

110TH CONGRESS
1ST SESSION

S. 495

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

FEBRUARY 6, 2007

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

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,*

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

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Personal Data Privacy and Security Act of 2007”.

6 (b) TABLE OF CONTENTS.—The table of contents of
7 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.

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.

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.
- 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-
20 curity, privacy, and confidentiality of that personally
21 identifiable information;

22 (6) individuals whose personal information has
23 been compromised or who have been victims of iden-
24 tity theft should receive the necessary information
25 and assistance to mitigate their damages and to re-

1 store the integrity of their personal information and
2 identities;

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

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

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

17 (10) government access to commercial data can
18 potentially improve safety, law enforcement, and na-
19 tional security; and

20 (11) because government use of commercial
21 data containing personal information potentially af-
22 fects individual privacy, and law enforcement and
23 national security operations, there is a need for Con-
24 gress to exercise oversight over government use of
25 commercial data.

1 **SEC. 3. DEFINITIONS.**

2 In this Act:

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

6 (2) AFFILIATE.—The term “affiliate” means
7 persons related by common ownership or by cor-
8 porate control.

9 (3) BUSINESS ENTITY.—The term “business
10 entity” means any organization, corporation, trust,
11 partnership, sole proprietorship, unincorporated as-
12 sociation, venture established to make a profit, or
13 nonprofit, and any contractor, subcontractor, affil-
14 iate, or licensee thereof engaged in interstate com-
15 merce.

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

19 (5) DATA BROKER.—The term “data broker”
20 means a business entity which for monetary fees or
21 dues regularly engages in the practice of collecting,
22 transmitting, or providing access to sensitive person-
23 ally identifiable information on more than 5,000 in-
24 dividuals who are not the customers or employees of
25 that business entity or affiliate primarily for the

1 purposes of providing such information to non-
2 affiliated third parties on an interstate basis.

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

8 (7) PERSONAL ELECTRONIC RECORD.—

9 (A) IN GENERAL.—The term “personal
10 electronic record” means data associated with
11 an individual contained in a database,
12 networked or integrated databases, or other
13 data system that holds sensitive personally
14 identifiable information of that individual and is
15 provided to nonaffiliated third parties.

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

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

20 (ii) any proprietary assessment or
21 evaluation of an individual or any propri-
22 etary assessment or evaluation of informa-
23 tion about an individual.

24 (8) PERSONALLY IDENTIFIABLE INFORMA-
25 TION.—The term “personally identifiable informa-

1 tion” means any information, or compilation of in-
2 formation, in electronic or digital form serving as a
3 means of identification, as defined by section
4 1028(d)(7) of title 18, United State Code.

5 (9) PUBLIC RECORD SOURCE.—The term “pub-
6 lic record source” means the Congress, any agency,
7 any State or local government agency, the govern-
8 ment of the District of Columbia and governments
9 of the territories or possessions of the United States,
10 and Federal, State or local courts, courts martial
11 and military commissions, that maintain personally
12 identifiable information in records available to the
13 public.

14 (10) SECURITY BREACH.—

15 (A) IN GENERAL.—The term “security
16 breach” means compromise of the security, con-
17 fidentiality, or integrity of computerized data
18 through misrepresentation or actions that result
19 in, or there is a reasonable basis to conclude
20 has resulted in, acquisition of or access to sen-
21 sitive personally identifiable information that is
22 unauthorized or in excess of authorization.

23 (B) EXCLUSION.—The term “security
24 breach” does not include—

1 (i) a good faith acquisition of sensitive
2 personally identifiable information by a
3 business entity or agency, or an employee
4 or agent of a business entity or agency, if
5 the sensitive personally identifiable infor-
6 mation is not subject to further unauthor-
7 ized disclosure; or

8 (ii) the release of a public record, or
9 information derived from a single public
10 record, not otherwise subject to confiden-
11 tiality or nondisclosure requirement, or in-
12 formation obtained from a news report or
13 periodical.

14 (11) SENSITIVE PERSONALLY IDENTIFIABLE IN-
15 FORMATION.—The term “sensitive personally identi-
16 fiable information” means any information or com-
17 pilation of information, in electronic or digital form
18 that includes—

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

22 (i) A non-truncated social security
23 number, driver’s license number, passport
24 number, or alien registration number.

25 (ii) Any 2 of the following:

1 (I) Home address or telephone
2 number.

3 (II) Mother's maiden name, if
4 identified as such.

5 (III) Month, day, and year of
6 birth.

7 (iii) Unique biometric data such as a
8 finger print, voice print, a retina or iris
9 image, or any other unique physical rep-
10 resentation.

11 (iv) A unique account identifier, elec-
12 tronic identification number, user name, or
13 routing code in combination with any asso-
14 ciated security code, access code, or pass-
15 word that is required for an individual to
16 obtain money, goods, services, or any other
17 thing of value; or

18 (B) a financial account number or credit
19 or debit card number in combination with any
20 security code, access code or password that is
21 required for an individual to obtain credit, with-
22 draw funds, or engage in a financial trans-
23 action.

1 **TITLE I—ENHANCING PUNISH-**
2 **MENT FOR IDENTITY THEFT**
3 **AND OTHER VIOLATIONS OF**
4 **DATA PRIVACY AND SECUR-**
5 **RITY**

6 **SEC. 101. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION**
7 **WITH UNAUTHORIZED ACCESS TO PERSON-**
8 **ALLY IDENTIFIABLE INFORMATION.**

9 Section 1961(1) of title 18, United States Code, is
10 amended by inserting “section 1030(a)(2)(D) (relating to
11 fraud and related activity in connection with unauthorized
12 access to sensitive personally identifiable information as
13 defined in the Personal Data Privacy and Security Act of
14 2007,” before “section 1084”.

15 **SEC. 102. CONCEALMENT OF SECURITY BREACHES INVOLV-**
16 **ING SENSITIVE PERSONALLY IDENTIFIABLE**
17 **INFORMATION.**

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

21 **“§ 1040. Concealment of security breaches involving**
22 **sensitive personally identifiable informa-**
23 **tion**

24 “(a) Whoever, having knowledge of a security breach
25 and of the obligation to provide notice of such breach to

1 individuals under title III of the Personal Data Privacy
2 and Security Act of 2007, and having not otherwise quali-
3 fied for an exemption from providing notice under section
4 312 of such Act, intentionally and willfully conceals the
5 fact of such security breach and which breach causes eco-
6 nomic damage to 1 or more persons, shall be fined under
7 this title or imprisoned not more than 5 years, or both.

8 “(b) For purposes of subsection (a), the term ‘person’
9 has the same meaning as in section 1030(e)(12) of title
10 18, United States Code.

11 “(c) Any person seeking an exemption under section
12 312(b) of the Personal Data Privacy and Security Act of
13 2007 shall be immune from prosecution under this section
14 if the United States Secret Service does not indicate, in
15 writing, that such notice be given under section 312(b)(3)
16 of such Act”.

17 (b) CONFORMING AND TECHNICAL AMENDMENTS.—
18 The table of sections for chapter 47 of title 18, United
19 States Code, is amended by adding at the end the fol-
20 lowing:

“1040. Concealment of security breaches involving personally identifiable infor-
mation.”.

21 (c) ENFORCEMENT AUTHORITY.—

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

1 (2) NON-EXCLUSIVITY.—The authority granted
2 in paragraph (1) shall not be exclusive of any exist-
3 ing authority held by any other Federal agency.

4 **SEC. 103. REVIEW AND AMENDMENT OF FEDERAL SEN-**
5 **TENCING GUIDELINES RELATED TO FRAUDU-**
6 **LENT ACCESS TO OR MISUSE OF DIGITIZED**
7 **OR ELECTRONIC PERSONALLY IDENTIFIABLE**
8 **INFORMATION.**

9 (a) REVIEW AND AMENDMENT.—The United States
10 Sentencing Commission, pursuant to its authority under
11 section 994 of title 28, United States Code, and in accord-
12 ance with this section, shall review and, if appropriate,
13 amend the Federal sentencing guidelines (including its
14 policy statements) applicable to persons convicted of using
15 fraud to access, or misuse of, digitized or electronic per-
16 sonally identifiable information, including identity theft or
17 any offense under—

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

20 (2) any other relevant provision.

21 (b) REQUIREMENTS.—In carrying out the require-
22 ments of this section, the United States Sentencing Com-
23 mission shall—

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

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

3 (B) the growing incidences of theft and
4 misuse of digitized or electronic personally iden-
5 tifiable information, including identity theft;
6 and

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

9 (2) consider the extent to which the Federal
10 sentencing guidelines (including its policy state-
11 ments) adequately address violations of the sections
12 amended by this Act to—

13 (A) sufficiently deter and punish such of-
14 fenses; and

15 (B) adequately reflect the enhanced pen-
16 alties established under this Act;

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

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

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

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

3 (B) the sale of fraudulently obtained or
4 stolen personally identifiable information to an
5 individual who is engaged in terrorist activity or
6 aiding other individuals engaged in terrorist ac-
7 tivity; or

8 (C) the sale of fraudulently obtained or
9 stolen personally identifiable information to fi-
10 nance terrorist activity or other criminal activi-
11 ties;

12 (6) make any necessary conforming changes to
13 the Federal sentencing guidelines to ensure that
14 such guidelines (including its policy statements) as
15 described in subsection (a) are sufficiently stringent
16 to deter, and adequately reflect crimes related to
17 fraudulent access to, or misuse of, personally identi-
18 fiable information; and

19 (7) ensure that the Federal sentencing guide-
20 lines adequately meet the purposes of sentencing
21 under section 3553(a)(2) of title 18, United States
22 Code.

23 (c) EMERGENCY AUTHORITY TO SENTENCING COM-
24 MISSION.—The United States Sentencing Commission
25 may, as soon as practicable, promulgate amendments

1 under this section in accordance with procedures estab-
2 lished in section 21(a) of the Sentencing Act of 1987 (28
3 U.S.C. 994 note) as though the authority under that Act
4 had not expired.

5 **TITLE II—DATA BROKERS**

6 **SEC. 201. TRANSPARENCY AND ACCURACY OF DATA COL-** 7 **LECTION.**

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

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

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

22 (2) any data broker that is subject to regulation
23 under the Gramm-Leach-Bliley Act (Public Law
24 106–102);

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

6 (4) information in a personal electronic record
7 that—

8 (A) the data broker has identified as inac-
9 curate, but maintains for the purpose of aiding
10 the data broker in preventing inaccurate infor-
11 mation from entering an individual’s personal
12 electronic record; and

13 (B) is not maintained primarily for the
14 purpose of transmitting or otherwise providing
15 that information, or assessments based on that
16 information, to non-affiliated third parties; and

17 (5) information concerning proprietary meth-
18 odologies, techniques, scores, or algorithms relating
19 to fraud prevention not normally provided to third
20 parties in the ordinary course of business.

21 (c) DISCLOSURES TO INDIVIDUALS.—

22 (1) IN GENERAL.—A data broker shall, upon
23 the request of an individual, disclose to such indi-
24 vidual for a reasonable fee all personal electronic
25 records pertaining to that individual maintained spe-

1 cifically for disclosure to third parties that request
2 information on that individual in the ordinary course
3 of business in the databases or systems of the data
4 broker at the time of such request.

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

9 (d) ACCURACY RESOLUTION PROCESS.—

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

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

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

1 available from a public record source or licen-
2 sor, the data broker shall—

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

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

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

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

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

24 (3) EXTENSION OF REVIEW PERIOD.—The 30-
25 day period described in paragraph (1) may be ex-

1 tended for not more than 30 additional days if a
2 data broker receives information from the individual
3 during the initial 30-day period that is relevant to
4 the completeness or accuracy of any disputed infor-
5 mation.

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

14 (5) DETERMINATION THAT DISPUTE IS FRIVO-
15 LOUS OR IRRELEVANT.—

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

23 (B) NOTICE.—A data broker shall notify
24 an individual of a determination under subpara-

1 graph (A) within a reasonable time by any
2 means available to such data broker.

3 **SEC. 202. ENFORCEMENT.**

4 (a) CIVIL PENALTIES.—

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

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

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

20 (4) OTHER RIGHTS AND REMEDIES.—The
21 rights and remedies available under this subsection
22 are cumulative and shall not affect any other rights
23 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 SECU-**
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, as identified by the
13 Federal Trade Commission, that are applicable to
14 the type of sensitive personally identifiable informa-
15 tion involved in the ordinary course of business of
16 such business entity.

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

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

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

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

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

22 (D) assess the vulnerability of sensitive
23 personally identifiable information during de-
24 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 or other reasonable means (in-
2 cluding as directed for disposal of records
3 under section 628 of the Fair Credit Re-
4 porting Act (15 U.S.C. 1681w) and the
5 implementing regulations of such Act as
6 set forth in section 682 of title 16, Code
7 of Federal Regulations); and

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

15 (b) TRAINING.—Each business entity subject to this
16 subtitle shall take steps to ensure employee training and
17 supervision for implementation of the data security pro-
18 gram of the business entity.

19 (c) VULNERABILITY TESTING.—

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

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

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

9 (1) exercise appropriate due diligence in select-
10 ing those service providers for responsibilities related
11 to sensitive personally identifiable information, and
12 take reasonable steps to select and retain service
13 providers that are capable of maintaining appro-
14 priate safeguards for the security, privacy, and in-
15 tegrity of the sensitive personally identifiable infor-
16 mation at issue; and

17 (2) require those service providers by contract
18 to implement and maintain appropriate measures de-
19 signed to meet the objectives and requirements gov-
20 erning entities subject to section 301, this section,
21 and subtitle B.

22 (e) PERIODIC ASSESSMENT AND PERSONAL DATA
23 PRIVACY AND SECURITY MODERNIZATION.—Each busi-
24 ness entity subject to this subtitle shall on a regular basis
25 monitor, evaluate, and adjust, as appropriate its data pri-

1 vacy and security program in light of any relevant changes
2 in—

3 (1) technology;

4 (2) the sensitivity of personally identifiable in-
5 formation;

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

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

10 (A) mergers and acquisitions;

11 (B) alliances and joint ventures;

12 (C) outsourcing arrangements;

13 (D) bankruptcy; and

14 (E) changes to sensitive personally identifi-
15 able information systems.

16 (f) IMPLEMENTATION TIME LINE.—Not later than 1
17 year after the date of enactment of this Act, a business
18 entity subject to the provisions of this subtitle shall imple-
19 ment a data privacy and security program pursuant to this
20 subtitle.

21 **SEC. 303. ENFORCEMENT.**

22 (a) CIVIL PENALTIES.—

23 (1) IN GENERAL.—Any business entity that vio-
24 lates the provisions of sections 301 or 302 shall be
25 subject to civil penalties of not more than \$5,000

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

3 (2) INTENTIONAL OR WILLFUL VIOLATION.—A
4 business entity that intentionally or willfully violates
5 the provisions of sections 301 or 302 shall be subject
6 to additional penalties in the amount of \$5,000 per
7 violation per day while such a violation exists, with
8 a maximum of an additional \$500,000 per violation.

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

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

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

20 (c) STATE ENFORCEMENT.—

21 (1) CIVIL ACTIONS.—In any case in which the
22 attorney general of a State or any State or local law
23 enforcement agency authorized by the State attorney
24 general or by State statute to prosecute violations of
25 consumer protection law, has reason to believe that

1 an interest of the residents of that State has been
2 or is threatened or adversely affected by the acts or
3 practices of a data broker that violate this subtitle,
4 the State may bring a civil action on behalf of the
5 residents of that State in a district court of the
6 United States of appropriate jurisdiction, or any
7 other court of competent jurisdiction, to—

8 (A) enjoin that act or practice;

9 (B) enforce compliance with this subtitle;

10 or

11 (C) obtain civil penalties of not more than
12 \$5,000 per violation per day while such viola-
13 tions persist, up to a maximum of \$500,000 per
14 violation.

15 (2) NOTICE.—

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

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

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

23 (B) EXCEPTION.—Subparagraph (A) shall
24 not apply with respect to the filing of an action
25 by an attorney general of a State under this

1 subsection, if the attorney general of a State
2 determines that it is not feasible to provide the
3 notice described in this subparagraph before the
4 filing of the action.

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

11 (3) FEDERAL TRADE COMMISSION AUTHOR-
12 ITY.—Upon receiving notice under paragraph (2),
13 the Federal Trade Commission shall have the right
14 to—

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

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

20 (C) file petitions for appeal.

21 (4) PENDING PROCEEDINGS.—If the Federal
22 Trade Commission has instituted a proceeding or ac-
23 tion for a violation of this subtitle or any regulations
24 thereunder, no attorney general of a State may, dur-
25 ing the pendency of such proceeding or action, bring

1 an action under this subsection against any defend-
2 ant named in such criminal proceeding or civil ac-
3 tion for any violation that is alleged in that pro-
4 ceeding or action.

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

11 (A) conduct investigations;

12 (B) administer oaths and affirmations; or

13 (C) compel the attendance of witnesses or
14 the production of documentary and other evi-
15 dence.

16 (6) VENUE; SERVICE OF PROCESS.—

17 (A) VENUE.—Any action brought under
18 this subsection may be brought in the district
19 court of the United States that meets applicable
20 requirements relating to venue under section
21 1391 of title 28, United States Code.

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

25 (i) is an inhabitant; or

1 (ii) may be found.

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

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

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

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

16 **Subtitle B—Security Breach**
17 **Notification**

18 **SEC. 311. NOTICE TO INDIVIDUALS.**

19 (a) IN GENERAL.—Any agency, or business entity en-
20 gaged in interstate commerce, that uses, accesses, trans-
21 mits, stores, disposes of or collects sensitive personally
22 identifiable information shall, following the discovery of a
23 security breach of the systems or databases of such agency
24 or business entity notify any resident of the United States
25 whose sensitive personally identifiable information has

1 been, or is reasonably believed to have been, accessed, or
2 acquired.

3 (b) OBLIGATION OF OWNER OR LICENSEE.—

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

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

21 (3) BUSINESS ENTITY RELIEVED FROM GIVING
22 NOTICE.—A business entity obligated to give notice
23 under subsection (a) shall be relieved of such obliga-
24 tion if an owner or licensee of the sensitive person-
25 ally identifiable information subject to the security

1 breach, or other designated third party, provides
2 such notification.

3 (c) TIMELINESS OF NOTIFICATION.—

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

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

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

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

22 (1) IN GENERAL.—If a Federal law enforce-
23 ment agency determines that the notification re-
24 quired under this section would impede a criminal
25 investigation, such notification shall be delayed upon

1 written notice from such Federal law enforcement
2 agency to the agency or business entity that experi-
3 enced the breach.

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

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

16 **SEC. 312. EXEMPTIONS.**

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

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

24 (A) cause damage to the national security;

25 or

1 (B) hinder a law enforcement investigation
2 or the ability of the agency to conduct law en-
3 forcement investigations.

4 (2) LIMITS ON CERTIFICATIONS.—An agency
5 may not execute a certification under paragraph (1)
6 to—

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

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

11 (C) restrain competition.

12 (3) NOTICE.—In every case in which an agency
13 issues a certification under paragraph (1), the cer-
14 tification, accompanied by a description of the fac-
15 tual basis for the certification, shall be immediately
16 provided to the United States Secret Service.

17 (b) SAFE HARBOR.—An agency or business entity
18 will be exempt from the notice requirements under section
19 311, if—

20 (1) a risk assessment concludes that there is no
21 significant risk that the security breach has resulted
22 in, or will result in, harm to the individuals whose
23 sensitive personally identifiable information was sub-
24 ject to the security breach;

1 (2) without unreasonable delay, but not later
2 than 45 days after the discovery of a security
3 breach, unless extended by the United States Secret
4 Service, the agency or business entity notifies the
5 United States Secret Service, in writing, of—

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

7 (B) its decision to invoke the risk assess-
8 ment exemption; and

9 (3) the United States Secret Service does not
10 indicate, in writing, within 10 days from receipt of
11 the decision, that notice should be given.

12 (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

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

17 (A) is designed to block the use of the sen-
18 sitive personally identifiable information to ini-
19 tiate unauthorized financial transactions before
20 they are charged to the account of the indi-
21 vidual; and

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

1 (2) LIMITATION.—The exemption by this sub-
2 section does not apply if the information subject to
3 the security breach includes sensitive personally
4 identifiable information in addition to the sensitive
5 personally identifiable information identified in sec-
6 tion 3.

7 **SEC. 313. METHODS OF NOTICE.**

8 An agency, or business entity shall be in compliance
9 with section 311 if it provides both:

10 (1) INDIVIDUAL NOTICE.—

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

14 (B) Telephone notice to the individual per-
15 sonally; or

16 (C) Electronic notice, if the primary meth-
17 od used by the agency or business entity to
18 communicate with the individual is by electronic
19 means, or the individual has consented to re-
20 ceive such notice and the notice is consistent
21 with the provisions permitting electronic trans-
22 mission of notices under section 101 of the
23 Electronic Signatures in Global and National
24 Commerce Act (15 U.S.C. 7001).

1 (2) MEDIA NOTICE.—Notice to major media
2 outlets serving a State or jurisdiction, if the number
3 of residents of such State whose sensitive personally
4 identifiable information was, or is reasonably be-
5 lieved to have been, acquired by an unauthorized
6 person exceeds 5,000.

7 **SEC. 314. CONTENT OF NOTIFICATION.**

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

11 (1) a description of the categories of sensitive
12 personally identifiable information that was, or is
13 reasonably believed to have been, acquired by an un-
14 authorized person;

15 (2) a toll-free number or, if the primary method
16 used by the agency or business entity to commu-
17 nicate with the individual is by electronic means, an
18 electronic mail address—

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

22 (B) from which the individual may learn
23 what types of sensitive personally identifiable
24 information the agency or business entity main-
25 tained about that individual; and

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

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

7 **SEC. 315. COORDINATION OF NOTIFICATION WITH CREDIT**
8 **REPORTING AGENCIES.**

9 If an agency or business entity is required to provide
10 notification to more than 1,000 individuals under section
11 311(a), the agency or business entity shall also notify,
12 without unreasonable delay, all consumer reporting agen-
13 cies that compile and maintain files on consumers on a
14 nationwide basis (as defined in section 603(p) of the Fair
15 Credit Reporting Act (15 U.S.C. 1681a(p)) of the timing
16 and distribution of the notices.

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

18 (a) **SECRET SERVICE.**—Any business entity or agen-
19 cy shall give notice of a security breach to the United
20 States Secret Service if—

21 (1) the number of individuals whose sensitive
22 personally identifying information was, or is reason-
23 ably believed to have been acquired by an unauthor-
24 ized person exceeds 10,000;

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

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

8 (4) the security breach involves primarily sen-
9 sitive personally identifiable information of individ-
10 uals known to the agency or business entity to be
11 employees and contractors of the Federal Govern-
12 ment involved in national security or law enforce-
13 ment.

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

17 (1) the Federal Bureau of Investigation, if the
18 security breach involves espionage, foreign counter-
19 intelligence, information protected against unauthor-
20 ized disclosure for reasons of national defense or for-
21 eign relations, or Restricted Data (as that term is
22 defined in section 11y of the Atomic Energy Act of
23 1954 (42 U.S.C. 2014(y)), except for offenses af-
24 fecting the duties of the United States Secret Serv-

1 ice under section 3056(a) of title 18, United States
2 Code;

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

5 (3) the attorney general of each State affected
6 by the security breach.

7 (c) 14-DAY RULE.—The notices to Federal law en-
8 forcement and the attorney general of each State affected
9 by a security breach required under this section shall be
10 delivered as promptly as possible, but not later than 14
11 days after discovery of the events requiring notice.

12 **SEC. 317. ENFORCEMENT.**

13 (a) CIVIL ACTIONS BY THE ATTORNEY GENERAL.—
14 The Attorney General may bring a civil action in the ap-
15 propriate United States district court against any business
16 entity that engages in conduct constituting a violation of
17 this subtitle and, upon proof of such conduct by a prepon-
18 derance of the evidence, such business entity shall be sub-
19 ject to a civil penalty of not more than \$1,000 per day
20 per individual whose sensitive personally identifiable infor-
21 mation was, or is reasonably believed to have been,
22 accessed or acquired by an unauthorized person, up to a
23 maximum of \$1,000,000 per violation, unless such conduct
24 is found to be willful or intentional.

1 (b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-
2 ERAL.—

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

8 (A) enjoining such act or practice; or

9 (B) enforcing compliance with this subtitle.

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

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

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

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

25 (a) IN GENERAL.—

1 (1) CIVIL ACTIONS.—In any case in which the
2 attorney general of a State or any State or local law
3 enforcement agency authorized by the State attorney
4 general or by State statute to prosecute violations of
5 consumer protection law, has reason to believe that
6 an interest of the residents of that State has been
7 or is threatened or adversely affected by the engage-
8 ment of a business entity in a practice that is pro-
9 hibited under this subtitle, the State or the State or
10 local law enforcement agency on behalf of the resi-
11 dents of the agency’s jurisdiction, may bring a civil
12 action on behalf of the residents of the State or ju-
13 risdiction in a district court of the United States of
14 appropriate jurisdiction or any other court of com-
15 petent jurisdiction, including a State court, to—

16 (A) enjoin that practice;

17 (B) enforce compliance with this subtitle;

18 or

19 (C) civil penalties of not more than \$1,000
20 per day per individual whose sensitive person-
21 ally identifiable information was, or is reason-
22 ably believed to have been, accessed or acquired
23 by an unauthorized person, up to a maximum
24 of \$1,000,000 per violation, unless such con-
25 duct is found to be willful or intentional.

1 (2) NOTICE.—

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

6 (i) written notice of the action; and

7 (ii) a copy of the complaint for the ac-
8 tion.

9 (B) EXEMPTION.—

10 (i) IN GENERAL.—Subparagraph (A)
11 shall not apply with respect to the filing of
12 an action by an attorney general of a State
13 under this subtitle, if the State attorney
14 general determines that it is not feasible to
15 provide the notice described in such sub-
16 paragraph before the filing of the action.

17 (ii) NOTIFICATION.—In an action de-
18 scribed in clause (i), the attorney general
19 of a State shall provide notice and a copy
20 of the complaint to the Attorney General
21 at the time the State attorney general files
22 the action.

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

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

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

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

10 (4) file petitions for appeal.

11 (c) PENDING PROCEEDINGS.—If the Attorney Gen-
12 eral has instituted a proceeding or action for a violation
13 of this subtitle or any regulations thereunder, no attorney
14 general of a State may, during the pendency of such pro-
15 ceeding or action, bring an action under this subtitle
16 against any defendant named in such criminal proceeding
17 or civil action for any violation that is alleged in that pro-
18 ceeding or action.

19 (d) CONSTRUCTION.—For purposes of bringing any
20 civil action under subsection (a), nothing in this subtitle
21 regarding notification shall be construed to prevent an at-
22 torney general of a State from exercising the powers con-
23 ferred on such attorney general by the laws of that State
24 to—

25 (1) conduct investigations;

1 (2) administer oaths or affirmations; or

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

4 (e) VENUE; SERVICE OF PROCESS.—

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

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

11 (B) another court of competent jurisdic-
12 tion.

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

16 (A) is an inhabitant; or

17 (B) may be found.

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

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

23 The provisions of this subtitle shall supersede any
24 other provision of Federal law or any provision of law of

1 any State relating to notification of a security breach, ex-
2 cept as provided in section 314(b).

3 **SEC. 320. AUTHORIZATION OF APPROPRIATIONS.**

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

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

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

14 (1) the number and nature of the security
15 breaches described in the notices filed by those busi-
16 ness entities invoking the risk assessment exemption
17 under section 312(b) and the response of the United
18 States Secret Service to such notices; and

19 (2) the number and nature of security breaches
20 subject to the national security and law enforcement
21 exemptions under section 312(a), provided that such
22 report may not disclose the contents of any risk as-
23 sessment provided to the United States Secret Serv-
24 ice pursuant to this subtitle.

1 **SEC. 322. EFFECTIVE DATE.**

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

5 **TITLE IV—GOVERNMENT AC-**
6 **CESS TO AND USE OF COM-**
7 **MERCIAL DATA**

8 **SEC. 401. GENERAL SERVICES ADMINISTRATION REVIEW**
9 **OF CONTRACTS.**

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

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

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

24 (3) the extent to which the databases and sys-
25 tems containing personally identifiable information

1 of a data broker have been compromised by security
2 breaches; and

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

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

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

19 (1) include monetary or other penalties—

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

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

1 (2) require a data broker that engages service
2 providers not subject to subtitle A of title III for re-
3 sponsibilities related to sensitive personally identifi-
4 able information to—

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

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

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

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

1 **SEC. 402. REQUIREMENT TO AUDIT INFORMATION SECU-**
2 **RITY PRACTICES OF CONTRACTORS AND**
3 **THIRD PARTY BUSINESS ENTITIES.**

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

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

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

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

11 “(9) procedures for evaluating and auditing the
12 information security practices of contractors or third
13 party business entities supporting the information
14 systems or operations of the agency involving per-
15 sonally identifiable information (as that term is de-
16 fined in section 3 of the Personal Data Privacy and
17 Security Act of 2007) and ensuring remedial action
18 to address any significant deficiencies.”.

19 **SEC. 403. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT**
20 **USE OF COMMERCIAL INFORMATION SERV-**
21 **ICES CONTAINING PERSONALLY IDENTIFI-**
22 **ABLE INFORMATION.**

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

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

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

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

4 “(iii) purchasing or subscribing for a
5 fee to personally identifiable information
6 from a data broker (as such terms are de-
7 fined in section 3 of the Personal Data
8 Privacy and Security Act of 2007).”.

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

17 (1) completes a privacy impact assessment
18 under section 208 of the E-Government Act of 2002
19 (44 U.S.C. 3501 note), which shall subject to the
20 provision in that Act pertaining to sensitive informa-
21 tion, include a description of—

22 (A) such database;

23 (B) the name of the data broker from
24 whom it is obtained; and

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

1 (2) adopts regulations that specify—

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

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

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

11 (D) standards limiting the retention and
12 redisclosure of personally identifiable informa-
13 tion obtained from such databases;

14 (E) procedures ensuring that such data
15 meet standards of accuracy, relevance, com-
16 pleteness, and timeliness;

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

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

1 (H) mechanisms, if any, for the enforce-
2 ment and independent oversight of existing or
3 planned procedures, policies, or guidelines; and

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

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

11 (A) providing for penalties—

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

14 (ii) if the entity knows or has reason
15 to know that the personally identifiable in-
16 formation being provided to the Federal
17 department or agency is inaccurate, and
18 provides such inaccurate information; and

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

23 (i) exercise appropriate due diligence
24 in selecting those service providers for re-

1 sponsibilities related to personally identifi-
2 able information;

3 (ii) take reasonable steps to select and
4 retain service providers that are capable of
5 maintaining appropriate safeguards for the
6 security, privacy, and integrity of the per-
7 sonally identifiable information at issue;
8 and

9 (iii) require such service providers, by
10 contract, to implement and maintain ap-
11 propriate measures designed to meet the
12 objectives and requirements in title III.

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

17 (d) STUDY OF GOVERNMENT USE.—

18 (1) SCOPE OF STUDY.—Not later than 180
19 days after the date of enactment of this Act, the
20 Comptroller General of the United States shall con-
21 duct a study and audit and prepare a report on Fed-
22 eral agency use of data brokers or commercial data-
23 bases containing personally identifiable information,
24 including the impact on privacy and security, and
25 the extent to which Federal contracts include suffi-

1 cient provisions to ensure privacy and security pro-
2 tections, and penalties for failures in privacy and se-
3 curity practices.

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

6 **SEC. 404. IMPLEMENTATION OF CHIEF PRIVACY OFFICER**
7 **REQUIREMENTS.**

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

19 (b) DUTIES AND RESPONSIBILITIES OF CHIEF PRI-
20 VACY OFFICER.—In addition to the duties and responsibil-
21 ities outlined under section 522 of the Transportation,
22 Treasury, Independent Agencies, and General Government
23 Appropriations Act, 2005 (division H of Public Law 108–
24 447; 118 Stat. 3199), the Department of Justice Chief
25 Privacy Officer shall—

1 (1) oversee the Department of Justice’s imple-
2 mentation of the requirements under section 403 to
3 conduct privacy impact assessments of the use of
4 commercial data containing personally identifiable
5 information by the Department; and

6 (2) coordinate with the Privacy and Civil Lib-
7 erties Oversight Board, established in the Intel-
8 ligence Reform and Terrorism Prevention Act of
9 2004 (Public Law 108–458), in implementing this
10 section.

○