

Calendar No. 208111TH CONGRESS
1ST SESSION**S. 1490**

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

JULY 22, 2009

Mr. LEAHY (for himself, Mr. BROWN, Mr. FEINGOLD, Mr. SCHUMER, Mr. SPECTER, Mr. CARDIN, and Mr. HATCH) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

NOVEMBER 5, 2009

Reported by Mr. LEAHY, with amendments

[Omit the part struck through and insert the part printed in *italie*]

A BILL

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

2 (a) **SHORT TITLE.**—This Act may be cited as the
 3 “Personal Data Privacy and Security Act of 2009”.

4 (b) **TABLE OF CONTENTS.**—The table of contents of
 5 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. Review and amendment of Federal sentencing guidelines related to fraudulent access to or misuse of digitized or electronic personally identifiable information.
- Sec. 104. Effects of identity theft on bankruptcy proceedings.

TITLE II—DATA BROKERS

- Sec. 201. Transparency and accuracy of data collection.
- Sec. 202. Enforcement.
- 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.

Subtitle C—Office of Federal Identity Protection

Sec. 331. Office of Federal Identity Protection.

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 informa-
tion services containing personally identifiable information.

Sec. 404. Implementation of chief privacy officer requirements.

1 **SEC. 2. FINDINGS.**

2 Congress finds that—

3 (1) databases of personally identifiable informa-
4 tion are increasingly prime targets of hackers, iden-
5 tity thieves, rogue employees, and other criminals,
6 including organized and sophisticated criminal oper-
7 ations;

8 (2) identity theft is a serious threat to the Na-
9 tion's economic stability, homeland security, the de-
10 velopment of e-commerce, and the privacy rights of
11 Americans;

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

14 (4) security breaches are a serious threat to
15 consumer confidence, homeland security, e-com-
16 merce, and economic stability;

17 (5) it is important for business entities that
18 own, use, or license personally identifiable informa-
19 tion to adopt reasonable procedures to ensure the se-

1 security, privacy, and confidentiality of that personally
2 identifiable information;

3 (6) individuals whose personal information has
4 been compromised or who have been victims of iden-
5 tity theft should receive the necessary information
6 and assistance to mitigate their damages and to re-
7 store the integrity of their personal information and
8 identities;

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

14 (8) data misuse and use of inaccurate data have
15 the potential to cause serious or irreparable harm to
16 an individual's livelihood, privacy, and liberty and
17 undermine efficient and effective business and gov-
18 ernment operations;

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

23 (10) government access to commercial data can
24 potentially improve safety, law enforcement, and na-
25 tional security; and

1 (11) because government use of commercial
2 data containing personal information potentially af-
3 fects individual privacy, and law enforcement and
4 national security operations, there is a need for Con-
5 gress to exercise oversight over government use of
6 commercial data.

7 **SEC. 3. DEFINITIONS.**

8 In this Act, the following definitions shall apply:

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

12 (2) AFFILIATE.—The term “affiliate” means
13 persons related by common ownership or by cor-
14 porate control.

15 (3) BUSINESS ENTITY.—The term “business
16 entity” means any organization, corporation, trust,
17 partnership, sole proprietorship, unincorporated as-
18 sociation, or venture established to make a profit, or
19 nonprofit.

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

23 (5) DATA BROKER.—The term “data broker”
24 means a business entity which for monetary fees or
25 dues regularly engages in the practice of collecting,

1 transmitting, or providing access to sensitive person-
 2 ally identifiable information on more than 5,000 in-
 3 dividuals who are not the customers or employees of
 4 that business entity or affiliate primarily for the
 5 purposes of providing such information to non-
 6 affiliated third parties on an interstate basis.

7 (6) DATA FURNISHER.—The term “data fur-
 8 nisher” means any agency, organization, corpora-
 9 tion, trust, partnership, sole proprietorship, unincor-
 10 porated association, or nonprofit that serves as a
 11 source of information for a data broker.

12 (7) ENCRYPTION.—The term “encryption”—

13 (A) means the protection of data in elec-
 14 tronic form, in storage or in transit, using an
 15 encryption technology that has been adopted by
 16 ~~an established~~ *a widely accepted* standards set-
 17 ting body *or, has been widely accepted as an ef-*
 18 *fective industry practice* which renders such
 19 data indecipherable in the absence of associated
 20 cryptographic keys necessary to enable
 21 decryption of such data; and

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

25 (8) PERSONAL ELECTRONIC RECORD.—

1 (A) IN GENERAL.—The term “personal
2 electronic record” means data associated with
3 an individual contained in a database,
4 networked or integrated databases, or other
5 data system that is provided to nonaffiliated
6 third parties and includes sensitive personally
7 identifiable information about that individual.

8 (B) EXCLUSIONS.—The term “personal
9 electronic record” does not include—

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

12 (ii) any proprietary assessment or
13 evaluation of an individual or any propri-
14 etary assessment or evaluation of informa-
15 tion about an individual.

16 (9) PERSONALLY IDENTIFIABLE INFORMA-
17 TION.—The term “personally identifiable informa-
18 tion” means any information, or compilation of in-
19 formation, in electronic or digital form serving as a
20 means of identification, as defined by section
21 1028(d)(7) of title 18, United State Code.

22 (10) PUBLIC RECORD SOURCE.—The term
23 “public record source” means the Congress, any
24 agency, any State or local government agency, the
25 government of the District of Columbia and govern-

1 ments of the territories or possessions of the United
2 States, and Federal, State or local courts, courts
3 martial and military commissions, that maintain
4 personally identifiable information in records avail-
5 able to the public.

6 (11) SECURITY BREACH.—

7 (A) IN GENERAL.—The term “security
8 breach” means compromise of the security, con-
9 fidentiality, or integrity of computerized data
10 through misrepresentation or actions that result
11 in, or there is a reasonable basis to conclude
12 has resulted in, acquisition of or access to sen-
13 sitive personally identifiable information that is
14 unauthorized or in excess of authorization *and*
15 *which present a significant risk of harm or fraud*
16 *to any individual.*

17 (B) EXCLUSION.—The term “security
18 breach” does not include—

19 (i) a good faith acquisition of sensitive
20 personally identifiable information by a
21 business entity or agency, or an employee
22 or agent of a business entity or agency, if
23 the sensitive personally identifiable infor-
24 mation is not subject to further unauthor-
25 ized disclosure; or

1 (ii) the release of a public record not
2 otherwise subject to confidentiality or non-
3 disclosure requirements.

4 (12) SENSITIVE PERSONALLY IDENTIFIABLE IN-
5 FORMATION.—The term “sensitive personally identi-
6 fiable information” means any information or com-
7 pilation of information, in electronic or digital form
8 that includes—

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

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

15 (ii) Any 2 of the following:

16 (I) Home address or telephone
17 number.

18 (II) Mother’s maiden name, if
19 identified as such.

20 (III) Month, day, and year of
21 birth.

22 (iii) Unique biometric data such as a
23 finger print, voice print, a retina or iris
24 image, or any other unique physical rep-
25 resentation.

1 (iv) A unique account identifier, elec-
2 tronic identification number, user name, or
3 routing code in combination with any asso-
4 ciated security code, access code, or pass-
5 word that is required for an individual to
6 obtain money, goods, services, or any other
7 thing of value; or

8 (B) a financial account number or credit
9 or debit card number in combination with any
10 security code, access code, or password that is
11 required for an individual to obtain credit, with-
12 draw funds, or engage in a financial trans-
13 action.

14 **TITLE I—ENHANCING PUNISH-**
15 **MENT FOR IDENTITY THEFT**
16 **AND OTHER VIOLATIONS OF**
17 **DATA PRIVACY AND SECU-**
18 **RITY**

19 **SEC. 101. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION**
20 **WITH UNAUTHORIZED ACCESS TO PERSON-**
21 **ALLY IDENTIFIABLE INFORMATION.**

22 Section 1961(1) of title 18, United States Code, is
23 amended by inserting “section 1030(a)(2)(D) (relating to
24 fraud and related activity in connection with unauthorized
25 access to sensitive personally identifiable information as

1 defined in the Personal Data Privacy and Security Act of
2 2009,” before “section 1084”.

3 **SEC. 102. CONCEALMENT OF SECURITY BREACHES INVOLV-**
4 **ING SENSITIVE PERSONALLY IDENTIFIABLE**
5 **INFORMATION.**

6 (a) IN GENERAL.—Chapter 47 of title 18, United
7 States Code, is amended by adding at the end the fol-
8 lowing:

9 **“§ 1041. Concealment of security breaches involving**
10 **sensitive personally identifiable informa-**
11 **tion**

12 “(a) Whoever, having knowledge of a security breach
13 and of the obligation to provide notice of such breach to
14 individuals under title III of the Personal Data Privacy
15 and Security Act of 2009, and having not otherwise quali-
16 fied for an exemption from providing notice under section
17 312 of such Act, intentionally and willfully conceals the
18 fact of such security breach and which breach causes eco-
19 nomic damage to 1 or more persons, shall be fined under
20 this title or imprisoned not more than 5 years, or both.

21 “(b) For purposes of subsection (a), the term ‘person’
22 has the same meaning as in section 1030(e)(12) of title
23 18, United States Code.

24 “(c) Any person seeking an exemption under section
25 312(b) of the Personal Data Privacy and Security Act of

1 2009 shall be immune from prosecution under this section
 2 if the United States Secret Service does not indicate, in
 3 writing, that such notice be given under section 312(b)(3)
 4 of such Act.”.

5 (b) CONFORMING AND TECHNICAL AMENDMENTS.—

6 The table of sections for chapter 47 of title 18, United
 7 States Code, is amended by adding at the end the fol-
 8 lowing:

“1041. Concealment of security breaches involving personally identifiable infor-
 mation.”.

9 (c) ENFORCEMENT AUTHORITY.—

10 (1) IN GENERAL.—The United States Secret
 11 Service shall have the authority to investigate of-
 12 fenses under this section.

13 (2) NONEXCLUSIVITY.—The authority granted
 14 in paragraph (1) shall not be exclusive of any exist-
 15 ing authority held by any other Federal agency.

16 **SEC. 103. REVIEW AND AMENDMENT OF FEDERAL SEN-**
 17 **TENCING GUIDELINES RELATED TO FRAUDU-**
 18 **LENT ACCESS TO OR MISUSE OF DIGITIZED**
 19 **OR ELECTRONIC PERSONALLY IDENTIFIABLE**
 20 **INFORMATION.**

21 (a) REVIEW AND AMENDMENT.—The United States
 22 Sentencing Commission, pursuant to its authority under
 23 section 994 of title 28, United States Code, and in accord-
 24 ance with this section, shall review and, if appropriate,

1 amend the Federal sentencing guidelines (including its
2 policy statements) applicable to persons convicted of using
3 fraud to access, or misuse of, digitized or electronic per-
4 sonally identifiable information, including identity theft or
5 any offense under—

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

8 (2) any other relevant provision.

9 (b) REQUIREMENTS.—In carrying out the require-
10 ments of this section, the United States Sentencing Com-
11 mission shall—

12 (1) ensure that the Federal sentencing guide-
13 lines (including its policy statements) reflect—

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

16 (B) the growing incidences of theft and
17 misuse of digitized or electronic personally iden-
18 tifiable information, including identity theft;
19 and

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

22 (2) consider the extent to which the Federal
23 sentencing guidelines (including its policy state-
24 ments) adequately address violations of the sections
25 amended by this Act to—

1 (A) sufficiently deter and punish such of-
2 fenses; and

3 (B) adequately reflect the enhanced pen-
4 alties established under this Act;

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

7 (4) account for any additional aggravating or
8 mitigating circumstances that might justify excep-
9 tions to the generally applicable sentencing ranges;

10 (5) consider whether to provide a sentencing en-
11 hancement for those convicted of the offenses de-
12 scribed in subsection (a), if the conduct involves—

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

15 (B) the sale of fraudulently obtained or
16 stolen personally identifiable information to an
17 individual who is engaged in terrorist activity or
18 aiding other individuals engaged in terrorist ac-
19 tivity; or

20 (C) the sale of fraudulently obtained or
21 stolen personally identifiable information to fi-
22 nance terrorist activity or other criminal activi-
23 ties;

24 (6) make any necessary conforming changes to
25 the Federal sentencing guidelines to ensure that

1 such guidelines (including its policy statements) as
2 described in subsection (a) are sufficiently stringent
3 to deter, and adequately reflect crimes related to
4 fraudulent access to, or misuse of, personally identi-
5 fiable information; and

6 (7) ensure that the Federal sentencing guide-
7 lines adequately meet the purposes of sentencing
8 under section 3553(a)(2) of title 18, United States
9 Code.

10 (c) EMERGENCY AUTHORITY TO SENTENCING COM-
11 MISSION.—The United States Sentencing Commission
12 may, as soon as practicable, promulgate amendments
13 under this section in accordance with procedures estab-
14 lished in section 21(a) of the Sentencing Act of 1987 (28
15 U.S.C. 994 note) as though the authority under that Act
16 had not expired.

17 **SEC. 104. EFFECTS OF IDENTITY THEFT ON BANKRUPTCY**
18 **PROCEEDINGS.**

19 (a) DEFINITIONS.—Section 101 of title 11, United
20 States Code, is amended—

21 (1) by redesignating paragraph (27B) as para-
22 graph (27D); and

23 (2) by inserting after paragraph (27A) the fol-
24 lowing:

1 “(27) The term ‘identity theft’ means a fraud
2 committed or attempted using the personally identi-
3 fiable information of another person.

4 “(28) The term ‘identity theft victim’ means a
5 debtor who, as a result of an identify theft in any
6 consecutive 12-month period during the 3-year pe-
7 riod before the date on which a petition is filed
8 under this title, had claims asserted against such
9 debtor in excess of the least of—

10 “(A) \$20,000;

11 “(B) 50 percent of all claims asserted
12 against such debtor; or

13 “(C) 25 percent of the debtor’s gross in-
14 come for such 12-month period.”.

15 (b) PROHIBITION.—Section 707(b) of title 11, United
16 States Code, is amended by adding at the end the fol-
17 lowing:

18 “(8) No judge, United States trustee (or bankruptcy
19 administrator, if any), trustee, or other party in interest
20 may file a motion under paragraph (2) if the debtor is
21 an identity theft victim.”.

1 **TITLE II—DATA BROKERS**

2 **SEC. 201. TRANSPARENCY AND ACCURACY OF DATA COL-**
3 **LECTION.**

4 (a) **IN GENERAL.**—Data brokers engaging in inter-
5 state commerce are subject to the requirements of this
6 title for any product or service offered to third parties that
7 allows access or use of sensitive personally identifiable in-
8 formation.

9 (b) **LIMITATION.**—Notwithstanding any other provi-
10 sion of this title, this section shall not apply to—

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

18 (2) any data broker that is subject to regulation
19 under the Gramm-Leach-Bliley Act (Public Law
20 106–102);

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

1 (4) information in a personal electronic record
2 that—

3 (A) the data broker has identified as inac-
4 curate, but maintains for the purpose of aiding
5 the data broker in preventing inaccurate infor-
6 mation from entering an individual's personal
7 electronic record; and

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

12 (5) information concerning proprietary meth-
13 odologies, techniques, scores, or algorithms relating
14 to fraud prevention not normally provided to third
15 parties in the ordinary course of business; *and*

16 (6) *information that is used for legitimate gov-*
17 *ernmental or fraud prevention purposes that would be*
18 *compromised by disclosure to the individual.*

19 (c) DISCLOSURES TO INDIVIDUALS.—

20 (1) IN GENERAL.—A data broker shall, upon
21 the request of an individual, disclose to such indi-
22 vidual for a reasonable fee all personal electronic
23 records pertaining to that individual maintained spe-
24 cifically for disclosure to third parties that request
25 information on that individual in the ordinary course

1 of business in the databases or systems of the data
2 broker at the time of such request.

3 (2) INFORMATION ON HOW TO CORRECT INAC-
4 CURACIES.—The disclosures required under para-
5 graph (1) shall also include guidance to individuals
6 on procedures for correcting inaccuracies.

7 (d) DISCLOSURE TO INDIVIDUALS OF ADVERSE AC-
8 TIONS TAKEN BY THIRD PARTIES.—

9 (1) IN GENERAL.—In addition to any other
10 rights established under this Act, if a person takes
11 any adverse action with respect to any individual
12 that is based, in whole or in part, on any informa-
13 tion contained in a personal electronic record that is
14 maintained, updated, or otherwise owned or pos-
15 sessed by a data broker, such person, at no cost to
16 the affected individual, shall provide—

17 (A) written or electronic notice of the ad-
18 verse action to the individual;

19 (B) to the individual, in writing or elec-
20 tronically, the name, address, and telephone
21 number of the data broker that furnished the
22 information to the person;

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

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

4 (2) ACCEPTED METHODS OF NOTICE.—A per-
5 son shall be in compliance with the notice require-
6 ments under paragraph (1) if such person provides
7 written or electronic notice in the same manner and
8 using the same methods as are required under sec-
9 tion 313(1) of this Act.

10 (e) ACCURACY RESOLUTION PROCESS.—

11 (1) INFORMATION FROM A PUBLIC RECORD OR
12 LICENSOR.—

13 (A) IN GENERAL.—If an individual notifies
14 a data broker of a dispute as to the complete-
15 ness or accuracy of information disclosed to
16 such individual under subsection (c) that is ob-
17 tained from a public record source or a license
18 agreement, such data broker shall determine
19 within 30 days whether the information in its
20 system accurately and completely records the
21 information available from the licensor or public
22 record source.

23 (B) DATA BROKER ACTIONS.—If a data
24 broker determines under subparagraph (A) that
25 the information in its systems does not accu-

1 rately and completely record the information
2 available from a public record source or licen-
3 sor, the data broker shall—

4 (i) correct any inaccuracies or incom-
5 pleteness, and provide to such individual
6 written notice of such changes; and

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

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

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

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

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

8 (4) NOTICE IDENTIFYING THE DATA FUR-
9 NISHER.—If the completeness or accuracy of any in-
10 formation not from a public record source or licensor
11 that was disclosed to an individual under subsection
12 (c) is disputed by such individual, the data broker
13 shall provide, upon the request of such individual,
14 the contact information of any data furnisher that
15 provided the disputed information.

16 (5) DETERMINATION THAT DISPUTE IS FRIVO-
17 LOUS OR IRRELEVANT.—

18 (A) IN GENERAL.—Notwithstanding para-
19 graphs (1) through (3), a data broker may de-
20 cline to investigate or terminate a review of in-
21 formation disputed by an individual under those
22 paragraphs if the data broker reasonably deter-
23 mines that the dispute by the individual is friv-
24 olous or intended to perpetrate fraud.

1 (B) NOTICE.—A data broker shall notify
2 an individual of a determination under subpara-
3 graph (A) within a reasonable time by any
4 means available to such data broker.

5 **SEC. 202. ENFORCEMENT.**

6 (a) CIVIL PENALTIES.—

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

12 (2) INTENTIONAL OR WILLFUL VIOLATION.—A
13 data broker that intentionally or willfully violates the
14 provisions of section 201 shall be subject to addi-
15 tional penalties in the amount of \$1,000 per viola-
16 tion per day, to a maximum of an additional
17 \$250,000 per violation, while such violations persist.

18 (3) EQUITABLE RELIEF.—A data broker en-
19 gaged in interstate commerce that violates this sec-
20 tion may be enjoined from further violations by a
21 court of competent jurisdiction.

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

1 (b) FEDERAL TRADE COMMISSION AUTHORITY.—
2 Any data broker shall have the provisions of this title en-
3 forced against it by the Federal Trade Commission.

4 (c) STATE ENFORCEMENT.—

5 (1) CIVIL ACTIONS.—In any case in which the
6 attorney general of a State or any State or local law
7 enforcement agency authorized by the State attorney
8 general or by State statute to prosecute violations of
9 consumer protection law, has reason to believe that
10 an interest of the residents of that State has been
11 or is threatened or adversely affected by the acts or
12 practices of a data broker that violate this title, the
13 State may bring a civil action on behalf of the resi-
14 dents of that State in a district court of the United
15 States of appropriate jurisdiction, or any other court
16 of competent jurisdiction, to—

17 (A) enjoin that act or practice;

18 (B) enforce compliance with this title; or

19 (C) obtain civil penalties of not more than
20 \$1,000 per violation per day while such viola-
21 tions persist, up to a maximum of \$250,000 per
22 violation.

23 (2) NOTICE.—

24 (A) IN GENERAL.—Before filing an action
25 under this subsection, the attorney general of

1 the State involved shall provide to the Federal
2 Trade Commission—

3 (i) a written notice of that action; and

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

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

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

19 (3) FEDERAL TRADE COMMISSION AUTHOR-
20 ITY.—Upon receiving notice under paragraph (2),
21 the Federal Trade Commission shall have the right
22 to—

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

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

3 (C) file petitions for appeal.

4 (4) PENDING PROCEEDINGS.—If the Federal
5 Trade Commission has instituted a proceeding or
6 civil action for a violation of this title, no attorney
7 general of a State may, during the pendency of such
8 proceeding or civil action, bring an action under this
9 subsection against any defendant named in such civil
10 action for any violation that is alleged in that civil
11 action.

12 (5) RULE OF CONSTRUCTION.—For purposes of
13 bringing any civil action under paragraph (1), noth-
14 ing in this title shall be construed to prevent an at-
15 torney general of a State from exercising the powers
16 conferred on the attorney general by the laws of that
17 State to—

18 (A) conduct investigations;

19 (B) administer oaths and affirmations; or

20 (C) compel the attendance of witnesses or
21 the production of documentary and other evi-
22 dence.

23 (6) VENUE; SERVICE OF PROCESS.—

24 (A) VENUE.—Any action brought under
25 this subsection may be brought in the district

1 court of the United States that meets applicable
2 requirements relating to venue under section
3 1391 of title 28, United States Code.

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

7 (i) is an inhabitant; or

8 (ii) may be found.

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

12 **SEC. 203. RELATION TO STATE LAWS.**

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

18 **SEC. 204. EFFECTIVE DATE.**

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

1 **TITLE III—PRIVACY AND SECUR-**
2 **RITY OF PERSONALLY IDEN-**
3 **TIFIABLE INFORMATION**

4 **Subtitle A—A Data Privacy and**
5 **Security Program**

6 **SEC. 301. PURPOSE AND APPLICABILITY OF DATA PRIVACY**
7 **AND SECURITY PROGRAM.**

8 (a) **PURPOSE.**—The purpose of this subtitle is to en-
9 sure standards for developing and implementing adminis-
10 trative, technical, and physical safeguards to protect the
11 security of sensitive personally identifiable information.

12 (b) **IN GENERAL.**—A business entity engaging in
13 interstate commerce that involves collecting, accessing,
14 transmitting, using, storing, or disposing of sensitive per-
15 sonally identifiable information in electronic or digital
16 form on 10,000 or more United States persons is subject
17 to the requirements for a data privacy and security pro-
18 gram under section 302 for protecting sensitive personally
19 identifiable information.

20 (c) **LIMITATIONS.**—Notwithstanding any other obli-
21 gation under this subtitle, this subtitle does not apply to:

22 (1) **FINANCIAL INSTITUTIONS.**—Financial insti-
23 tutions—

24 (A) subject to the data security require-
25 ments and implementing regulations under the

1 Gramm-Leach-Bliley Act (15 U.S.C. 6801 et
2 seq.); and

3 (B) subject to—

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

10 (ii) compliance with part 314 of title
11 16, Code of Federal Regulations.

12 (2) HIPPA REGULATED ENTITIES.—

13 (A) COVERED ENTITIES.—Covered entities
14 subject to the Health Insurance Portability and
15 Accountability Act of 1996 (42 U.S.C. 1301 et
16 seq.), including the data security requirements
17 and implementing regulations of that Act.

18 (B) BUSINESS ENTITIES.—A business enti-
19 ty shall be deemed in compliance with the pri-
20 vacy and security program requirements under
21 section 302 if the business entity is acting as
22 a “business associate” as that term is defined
23 in the Health Insurance Portability and Ac-
24 countability Act of 1996 (42 U.S.C. 1301 et
25 seq.) and is in compliance with requirements

1 imposed under that Act and its implementing
2 regulations.

3 (3) PUBLIC RECORDS.—Public records not oth-
4 erwise subject to a confidentiality or nondisclosure
5 requirement, or information obtained from a news
6 report or periodical.

7 (d) SAFE HARBORS.—

8 (1) IN GENERAL.—A business entity shall be
9 deemed in compliance with the privacy and security
10 program requirements under section 302 if the busi-
11 ness entity complies with or provides protection
12 equal to industry standards *or widely accepted as an*
13 *effective industry practice*, as identified by the Fed-
14 eral Trade Commission, that are applicable to the
15 type of sensitive personally identifiable information
16 involved in the ordinary course of business of such
17 business entity.

18 (2) LIMITATION.—Nothing in this subsection
19 shall be construed to permit, and nothing does per-
20 mit, the Federal Trade Commission to issue regula-
21 tions requiring, or according greater legal status to,
22 the implementation of or application of a specific
23 technology or technological specifications for meeting
24 the requirements of this title.

1 **SEC. 302. REQUIREMENTS FOR A PERSONAL DATA PRIVACY**
2 **AND SECURITY PROGRAM.**

3 (a) **PERSONAL DATA PRIVACY AND SECURITY PRO-**
4 **GRAM.**—A business entity subject to this subtitle shall
5 comply with the following safeguards and any other ad-
6 ministrative, technical, or physical safeguards identified by
7 the Federal Trade Commission in a rulemaking process
8 pursuant to section 553 of title 5, United States Code,
9 for the protection of sensitive personally identifiable infor-
10 mation:

11 (1) **SCOPE.**—A business entity shall implement
12 a comprehensive personal data privacy and security
13 program that includes administrative, technical, and
14 physical safeguards appropriate to the size and com-
15 plexity of the business entity and the nature and
16 scope of its activities.

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

19 (A) ensure the privacy, security, and con-
20 fidentiality of sensitive personally identifying in-
21 formation;

22 (B) protect against any anticipated
23 vulnerabilities to the privacy, security, or integ-
24 rity of sensitive personally identifying informa-
25 tion; and

1 (C) protect against unauthorized access to
2 use of sensitive personally identifying informa-
3 tion that could ~~result in substantial harm or in-~~
4 ~~convenience to any individual~~ *create a significant*
5 *risk of harm or fraud to any individual.*

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

8 (A) identify reasonably foreseeable internal
9 and external vulnerabilities that could result in
10 unauthorized access, disclosure, use, or alter-
11 ation of sensitive personally identifiable infor-
12 mation or systems containing sensitive person-
13 ally identifiable information;

14 (B) assess the likelihood of and potential
15 damage from unauthorized access, disclosure,
16 use, or alteration of sensitive personally identifi-
17 able information;

18 (C) assess the sufficiency of its policies,
19 technologies, and safeguards in place to control
20 and minimize risks from unauthorized access,
21 disclosure, use, or alteration of sensitive person-
22 ally identifiable information; and

23 (D) assess the vulnerability of sensitive
24 personally identifiable information during de-
25 struction and disposal of such information, in-

1 including through the disposal or retirement of
2 hardware.

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

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

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

12 (i) control access to systems and fa-
13 cilities containing sensitive personally iden-
14 tifiable information, including controls to
15 authenticate and permit access only to au-
16 thorized individuals;

17 (ii) detect actual and attempted
18 fraudulent, unlawful, or unauthorized ac-
19 cess, disclosure, use, or alteration of sen-
20 sitive personally identifiable information,
21 including by employees and other individ-
22 uals otherwise authorized to have access;

23 (iii) protect sensitive personally identi-
24 fiable information during use, trans-
25 mission, storage, and disposal by

1 encryption, redaction, or access controls
2 that are widely accepted as an effective in-
3 dustry practice or industry standard, or
4 other reasonable means (including as di-
5 rected for disposal of records under section
6 628 of the Fair Credit Reporting Act (15
7 U.S.C. 1681w) and the implementing regu-
8 lations of such Act as set forth in section
9 682 of title 16, Code of Federal Regula-
10 tions);

11 (iv) ensure that sensitive personally
12 identifiable information is properly de-
13 stroyed and disposed of, including during
14 the destruction of computers, diskettes,
15 and other electronic media that contain
16 sensitive personally identifiable informa-
17 tion;

18 (v) trace access to records containing
19 sensitive personally identifiable information
20 so that the business entity can determine
21 who accessed or acquired such sensitive
22 personally identifiable information per-
23 taining to specific individuals; and

24 (vi) ensure that no third party or cus-
25 tomer of the business entity is authorized

1 to access or acquire sensitive personally
2 identifiable information without the busi-
3 ness entity first performing sufficient due
4 diligence to ascertain, with reasonable cer-
5 tainty, that such information is being
6 sought for a valid legal purpose.

7 (b) TRAINING.—Each business entity subject to this
8 subtitle shall take steps to ensure employee training and
9 supervision for implementation of the data security pro-
10 gram of the business entity.

11 (c) VULNERABILITY TESTING.—

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

18 (2) FREQUENCY.—The frequency and nature of
19 the tests required under paragraph (1) shall be de-
20 termined by the risk assessment of the business enti-
21 ty under subsection (a)(3).

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

1 (1) exercise appropriate due diligence in select-
2 ing those service providers for responsibilities related
3 to sensitive personally identifiable information, and
4 take reasonable steps to select and retain service
5 providers that are capable of maintaining appro-
6 priate safeguards for the security, privacy, and in-
7 tegrity of the sensitive personally identifiable infor-
8 mation at issue; and

9 (2) require those service providers by contract
10 to implement and maintain appropriate measures de-
11 signed to meet the objectives and requirements gov-
12 erning entities subject to section 301, this section,
13 and subtitle B.

14 (e) PERIODIC ASSESSMENT AND PERSONAL DATA
15 PRIVACY AND SECURITY MODERNIZATION.—Each busi-
16 ness entity subject to this subtitle shall on a regular basis
17 monitor, evaluate, and adjust, as appropriate its data pri-
18 vacy and security program in light of any relevant changes
19 in—

20 (1) technology;

21 (2) the sensitivity of personally identifiable in-
22 formation;

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

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

3 (A) mergers and acquisitions;

4 (B) alliances and joint ventures;

5 (C) outsourcing arrangements;

6 (D) bankruptcy; and

7 (E) changes to sensitive personally identifi-
8 able information systems.

9 (f) IMPLEMENTATION TIMELINE.—Not later than 1
10 year after the date of enactment of this Act, a business
11 entity subject to the provisions of this subtitle shall imple-
12 ment a data privacy and security program pursuant to this
13 subtitle.

14 **SEC. 303. ENFORCEMENT.**

15 (a) CIVIL PENALTIES.—

16 (1) IN GENERAL.—Any business entity that vio-
17 lates the provisions of sections 301 or 302 shall be
18 subject to civil penalties of not more than \$5,000
19 per violation per day while such a violation exists,
20 with a maximum of \$500,000 per violation.

21 (2) INTENTIONAL OR WILLFUL VIOLATION.—A
22 business entity that intentionally or willfully violates
23 the provisions of sections 301 or 302 shall be subject
24 to additional penalties in the amount of \$5,000 per

1 violation per day while such a violation exists, with
2 a maximum of an additional \$500,000 per violation.

3 (3) **EQUITABLE RELIEF.**—A business entity en-
4 gaged in interstate commerce that violates this sec-
5 tion may be enjoined from further violations by a
6 court of competent jurisdiction.

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

11 (b) **FEDERAL TRADE COMMISSION AUTHORITY.**—
12 Any ~~data broker~~*business entity* shall have the provisions
13 of this subtitle enforced against it by the Federal Trade
14 Commission.

15 (c) **STATE ENFORCEMENT.**—

16 (1) **CIVIL ACTIONS.**—In any case in which the
17 attorney general of a State or any State or local law
18 enforcement agency authorized by the State attorney
19 general or by State statute to prosecute violations of
20 consumer protection law, has reason to believe that
21 an interest of the residents of that State has been
22 or is threatened or adversely affected by the acts or
23 practices of a ~~data broker~~*business entity* that violate
24 this subtitle, the State may bring a civil action on
25 behalf of the residents of that State in a district

1 court of the United States of appropriate jurisdic-
2 tion, or any other court of competent jurisdiction,
3 to—

4 (A) enjoin that act or practice;

5 (B) enforce compliance with this subtitle;

6 or

7 (C) obtain civil penalties of not more than
8 \$5,000 per violation per day while such viola-
9 tions persist, up to a maximum of \$500,000 per
10 violation.

11 (2) NOTICE.—

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

16 (i) a written notice of that action; and

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

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

1 (C) NOTIFICATION WHEN PRACTICABLE.—

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

7 (3) FEDERAL TRADE COMMISSION AUTHOR-
8 ITY.—Upon receiving notice under paragraph (2),
9 the Federal Trade Commission shall have the right
10 to—

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

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

16 (C) file petitions for appeal.

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

1 (5) RULE OF CONSTRUCTION.—For purposes of
2 bringing any civil action under paragraph (1) noth-
3 ing in this subtitle shall be construed to prevent an
4 attorney general of a State from exercising the pow-
5 ers conferred on the attorney general by the laws of
6 that State to—

7 (A) conduct investigations;

8 (B) administer oaths and affirmations; or

9 (C) compel the attendance of witnesses or
10 the production of documentary and other evi-
11 dence.

12 (6) VENUE; SERVICE OF PROCESS.—

13 (A) VENUE.—Any action brought under
14 this subsection may be brought in the district
15 court of the United States that meets applicable
16 requirements relating to venue under section
17 1391 of title 28, United States Code.

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

21 (i) is an inhabitant; or

22 (ii) may be found.

23 (d) NO PRIVATE CAUSE OF ACTION.—Nothing in
24 this subtitle establishes a private cause of action against

1 a business entity for violation of any provision of this sub-
2 title.

3 **SEC. 304. RELATION TO OTHER LAWS.**

4 (a) IN GENERAL.—No State may require any busi-
5 ness entity subject to this subtitle to comply with any re-
6 quirements with respect to administrative, technical, and
7 physical safeguards for the protection of sensitive person-
8 ally identifying information.

9 (b) LIMITATIONS.—Nothing in this subtitle shall be
10 construed to modify, limit, or supersede the operation of
11 the Gramm-Leach-Bliley Act or its implementing regula-
12 tions, including those adopted or enforced by States.

13 **Subtitle B—Security Breach**
14 **Notification**

15 **SEC. 311. NOTICE TO INDIVIDUALS.**

16 (a) IN GENERAL.—Any agency, or business entity en-
17 gaged in interstate commerce, that uses, accesses, trans-
18 mits, stores, disposes of or collects sensitive personally
19 identifiable information shall, following the discovery of a
20 security breach of such information, notify any resident
21 of the United States whose sensitive personally identifiable
22 information has been, or is reasonably believed to have
23 been, accessed, or acquired.

24 (b) OBLIGATION OF OWNER OR LICENSEE.—

1 (1) NOTICE TO OWNER OR LICENSEE.—Any
2 agency, or business entity engaged in interstate com-
3 merce, that uses, accesses, transmits, stores, dis-
4 poses of, or collects sensitive personally identifiable
5 information that the agency or business entity does
6 not own or license shall notify the owner or licensee
7 of the information following the discovery of a secu-
8 rity breach involving such information.

9 (2) NOTICE BY OWNER, LICENSEE OR OTHER
10 DESIGNATED THIRD PARTY.—Nothing in this sub-
11 title shall prevent or abrogate an agreement between
12 an agency or business entity required to give notice
13 under this section and a designated third party, in-
14 cluding an owner or licensee of the sensitive person-
15 ally identifiable information subject to the security
16 breach, to provide the notifications required under
17 subsection (a).

18 (3) BUSINESS ENTITY RELIEVED FROM GIVING
19 NOTICE.—A business entity obligated to give notice
20 under subsection (a) shall be relieved of such obliga-
21 tion if an owner or licensee of the sensitive person-
22 ally identifiable information subject to the security
23 breach, or other designated third party, provides
24 such notification.

25 (c) TIMELINESS OF NOTIFICATION.—

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

5 (2) REASONABLE DELAY.—Reasonable delay
6 under this subsection may include any time nec-
7 essary to determine the scope of the security breach,
8 prevent further disclosures, and restore the reason-
9 able integrity of the data system and provide notice
10 to law enforcement when required.

11 (3) BURDEN OF PROOF.—The agency, business
12 entity, owner, or licensee required to provide notifi-
13 cation under this section shall have the burden of
14 demonstrating that all notifications were made as re-
15 quired under this subtitle, including evidence dem-
16 onstrating the reasons for any delay.

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

19 (1) IN GENERAL.—If a Federal law enforce-
20 ment agency determines that the notification re-
21 quired under this section would impede a criminal
22 investigation, such notification shall be delayed upon
23 written notice from such Federal law enforcement
24 agency to the agency or business entity that experi-
25 enced the breach.

1 (2) EXTENDED DELAY OF NOTIFICATION.—If
2 the notification required under subsection (a) is de-
3 layed pursuant to paragraph (1), an agency or busi-
4 ness entity shall give notice 30 days after the day
5 such law enforcement delay was invoked unless a
6 Federal law enforcement agency provides written no-
7 tification that further delay is necessary.

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

13 **SEC. 312. EXEMPTIONS.**

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

16 (1) IN GENERAL.—Section 311 shall not apply
17 to an agency or business entity if the agency or busi-
18 ness entity certifies, in writing, that notification of
19 the security breach as required by section 311 rea-
20 sonably could be expected to—

21 (A) cause damage to the national security;

22 or

23 (B) hinder a law enforcement investigation
24 or the ability of the agency to conduct law en-
25 forcement investigations.

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

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

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

8 (C) restrain competition.

9 (3) NOTICE.—In every case in which an agency
10 or business agency issues a certification under para-
11 graph (1), the certification, accompanied by a de-
12 scription of the factual basis for the certification,
13 shall be immediately provided to the United States
14 Secret Service.

15 (4) SECRET SERVICE REVIEW OF CERTIFI-
16 CATIONS.—

17 (A) IN GENERAL.—The United States Se-
18 cret Service may review a certification provided
19 by an agency under paragraph (3), and shall re-
20 view a certification provided by a business enti-
21 ty under paragraph (3), to determine whether
22 an exemption under paragraph (1) is merited.
23 Such review shall be completed not later than
24 10 business days after the date of receipt of the

1 certification, except as provided in paragraph
2 (5)(C).

3 (B) NOTICE.—Upon completing a review
4 under subparagraph (A) the United States Se-
5 cret Service shall immediately notify the agency
6 or business entity, in writing, of its determina-
7 tion of whether an exemption under paragraph
8 (1) is merited.

9 (C) EXEMPTION.—The exemption under
10 paragraph (1) shall not apply if the United
11 States Secret Service determines under this
12 paragraph that the exemption is not merited.

13 (5) ADDITIONAL AUTHORITY OF THE SECRET
14 SERVICE.—

15 (A) IN GENERAL.—In determining under
16 paragraph (4) whether an exemption under
17 paragraph (1) is merited, the United States Se-
18 cret Service may request additional information
19 from the agency or business entity regarding
20 the basis for the claimed exemption, if such ad-
21 ditional information is necessary to determine
22 whether the exemption is merited.

23 (B) REQUIRED COMPLIANCE.—Any agency
24 or business entity that receives a request for

1 additional information under subparagraph (A)
2 shall cooperate with any such request.

3 (C) TIMING.—If the United States Secret
4 Service requests additional information under
5 subparagraph (A), the United States Secret
6 Service shall notify the agency or business enti-
7 ty not later than 10 business days after the
8 date of receipt of the additional information
9 whether an exemption under paragraph (1) is
10 merited.

11 (b) SAFE HARBOR.—An agency or business entity
12 will be exempt from the notice requirements under section
13 311, if—

14 (1) a risk assessment concludes that—

15 (A) there is no significant risk that a secu-
16 rity breach has resulted in, or will result in,
17 harm to the individuals whose sensitive person-
18 ally identifiable information was subject to the
19 security breach, with the encryption of such in-
20 formation establishing a presumption that no
21 significant risk exists; or

22 (B) there is no significant risk that a secu-
23 rity breach has resulted in, or will result in,
24 harm to the individuals whose sensitive person-
25 ally identifiable information was subject to the

1 security breach, with the rendering of such sen-
2 sitive personally identifiable information indeci-
3 pherable through the use of best practices or
4 methods, such as redaction, access controls, or
5 other such mechanisms, which are widely ac-
6 cepted as an effective industry practice, or an
7 effective industry standard, establishing a pre-
8 sumption that no significant risk exists;

9 (2) without unreasonable delay, but not later
10 than 45 days after the discovery of a security
11 breach, unless extended by the United States Secret
12 Service, the agency or business entity notifies the
13 United States Secret Service, in writing, of—

14 (A) the results of the risk assessment; and

15 (B) its decision to invoke the risk assess-
16 ment exemption; and

17 (3) the United States Secret Service does not
18 indicate, in writing, within 10 business days from re-
19 ceipt of the decision, that notice should be given.

20 (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

21 (1) IN GENERAL.—A business entity will be ex-
22 empt from the notice requirement under section 311
23 if the business entity utilizes or participates in a se-
24 curity program that—

1 (A) is designed to block the use of the sen-
2 sitive personally identifiable information to ini-
3 tiate unauthorized financial transactions before
4 they are charged to the account of the indi-
5 vidual; and

6 (B) provides for notice to affected individ-
7 uals after a security breach that has resulted in
8 fraud or unauthorized transactions.

9 (2) LIMITATION.—The exemption by this sub-
10 section does not apply if—

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

17 (B) the security breach includes both the
18 individual's credit card number and the individ-
19 ual's first and last name.

20 **SEC. 313. METHODS OF NOTICE.**

21 An agency or business entity shall be in compliance
22 with section 311 if it provides both:

23 (1) INDIVIDUAL NOTICE.—Notice to individuals
24 by 1 of the following means:

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

4 (B) Telephone notice to the individual per-
5 sonally.

6 (C) E-mail notice, if the individual has
7 consented to receive such notice and the notice
8 is consistent with the provisions permitting elec-
9 tronic transmission of notices under section 101
10 of the Electronic Signatures in Global and Na-
11 tional Commerce Act (15 U.S.C. 7001).

12 (2) MEDIA NOTICE.—Notice to major media
13 outlets serving a State or jurisdiction, if the number
14 of residents of such State whose sensitive personally
15 identifiable information was, or is reasonably be-
16 lieved to have been, *accessed or* acquired by an unau-
17 thorized person exceeds 5,000.

18 **SEC. 314. CONTENT OF NOTIFICATION.**

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

22 (1) a description of the categories of sensitive
23 personally identifiable information that was, or is
24 reasonably believed to have been, *accessed or* ac-
25 quired by an unauthorized person;

1 (2) a toll-free number—

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

5 (B) from which the individual may learn
6 what types of sensitive personally identifiable
7 information the agency or business entity main-
8 tained about that individual; and

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

11 (b) **ADDITIONAL CONTENT.**—Notwithstanding sec-
12 tion 319, a State may require that a notice under sub-
13 section (a) shall also include information regarding victim
14 protection assistance provided for by that State.

15 **SEC. 315. COORDINATION OF NOTIFICATION WITH CREDIT**
16 **REPORTING AGENCIES.**

17 If an agency or business entity is required to provide
18 notification to more than 5,000 individuals under section
19 311(a), the agency or business entity shall also notify all
20 consumer reporting agencies that compile and maintain
21 files on consumers on a nationwide basis (as defined in
22 section 603(p) of the Fair Credit Reporting Act (15
23 U.S.C. 1681a(p)) of the timing and distribution of the no-
24 tices. Such notice shall be given to the consumer credit
25 reporting agencies without unreasonable delay and, if it

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

3 **SEC. 316. NOTICE TO LAW ENFORCEMENT.**

4 (a) SECRET SERVICE.—Any business entity or agen-
5 cy shall notify the United States Secret Service of the fact
6 that a security breach has occurred if—

7 (1) the number of individuals whose sensitive
8 personally identifying information was, or is reason-
9 ably believed to have been *accessed or* acquired by an
10 unauthorized person exceeds 10,000;

11 (2) the security breach involves a database,
12 networked or integrated databases, or other data
13 system containing the sensitive personally identifi-
14 able information of more than 1,000,000 individuals
15 nationwide;

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

18 (4) the security breach involves primarily sen-
19 sitive personally identifiable information of individ-
20 uals known to the agency or business entity to be
21 employees and contractors of the Federal Govern-
22 ment involved in national security or law enforce-
23 ment.

1 (b) NOTICE TO OTHER LAW ENFORCEMENT AGEN-
2 CIES.—The United States Secret Service shall be respon-
3 sible for notifying—

4 (1) the Federal Bureau of Investigation, if the
5 security breach involves espionage, foreign counter-
6 intelligence, information protected against unauthor-
7 ized disclosure for reasons of national defense or for-
8 eign relations, or Restricted Data (as that term is
9 defined in section 11y of the Atomic Energy Act of
10 1954 (42 U.S.C. 2014(y)), except for offenses af-
11 fecting the duties of the United States Secret Serv-
12 ice under section 3056(a) of title 18, United States
13 Code;

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

16 (3) the attorney general of each State affected
17 by the security breach.

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

20 (1) Notice under subsection (a) shall be deliv-
21 ered as promptly as possible, but not later than 14
22 days after discovery of the events requiring notice.

23 (2) Notice under subsection (b) shall be deliv-
24 ered not later than 14 days after the Service receives

1 notice of a security breach from an agency or busi-
2 ness entity.

3 **SEC. 317. ENFORCEMENT.**

4 (a) CIVIL ACTIONS BY THE ATTORNEY GENERAL.—

5 The Attorney General may bring a civil action in the ap-
6 propriate United States district court against any business
7 entity that engages in conduct constituting a violation of
8 this subtitle and, upon proof of such conduct by a prepon-
9 derance of the evidence, such business entity shall be sub-
10 ject to a civil penalty of not more than \$1,000 per day
11 per individual whose sensitive personally identifiable infor-
12 mation was, or is reasonably believed to have been,
13 accessed or acquired by an unauthorized person, up to a
14 maximum of \$1,000,000 per violation, unless such conduct
15 is found to be willful or intentional.

16 (b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-
17 ERAL.—

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

23 (A) enjoining such act or practice; or

24 (B) enforcing compliance with this subtitle.

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

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

9 (d) FRAUD ALERT.—Section 605A(b)(1) of the Fair
10 Credit Reporting Act (15 U.S.C. 1681c–1(b)(1)) is
11 amended by inserting “, or evidence that the consumer
12 has received notice that the consumer’s financial informa-
13 tion has or may have been compromised,” after “identity
14 theft report”.

15 **SEC. 318. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

16 (a) IN GENERAL.—

17 (1) CIVIL ACTIONS.—In any case in which the
18 attorney general of a State or any State or local law
19 enforcement agency authorized by the State attorney
20 general or by State statute to prosecute violations of
21 consumer protection law, has reason to believe that
22 an interest of the residents of that State has been
23 or is threatened or adversely affected by the engage-
24 ment of a business entity in a practice that is pro-
25 hibited under this subtitle, the State or the State or

1 local law enforcement agency on behalf of the resi-
2 dents of the agency's jurisdiction, may bring a civil
3 action on behalf of the residents of the State or ju-
4 risdiction in a district court of the United States of
5 appropriate jurisdiction or any other court of com-
6 petent jurisdiction, including a State court, to—

7 (A) enjoin that practice;

8 (B) enforce compliance with this subtitle;

9 or

10 (C) civil penalties of not more than \$1,000
11 per day per individual whose sensitive person-
12 ally identifiable information was, or is reason-
13 ably believed to have been, accessed or acquired
14 by an unauthorized person, up to a maximum
15 of \$1,000,000 per violation, unless such con-
16 duct is found to be willful or intentional.

17 (2) NOTICE.—

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

22 (i) written notice of the action; and

23 (ii) a copy of the complaint for the ac-
24 tion.

25 (B) EXEMPTION.—

1 (i) IN GENERAL.—Subparagraph (A)
2 shall not apply with respect to the filing of
3 an action by an attorney general of a State
4 under this subtitle, if the State attorney
5 general determines that it is not feasible to
6 provide the notice described in such sub-
7 paragraph before the filing of the action.

8 (ii) NOTIFICATION.—In an action de-
9 scribed in clause (i), the attorney general
10 of a State shall provide notice and a copy
11 of the complaint to the Attorney General
12 at the time the State attorney general files
13 the action.

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

17 (1) move to stay the action, pending the final
18 disposition of a pending Federal proceeding or ac-
19 tion;

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

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

1 (4) file petitions for appeal.

2 (c) PENDING PROCEEDINGS.—If the Attorney Gen-
3 eral has instituted a proceeding or action for a violation
4 of this subtitle or any regulations thereunder, no attorney
5 general of a State may, during the pendency of such pro-
6 ceeding or action, bring an action under this subtitle
7 against any defendant named in such criminal proceeding
8 or civil action for any violation that is alleged in that pro-
9 ceeding or action.

10 (d) CONSTRUCTION.—For purposes of bringing any
11 civil action under subsection (a), nothing in this subtitle
12 regarding notification shall be construed to prevent an at-
13 torney general of a State from exercising the powers con-
14 ferred on such attorney general by the laws of that State
15 to—

16 (1) conduct investigations;

17 (2) administer oaths or affirmations; or

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

20 (e) VENUE; SERVICE OF PROCESS.—

21 (1) VENUE.—Any action brought under sub-
22 section (a) may be brought in—

23 (A) the district court of the United States
24 that meets applicable requirements relating to

1 venue under section 1391 of title 28, United
2 States Code; or

3 (B) another court of competent jurisdic-
4 tion.

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

8 (A) is an inhabitant; or

9 (B) may be found.

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

14 **SEC. 319. EFFECT ON FEDERAL AND STATE LAW.**

15 The provisions of this subtitle shall supersede any
16 other provision of Federal law or any provision of law of
17 any State relating to notification by a business entity en-
18 gaged in interstate commerce or an agency of a security
19 breach, except as provided in section 314(b).

20 **SEC. 320. AUTHORIZATION OF APPROPRIATIONS.**

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

1 **SEC. 321. REPORTING ON RISK ASSESSMENT EXEMPTIONS.**

2 The United States Secret Service shall report to Con-
3 gress not later than 18 months after the date of enactment
4 of this Act, and upon the request by Congress thereafter,
5 on—

6 (1) the number and nature of the security
7 breaches described in the notices filed by those busi-
8 ness entities invoking the risk assessment exemption
9 under section 312(b) and the response of the United
10 States Secret Service to such notices; and

11 (2) the number and nature of security breaches
12 subject to the national security and law enforcement
13 exemptions under section 312(a), provided that such
14 report may not disclose the contents of any risk as-
15 sessment provided to the United States Secret Serv-
16 ice pursuant to this subtitle.

17 **SEC. 322. EFFECTIVE DATE.**

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

21 **Subtitle C—Office of Federal**
22 **Identity Protection**

23 **SEC. 331. OFFICE OF FEDERAL IDENTITY PROTECTION.**

24 (a) **ESTABLISHMENT.**—There is established in the
25 Federal Trade Commission an Office of Federal Identity
26 Protection.

1 (b) DUTIES.—The Office of Federal Identity Protec-
2 tion shall be responsible for assisting each consumer
3 with—

4 (1) addressing the consequences of the theft or
5 compromise of the personally identifiable informa-
6 tion of that consumer;

7 (2) accessing remedies provided under Federal
8 law and providing information about remedies avail-
9 able under State law;

10 (3) restoring the accuracy of—

11 (A) the personally identifiable information
12 of that consumer; and

13 (B) records containing the personally iden-
14 tifiable information of that consumer that were
15 stolen or compromised; and

16 (4) retrieving any stolen or compromised per-
17 sonally identifiable information of that consumer.

18 (c) ACTIVITIES.—In order to perform the duties re-
19 quired under subsection (b), the Office of Federal Identity
20 Protection shall carry out the following activities:

21 (1) Establish a website, easily and conspicu-
22 ously accessible from fte.gov, dedicated to assisting
23 consumers with the retrieval of the stolen or com-
24 promised personally identifiable information of the
25 consumer.

1 (2) Maintain a toll-free phone number to help
2 answer questions concerning identity theft from con-
3 sumers.

4 (3) Establish online and offline consumer-serv-
5 ice teams to assist consumers seeking the retrieval
6 of the personally identifiable information of the con-
7 sumer.

8 (4) Provide guidance and information to service
9 organizations or pro bono legal services programs
10 that offer individualized assistance or counseling to
11 victims of identity theft.

12 (5) Establish a reasonable standard for deter-
13 mining when an individual becomes a victim of iden-
14 tity theft.

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

18 (7) Permit an individual to use the Office of
19 Federal Identity Protection certification—

20 (A) in all Federal, State, and local juris-
21 dictions, in lieu of a police report or any other
22 document required by State or local law, as a
23 prerequisite to accessing business records of
24 transactions done by someone claiming to be
25 the individual; and

1 (B) to establish the eligibility of that indi-
2 vidual for—

3 (i) the fraud alert protections under
4 section 605A of the Fair Credit Reporting
5 Act (15 U.S.C. 1681e-1); and

6 (ii) the reporting protections under
7 section 605B(a) of the Fair Credit Report-
8 ing Act (15 U.S.C. 1681e-2(a)).

9 (8) Coordinate, as the Office determines nec-
10 essary, with the designated Chief Privacy Officer of
11 each Federal agency, or any other designated senior
12 official in such agency in charge of privacy, in order
13 to meet the duties of assisting consumers as re-
14 quired under subsection (b).

15 (9) In addition to the requirements in para-
16 graphs (1) through (7), the Federal Trade Commis-
17 sion shall promulgate regulations that enable the Of-
18 fice of Federal Identity Protection to help consumers
19 restore their stolen or otherwise compromised per-
20 sonally identifiable information quickly and inexpen-
21 sively.

22 (d) AUTHORIZATION OF APPROPRIATIONS.—There
23 are authorized to be appropriated for the Office of Federal
24 Identity Protection such sums as are necessary for fiscal
25 year 2010 and each of the 4 succeeding fiscal years.

1 **TITLE IV—GOVERNMENT AC-**
2 **CESS TO AND USE OF COM-**
3 **MERCIAL DATA**

4 **SEC. 401. GENERAL SERVICES ADMINISTRATION REVIEW**
5 **OF CONTRACTS.**

6 (a) IN GENERAL.—In considering contract awards
7 totaling more than \$500,000 and entered into after the
8 date of enactment of this Act with data brokers, the Ad-
9 ministrator of the General Services Administration shall
10 evaluate—

11 (1) the data privacy and security program of a
12 data broker to ensure the privacy and security of
13 data containing personally identifiable information,
14 including whether such program adequately address-
15 es privacy and security threats created by malicious
16 software or code, or the use of peer-to-peer file shar-
17 ing software;

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

20 (3) the extent to which the databases and sys-
21 tems containing personally identifiable information
22 of a data broker have been compromised by security
23 breaches; and

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

4 (b) COMPLIANCE SAFE HARBOR.—The data privacy
5 and security program of a data broker shall be deemed
6 sufficient for the purposes of subsection (a), if the data
7 broker complies with or provides protection equal to indus-
8 try standards, as identified by the Federal Trade Commis-
9 sion, that are applicable to the type of personally identifi-
10 able information involved in the ordinary course of busi-
11 ness of such data broker.

12 (c) PENALTIES.—In awarding contracts with data
13 brokers for products or services related to access, use,
14 compilation, distribution, processing, analyzing, or evalu-
15 ating personally identifiable information, the Adminis-
16 trator of the General Services Administration shall—

17 (1) include monetary or other penalties—

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

20 (B) if a contractor knows or has reason to
21 know that the personally identifiable informa-
22 tion being provided is inaccurate, and provides
23 such inaccurate information; and

24 (2) require a data broker that engages service
25 providers not subject to subtitle A of title III for re-

1 sponsibilities related to sensitive personally identifi-
2 able information to—

3 (A) exercise appropriate due diligence in
4 selecting those service providers for responsibil-
5 ities related to personally identifiable informa-
6 tion;

7 (B) take reasonable steps to select and re-
8 tain service providers that are capable of main-
9 taining appropriate safeguards for the security,
10 privacy, and integrity of the personally identifi-
11 able information at issue; and

12 (C) require such service providers, by con-
13 tract, to implement and maintain appropriate
14 measures designed to meet the objectives and
15 requirements in title III.

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

20 **SEC. 402. REQUIREMENT TO AUDIT INFORMATION SECU-**
21 **RITY PRACTICES OF CONTRACTORS AND**
22 **THIRD PARTY BUSINESS ENTITIES.**

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

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

3 (2) in paragraph (8), by striking the period and
4 inserting “; and”; and

5 (3) by adding at the end the following:

6 “(9) procedures for evaluating and auditing the
7 information security practices of contractors or third
8 party business entities supporting the information
9 systems or operations of the agency involving per-
10 sonally identifiable information (as that term is de-
11 fined in section 3 of the Personal Data Privacy and
12 Security Act of 2009) and ensuring remedial action
13 to address any significant deficiencies.”.

14 **SEC. 403. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT**
15 **USE OF COMMERCIAL INFORMATION SERV-**
16 **ICES CONTAINING PERSONALLY IDENTIFI-**
17 **ABLE INFORMATION.**

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

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

22 (2) in subparagraph (A)(ii), by striking the pe-
23 riod and inserting “; or”; and

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

1 “(iii) purchasing or subscribing for a
2 fee to personally identifiable information
3 from a data broker (as such terms are de-
4 fined in section 3 of the Personal Data
5 Privacy and Security Act of 2009).”.

6 (b) LIMITATION.—Notwithstanding any other provi-
7 sion of law, commencing 1 year after the date of enact-
8 ment of this Act, no Federal agency may enter into a con-
9 tract with a data broker to access for a fee any database
10 consisting primarily of personally identifiable information
11 concerning United States persons (other than news report-
12 ing or telephone directories) unless the head of such de-
13 partment or agency—

14 (1) completes a privacy impact assessment
15 under section 208 of the E-Government Act of 2002
16 (44 U.S.C. 3501 note), which shall subject to the
17 provision in that Act pertaining to sensitive informa-
18 tion, include a description of—

19 (A) such database;

20 (B) the name of the data broker from
21 whom it is obtained; and

22 (C) the amount of the contract for use;

23 (2) adopts regulations that specify—

24 (A) the personnel permitted to access, ana-
25 lyze, or otherwise use such databases;

1 (B) standards governing the access, anal-
2 ysis, or use of such databases;

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

8 (D) standards limiting the retention and
9 redisclosure of personally identifiable informa-
10 tion obtained from such databases;

11 (E) procedures ensuring that such data
12 meet standards of accuracy, relevance, com-
13 pleteness, and timeliness;

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

17 (G) applicable mechanisms by which indi-
18 viduals may secure timely redress for any ad-
19 verse consequences wrongly incurred due to the
20 access, analysis, or use of such databases;

21 (H) mechanisms, if any, for the enforce-
22 ment and independent oversight of existing or
23 planned procedures, policies, or guidelines; and

24 (I) an outline of enforcement mechanisms
25 for accountability to protect individuals and the

1 public against unlawful or illegitimate access or
2 use of databases; and

3 (3) incorporates into the contract or other
4 agreement totaling more than \$500,000, provi-
5 sions—

6 (A) providing for penalties—

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

9 (ii) if the entity knows or has reason
10 to know that the personally identifiable in-
11 formation being provided to the Federal
12 department or agency is inaccurate, and
13 provides such inaccurate information; and

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

18 (i) exercise appropriate due diligence
19 in selecting those service providers for re-
20 sponsibilities related to personally identifi-
21 able information;

22 (ii) take reasonable steps to select and
23 retain service providers that are capable of
24 maintaining appropriate safeguards for the
25 security, privacy, and integrity of the per-

1 sonally identifiable information at issue;
2 and

3 (iii) require such service providers, by
4 contract, to implement and maintain ap-
5 propriate measures designed to meet the
6 objectives and requirements in title III.

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

11 (d) STUDY OF GOVERNMENT USE.—

12 (1) SCOPE OF STUDY.—Not later than 180
13 days after the date of enactment of this Act, the
14 Comptroller General of the United States shall con-
15 duct a study and audit and prepare a report on Fed-
16 eral agency actions to address the recommendations
17 in the Government Accountability Office’s April
18 2006 report on agency adherence to key privacy
19 principles in using data brokers or commercial data-
20 bases containing personally identifiable information.

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

1 **SEC. 404. IMPLEMENTATION OF CHIEF PRIVACY OFFICER**
2 **REQUIREMENTS.**

3 (a) DESIGNATION OF THE CHIEF PRIVACY OFFI-
4 CER.—Pursuant to the requirements under section 522 of
5 the Transportation, Treasury, Independent Agencies, and
6 General Government Appropriations Act, 2005 (division H
7 of Public Law 108–447; 118 Stat. 3199) that each agency
8 designate a Chief Privacy Officer, the Department of Jus-
9 tice shall implement such requirements by designating a
10 department-wide Chief Privacy Officer, whose primary
11 role shall be to fulfill the duties and responsibilities of
12 Chief Privacy Officer and who shall report directly to the
13 Deputy Attorney General.

14 (b) DUTIES AND RESPONSIBILITIES OF CHIEF PRI-
15 VACY OFFICER.—In addition to the duties and responsibil-
16 ities outlined under section 522 of the Transportation,
17 Treasury, Independent Agencies, and General Government
18 Appropriations Act, 2005 (division H of Public Law 108–
19 447; 118 Stat. 3199), the Department of Justice Chief
20 Privacy Officer shall—

21 (1) oversee the Department of Justice’s imple-
22 mentation of the requirements under section 403 to
23 conduct privacy impact assessments of the use of
24 commercial data containing personally identifiable
25 information by the Department; and

1 (2) coordinate with the Privacy and Civil Lib-
2 erties Oversight Board, established in the Intel-
3 ligence Reform and Terrorism Prevention Act of
4 2004 (Public Law 108–458), in implementing this
5 section.

Calendar No. 208

111TH CONGRESS
1ST Session
S. 1490

A BILL

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.

NOVEMBER 5, 2009

Reported with amendments