
ing the pendency of such proceeding or action, bring
an action under this subsection against any defend-
ant named in such criminal proceeding or civil ac-
tion for any violation that is alleged in that pro-
ceeding or action.

(5) RULE OF CONSTRUCTION.—For purposes of
bringing any civil action under paragraph (1) noth-
ing in this subtitle shall be construed to prevent an
attorney general of a State from exercising the pow-
ers conferred on the attorney general by the laws of
that State to—
(A) conduct investigations;
(B) administer oaths and affirmations; or
(C) compel the attendance of witnesses or
the production of documentary and other evi-
dence.

(6) VENUE; SERVICE OF PROCESS.—

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

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

(i) is an inhabitant; or

(ii) may be found.

(d) NO PRIVATE CAUSE OF ACTION.—Nothing in
this subtitle establishes a private cause of action against
a business entity for violation of any provision of this sub-
title.

SEC. 304. RELATION TO OTHER LAWS.

(a) IN GENERAL.—No State may require any busi-
ness entity subject to this subtitle to comply with any re-
quirements with respect to administrative, technical, and
physical safeguards for the protection of sensitive person-
ally identifying information.
(b) LIMITATIONS.—Nothing in this subtitle shall be construed to modify, limit, or supersede the operation of the Gramm-Leach-Bliley Act or its implementing regulations, including those adopted or enforced by States.

Subtitle B—Security Breach Notification

SEC. 311. 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 shall, following the discovery of a 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, prevent further disclosures, conduct the risk assess-
ment described in section 302(a)(3), and restore the reasonable integrity of the data system 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, 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 or intelligence agency determines that the notification required under this section would impede a criminal investigation, 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 pro-
vides written notification that further delay is neces-
sary.

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

**SEC. 312. EXEMPTIONS.**

(a) **Exemption for National Security and Law
    Enforcement.**—

    (1) **In general.**—Section 311 shall not apply
to an agency or business entity if the agency or busi-
ness entity certifies, in writing, that notification of
the security breach as required by section 311 rea-
sonably 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 en-
forcement 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; or

(C) restrain competition.

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

(4) SECRET SERVICE AND FBI REVIEW OF CER-
tIFICATIONS.—

(A) IN GENERAL.—The United States Se-
cret Service or the Federal Bureau of Investiga-
tion 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 exemp-
tion under paragraph (1) is merited. Such re-
view shall be completed not later than 10 busi-
ness days after the date of receipt of the certifi-
cation, except as provided in paragraph (5)(C).

(B) NOTICE.—Upon completing a review
under subparagraph (A) the United States Se-
cret Service or the Federal Bureau of Investiga-
tion 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 10 business days after the date of receipt of the additional information whether an exemption under paragraph (1) is merited.

(b) **Safe Harbor.**—An agency or business entity will be exempt from the notice requirements under section 311, if—

(1) a risk assessment concludes that—

(A) 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, with the encryption of such information establishing a presumption that no significant risk exists; or

(B) 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, with the rendering of such sen-
sitively 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, establishing a presumption that no significant risk exists;

(2) without unreasonable delay, but not later than 45 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 notifies the United States Secret Service and the Federal Bureau of Investigation, in writing, of—

(A) the results of the risk assessment; and

(B) its decision to invoke the risk assessment exemption; and

(3) the United States Secret Service or the Federal Bureau of Investigation does not indicate, in writing, within 10 business days from receipt of the decision, that notice should be given.

(c) **Financial Fraud Prevention Exemption.**—

(1) **In General.**—A business entity will be exempt from the notice requirement under section 311
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.—The exemption by this subsection does not apply 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. 313. METHODS OF NOTICE.

An agency or business entity shall be in compliance with section 311 if it provides both:
(1) **INDIVIDUAL NOTICE.**—Notice to individuals by 1 of the following means:

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

(B) Telephone notice to the individual personally.

(C) E-mail notice, if the individual has consented to receive such notice and the notice is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).

(2) **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. 314. CONTENT OF NOTIFICATION.**

(a) **IN GENERAL.**—Regardless of the method by which notice is provided to individuals under section 313, such notice shall include, to the extent possible—

(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;

(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; and

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

(b) ADDITIONAL CONTENT.—Notwithstanding section 319, a State may require that a notice under subsection (a) shall also include information regarding victim protection assistance provided for by that State.

SEC. 315. COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.

If an agency or business entity is required to provide notification to more than 5,000 individuals under section 311(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 no-
ties. 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. 316. 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 10,000;

(2) the security breach involves a database, networked or integrated databases, or other data system containing the sensitive personally identifiable information of more than 1,000,000 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 Gover-
ment involved in national security or law enforcement.

(b) FTC REVIEW OF THRESHOLDS.—The Federal Trade Commission may review and adjust the thresholds for notice to law enforcement under subsection (a), after notice and the opportunity for public comment, in a manner consistent with this section.

(c) ADVANCE NOTICE TO LAW ENFORCEMENT.—Not later than 48 hours before notifying an individual of a security breach under section 311, a business entity or agency that is required to provide notice under this section shall notify the United States Secret Service and the Federal Bureau of Investigation of the fact that the business entity or agency intends to provide the notice.

(d) 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.

(c) **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 14 days after discovery of the events requiring notice.
2. Notice under subsection (d) shall be delivered not later than 14 days after the Service receives notice of a security breach from an agency or business entity.

**SEC. 317. ENFORCEMENT.**

(a) **CIVIL ACTIONS BY THE ATTORNEY 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 $1,000 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 $1,000,000 per violation, unless such conduct is found to be willful or intentional. In determining the amount of a civil penalty under this subsection, the court
shall take into account the degree of culpability of the
business entity, any prior violations of this subtitle by the
business entity, the ability of the business entity to pay,
the effect on the ability of the business entity to continue
to do business, and such other matters as justice may re-
quire.

(b) Injunctive Actions by the Attorney Gen-
eral.—

(1) In General.—If it appears that a business
ty has engaged, or is engaged, in any act or
practice constituting a violation of this subtitle, the
Attorney General may petition an appropriate dis-
trict 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 subtitle are cumulative and
shall not affect any other rights and remedies available
under law.

d) 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 informa-
tion has or may have been compromised,’’ after ‘‘identity
theft report’’.

SEC. 318. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) In General.—

(1) Civil Actions.—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 engage-
ment of a business entity in a practice that is pro-
hibited under this subtitle, the State or the State or
local law enforcement agency on behalf of the resi-
dents of the agency’s jurisdiction, may bring a civil
action on behalf of the residents of the State or ju-
risdiction in a district court of the United States of
appropriate jurisdiction or any other court of com-
petent jurisdiction, including a State court, to—

(A) enjoin that practice;

(B) enforce compliance with this subtitle;

or
(C) civil penalties of not more than $1,000 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 $1,000,000 per violation, unless such conduct is found to be willful or intentional.

(2) Notice.—

(A) In general.—Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Attorney General 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 ac-
tion;

(2) initiate an action in the appropriate United
States district court under section 317 and move to
consolidate all pending actions, including State ac-
tions, in such court;

(3) intervene in an action brought under sub-
section (a)(2); and

(4) file petitions for appeal.

(c) Pending Proceedings.—If the Attorney Gen-
eral 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 pro-
ceeding 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 pro-
ceeding 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.
(f) NO PRIVATE CAUSE OF ACTION.—Nothing in this subtitle establishes a private cause of action against a business entity for violation of any provision of this subtitle.

SEC. 319. EFFECT ON FEDERAL AND STATE LAW.

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 314(b).

SEC. 320. 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. 321. 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 312(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 312(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.

SEC. 322. 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 IV—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL DATA

SEC. 401. 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 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 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.

(e) PENALTIES.—In awarding contracts with data brokers for products or services related to access, use, compilation, distribution, processing, analyzing, or evalu-
ating 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. 402. 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 Privacy and Security Act of 2011) and ensuring remedial action to address any significant deficiencies.”.
SEC. 403. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT USE OF COMMERCIAL INFORMATION SERVICES CONTAINING PERSONALLY IDENTIFIABLE INFORMATION.

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

(1) in subparagraph (A)(i), by striking “or”;

and

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

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

“(iii) purchasing or subscribing for a fee to personally identifiable information from a data broker (as such terms are defined in section 3 of the Personal Data Privacy and Security 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 informa-
tion, 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, ana-
lyze, or otherwise use such databases;

(B) standards governing the access, anal-
ysis, 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 informa-
tion obtained from such databases;

(E) procedures ensuring that such data
meet standards of accuracy, relevance, com-
pleteness, 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.

TITLE V—COMPLIANCE WITH STATUTORY PAY-AS-YOU-GO ACT

SEC. 501. 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.