

Calendar No. 168110TH CONGRESS
1ST SESSION**S. 495****[Report No. 110-70]**

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, Mr. SANDERS, Mr. BROWN, and Mr. CARDIN) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

MAY 23, 2007

Reported by Mr. LEAHY, with amendments

[Omit the part struck through and insert the part printed in *italic*]**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 2007”.

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 identi-
 fiable information.

Sec. 103. Review and amendment of Federal sentencing guidelines related to
 fraudulent access to or misuse of digitized or electronic person-
 ally 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 insure 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:

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; ~~and any contractor, subcontractor, affil-~~
20 ~~iate, or licensee thereof engaged in interstate com-~~
21 ~~merce.~~

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

1 (5) DATA BROKER.—The term “data broker”
2 means a business entity which for monetary fees or
3 dues regularly engages in the practice of collecting,
4 transmitting, or providing access to sensitive person-
5 ally identifiable information on more than 5,000 in-
6 dividuals who are not the customers or employees of
7 that business entity or affiliate primarily for the
8 purposes of providing such information to non-
9 affiliated third parties on an interstate basis.

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

15 (7) ENCRYPTION.—*The term “encryption”—*

16 (A) *means the protection of data in elec-*
17 *tronic form, in storage or in transit, using an*
18 *encryption technology that has been adopted by*
19 *an established standards setting body which ren-*
20 *ders such data indecipherable in the absence of*
21 *associated cryptographic keys necessary to enable*
22 *decryption of such data; and*

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

1 (7 8) PERSONAL ELECTRONIC RECORD.—

2 (A) IN GENERAL.—The term “personal
3 electronic record” means data associated with
4 an individual contained in a database,
5 networked or integrated databases, or other
6 data system that ~~holds~~ *is provided to non-affili-*
7 *ated third parties and includes* sensitive person-
8 ally identifiable information ~~of~~ *about* that indi-
9 vidual ~~and is provided to nonaffiliated third~~
10 ~~parties.~~

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

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

15 (ii) any proprietary assessment or
16 evaluation of an individual or any propri-
17 etary assessment or evaluation of informa-
18 tion about an individual.

19 (8 9) PERSONALLY IDENTIFIABLE INFORMA-
20 TION.—The term “personally identifiable informa-
21 tion” means any information, or compilation of in-
22 formation, in electronic or digital form serving as a
23 means of identification, as defined by section
24 1028(d)(7) of title 18, United States Code.

1 (~~9~~ **10**) PUBLIC RECORD SOURCE.—The term
2 “public record source” means the Congress, any
3 agency, any State or local government agency, the
4 government of the District of Columbia and govern-
5 ments of the territories or possessions of the United
6 States, and Federal, State or local courts, courts
7 martial and military commissions, that maintain
8 personally identifiable information in records avail-
9 able to the public.

10 (~~10~~ **11**) SECURITY BREACH.—

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

19 (B) EXCLUSION.—The term “security
20 breach” does not include—

21 (i) a good faith acquisition of sensitive
22 personally identifiable information by a
23 business entity or agency, or an employee
24 or agent of a business entity or agency, if
25 the sensitive personally identifiable infor-

1 mation is not subject to further unauthor-
 2 ized disclosure; or

3 ~~(ii) the release of a public record, or~~
 4 ~~information derived from a single public~~
 5 ~~record, not otherwise subject to confiden-~~
 6 ~~tiality or nondisclosure requirement, or in-~~
 7 ~~formation obtained from a news report or~~
 8 ~~periodical.~~

9 *(ii) the release of a public record not*
 10 *otherwise subject to confidentiality or non-*
 11 *disclosure requirements.*

12 ~~(11~~ **12**) SENSITIVE PERSONALLY IDENTIFIABLE
 13 INFORMATION.—The term “sensitive personally iden-
 14 tifiable information” means any information or com-
 15 pilation of information, in electronic or digital form
 16 that includes—

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

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

23 (ii) Any 2 of the following:

24 (I) Home address or telephone
 25 number.

1 (II) Mother's maiden name, if
2 identified as such.

3 (III) Month, day, and year of
4 birth.

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

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

16 (B) a financial account number or credit
17 or debit card number in combination with any
18 security code, access code or password that is
19 required for an individual to obtain credit, with-
20 draw funds, or engage in a financial trans-
21 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 **SEC. 104. EFFECTS OF IDENTITY THEFT ON BANKRUPTCY**
 6 **PROCEEDINGS.**

7 (a) *DEFINITIONS.*—Section 101 of title 11, United
 8 States Code, is amended—

9 (1) by redesignating paragraph (27B) as para-
 10 graph (27D); and

11 (2) by inserting after paragraph (27A) the fol-
 12 lowing:

13 “(27B) ‘identity theft’ means a fraud committed
 14 or attempted using the personally identifiable infor-
 15 mation of another person;

16 “(27C) ‘identity theft victim’ means a debtor
 17 who, as a result of an identify theft in any consec-
 18 tive 12-month period during the 3-year period before
 19 the date on which a petition is filed under this title,
 20 had claims asserted against such debtor in excess of
 21 the least of—

22 “(A) \$20,000;

23 “(B) 50 percent of all claims asserted
 24 against such debtor; or

1 “(C) 25 percent of the debtor’s gross income
2 for such 12-month period.”.

3 (b) *PROHIBITION.*—Section 707(b) of title 11, United
4 States Code, is amended by adding at the end the following:

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

9 **TITLE II—DATA BROKERS**

10 **SEC. 201. TRANSPARENCY AND ACCURACY OF DATA COL-** 11 **LECTION.**

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

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

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

1 (2) any data broker that is subject to regulation
2 under the Gramm-Leach-Bliley Act (Public Law
3 106–102);

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

9 (4) information in a personal electronic record
10 that—

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

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

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

24 (c) DISCLOSURES TO INDIVIDUALS.—

1 (1) IN GENERAL.—A data broker shall, upon
2 the request of an individual, disclose to such indi-
3 vidual for a reasonable fee all personal electronic
4 records pertaining to that individual maintained spe-
5 cifically for disclosure to third parties that request
6 information on that individual in the ordinary course
7 of business in the databases or systems of the data
8 broker at the time of such request.

9 (2) INFORMATION ON HOW TO CORRECT INAC-
10 CURACIES.—The disclosures required under para-
11 graph (1) shall also include guidance to individuals
12 on procedures for correcting inaccuracies.

13 (d) *DISCLOSURE TO INDIVIDUALS OF ADVERSE AC-*
14 *TIONS TAKEN BY THIRD PARTIES.—*

15 (1) *IN GENERAL.—In addition to any other*
16 *rights established under this Act, if a person takes*
17 *any adverse action with respect to any individual*
18 *that is based, in whole or in part, on any informa-*
19 *tion contained in a personal electronic record that is*
20 *maintained, updated, or otherwise owned or possessed*
21 *by a data broker, such person, at no cost to the af-*
22 *ected individual, shall provide—*

23 (A) *written or electronic notice of the ad-*
24 *verse action to the individual;*

1 (B) to the individual, in writing or elec-
 2 tronically, the name, address, and telephone
 3 number of the data broker that furnished the in-
 4 formation to the person;

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

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

10 (2) *ACCEPTED METHODS OF NOTICE.*—A person
 11 shall be in compliance with the notice requirements
 12 under paragraph (1) if such person provides written
 13 or electronic notice in the same manner and using the
 14 same methods as are required under section 313(1) of
 15 this Act.

16 (4 e) *ACCURACY RESOLUTION PROCESS.*—

17 (1) *INFORMATION FROM A PUBLIC RECORD OR*
 18 *LICENSOR.*—

19 (A) *IN GENERAL.*—If an individual notifies
 20 a data broker of a dispute as to the complete-
 21 ness or accuracy of information disclosed to
 22 such individual under subsection (c) that is ob-
 23 tained from a public record source or a license
 24 agreement, such data broker shall determine
 25 within 30 days whether the information in its

1 system accurately and completely records the
2 information available from the ~~public record~~
3 ~~source or~~ *licensor or public record source*.

4 (B) DATA BROKER ACTIONS.—If a data
5 broker determines under subparagraph (A) that
6 the information in its systems does not accu-
7 rately and completely record the information
8 available from a public record source or licen-
9 sor, the data broker shall—

10 (i) correct any inaccuracies or incom-
11 pleteness, and provide to such individual
12 written notice of such changes; and

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

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

23 (A) review and consider free of charge any
24 information submitted by such individual that is

1 relevant to the completeness or accuracy of the
2 disputed information; and

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

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

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

22 (5) DETERMINATION THAT DISPUTE IS FRIVO-
23 LOUS OR IRRELEVANT.—

24 (A) IN GENERAL.—Notwithstanding para-
25 graphs (1) through (3), a data broker may de-

1 cline to investigate or terminate a review of in-
2 formation disputed by an individual under those
3 paragraphs if the data broker reasonably deter-
4 mines that the dispute by the individual is friv-
5 olous or intended to perpetrate fraud.

6 (B) NOTICE.—A data broker shall notify
7 an individual of a determination under subpara-
8 graph (A) within a reasonable time by any
9 means available to such data broker.

10 **SEC. 202. ENFORCEMENT.**

11 (a) CIVIL PENALTIES.—

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

17 (2) INTENTIONAL OR WILLFUL VIOLATION.—A
18 data broker that intentionally or willfully violates the
19 provisions of section 201 shall be subject to addi-
20 tional penalties in the amount of \$1,000 per viola-
21 tion per day, to a maximum of an additional
22 \$250,000 per violation, while such violations persist.

23 (3) EQUITABLE RELIEF.—A data broker en-
24 gaged in interstate commerce that violates this sec-

1 tion may be enjoined from further violations by a
2 court of competent jurisdiction.

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

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

10 (c) STATE ENFORCEMENT.—

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

23 (A) enjoin that act or practice;

24 (B) enforce compliance with this title; or

1 (C) obtain civil penalties of not more than
2 \$1,000 per violation per day while such viola-
3 tions persist, up to a maximum of \$250,000 per
4 violation.

5 (2) NOTICE.—

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

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

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

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

20 (C) NOTIFICATION WHEN PRACTICABLE.—

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

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

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

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

10 (C) file petitions for appeal.

11 (4) PENDING PROCEEDINGS.—If the Federal
12 Trade Commission has instituted a proceeding or
13 civil action for a violation of this title, no attorney
14 general of a State may, during the pendency of such
15 proceeding or civil action, bring an action under this
16 subsection against any defendant named in such civil
17 action for any violation that is alleged in that civil
18 action.

19 (5) RULE OF CONSTRUCTION.—For purposes of
20 bringing any civil action under paragraph (1), noth-
21 ing in this title shall be construed to prevent an at-
22 torney general of a State from exercising the powers
23 conferred on the attorney general by the laws of that
24 State to—

25 (A) conduct investigations;

1 (B) administer oaths and affirmations; or

2 (C) compel the attendance of witnesses or
3 the production of documentary and other evi-
4 dence.

5 (6) VENUE; SERVICE OF PROCESS.—

6 (A) VENUE.—Any action brought under
7 this subsection may be brought in the district
8 court of the United States that meets applicable
9 requirements relating to venue under section
10 1391 of title 28, United States Code.

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

14 (i) is an inhabitant; or

15 (ii) may be found.

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

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

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

1 **SEC. 204. EFFECTIVE DATE.**

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

4 **TITLE III—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION**

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

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

7 (a) **PURPOSE.**—The purpose of this subtitle is to ensure standards for developing and implementing administrative, technical, and physical safeguards to protect the security of sensitive personally identifiable information.

8 (b) **IN GENERAL.**—A business entity engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form on 10,000 or more United States persons is subject to the requirements for a data privacy and security program under section 302 for protecting sensitive personally identifiable information.

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

10 (1) **FINANCIAL INSTITUTIONS.**—Financial institutions—

1 (A) subject to the data security require-
2 ments and implementing regulations under the
3 Gramm-Leach-Bliley Act (15 U.S.C. 6801 et
4 seq.); and

5 (B) subject to—

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

12 (ii) compliance with part 314 of title
13 16, Code of Federal Regulations.

14 (2) HIPPA REGULATED ENTITIES.—

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

20 (B) BUSINESS ENTITIES.—A business enti-
21 ty shall be deemed in compliance with the pri-
22 vacy and security program requirements under
23 section 302 if the business entity is acting as
24 a “business associate” as that term is defined
25 in the Health Insurance Portability and Ac-

1 countability Act of 1996 (42 U.S.C. 1301 et
2 seq.) and is in compliance with requirements
3 imposed under that Act and its implementing
4 regulations.

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

9 (d) SAFE HARBORS.—

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

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

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; *and*

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 per-*
22 *sonally identifiable information pertaining*
23 *to specific individuals; and*

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

1 *access or acquire sensitive personally identi-*
2 *fiable information without the business enti-*
3 *ty first performing sufficient due diligence*
4 *to ascertain, with reasonable certainty, that*
5 *such information is being sought for a valid*
6 *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 TIME LINE.—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 shall have the provisions of this subtitle
13 enforced against it by the Federal Trade Commission.

14 (c) **STATE ENFORCEMENT.**—

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

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

3 (A) enjoin that act or practice;

4 (B) enforce compliance with this subtitle;

5 or

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

10 (2) NOTICE.—

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

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

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

18 (B) EXCEPTION.—Subparagraph (A) shall
19 not apply with respect to the filing of an action
20 by an attorney general of a State under this
21 subsection, if the attorney general of a State
22 determines that it is not feasible to provide the
23 notice described in this subparagraph before the
24 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 the systems or databases of such agency~~
21 ~~or business entity~~ *of such information*, notify any resident
22 of the United States whose sensitive personally identifiable
23 information has been, or is reasonably believed to have
24 been, accessed, or acquired.

25 (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 Secret*
18 *Service may review a certification provided by*
19 *an agency under paragraph (3), and shall re-*
20 *view a certification provided by a business entity*
21 *under paragraph (3), to determine whether an*
22 *exemption under paragraph (1) is merited. Such*
23 *review shall be completed not later than 10 busi-*
24 *ness days after the date of receipt of the certifi-*
25 *cation, except as provided in paragraph (5)(C).*

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

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

11 (5) *ADDITIONAL AUTHORITY OF THE SECRET*
12 *SERVICE.*—

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

21 (B) *REQUIRED COMPLIANCE.*—Any agency
22 or business entity that receives a request for ad-
23 ditional information under subparagraph (A)
24 shall cooperate with any such request.

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

8 (b) *SAFE HARBOR.*—*An agency or business entity*
9 *will be exempt from the notice requirements under section*
10 *311, if—*

11 ~~(1) a risk assessment concludes that there is no~~
12 ~~significant risk that the security breach has resulted~~
13 ~~in, or will result in, harm to the individuals whose~~
14 ~~sensitive personally identifiable information was sub-~~
15 ~~ject to the security breach;~~

16 ~~(1) a risk assessment concludes that—~~

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

24 ~~(B) there is no significant risk that a secu-~~
25 ~~rity breach has resulted in, or will result in,~~

1 *harm to the individuals whose sensitive person-*
2 *ally identifiable information was subject to the*
3 *security breach, with the rendering of such sen-*
4 *sitive personally identifiable information indeci-*
5 *pherable through the use of best practices or*
6 *methods, such as redaction, access controls, or*
7 *other such mechanisms, which are widely accept-*
8 *ed as an effective industry practice, or an effec-*
9 *tive industry standard, establishing a presump-*
10 *tion that no significant risk exist;*

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

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

17 (B) its decision to invoke the risk assess-
18 ment exemption; and

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

22 (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

23 (1) IN GENERAL.—A business entity will be ex-
24 empt from the notice requirement under section 311

1 if the business entity utilizes or participates in a se-
2 curity program that—

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

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

11 (2) LIMITATION.—The exemption by this sub-
12 section does not apply ~~if the information subject to~~
13 ~~the security breach includes sensitive personally~~
14 ~~identifiable information in addition to the sensitive~~
15 ~~personally identifiable information identified in sec-~~
16 ~~tion 3 if—~~

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

23 (B) *the security breach includes both the in-*
24 *dividual's credit card number and the individ-*
25 *ual's first and last name.*

1 **SEC. 313. METHODS OF NOTICE.**

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

4 (1) INDIVIDUAL NOTICE.—

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

8 (B) Telephone notice to the individual per-
9 sonally; or

10 (C) ~~Electronic notice, if the primary meth-~~
11 ~~od used by the agency or business entity to~~
12 ~~communicate with the individual is by electronic~~
13 ~~means, or E-mail notice, if the individual has~~
14 consented to receive such notice and the notice
15 is consistent with the provisions permitting elec-
16 tronic transmission of notices under section 101
17 of the Electronic Signatures in Global and Na-
18 tional Commerce Act (15 U.S.C. 7001).

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

1 **SEC. 314. CONTENT OF NOTIFICATION.**

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

5 (1) a description of the categories of sensitive
6 personally identifiable information that was, or is
7 reasonably believed to have been, acquired by an un-
8 authorized person;

9 (2) a toll-free number ~~or, if the primary method~~
10 ~~used by the agency or business entity to commu-~~
11 ~~nicate with the individual is by electronic means, an~~
12 ~~electronic mail address—~~

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

16 (B) from which the individual may learn
17 what types of sensitive personally identifiable
18 information the agency or business entity main-
19 tained about that individual; and

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

22 (b) ADDITIONAL CONTENT.—Notwithstanding sec-
23 tion 319, a State may require that a notice under sub-
24 section (a) shall also include information regarding victim
25 protection assistance provided for by that State.

1 **SEC. 315. COORDINATION OF NOTIFICATION WITH CREDIT**
 2 **REPORTING AGENCIES.**

3 If an agency or business entity is required to provide
 4 notification to more than ~~1,000 individuals~~ *5,000 individ-*
 5 *uals* under section 311(a), the agency or business entity
 6 shall also notify, ~~without unreasonable delay,~~ all consumer
 7 reporting agencies that compile and maintain files on con-
 8 sumers on a nationwide basis (as defined in section 603(p)
 9 of the Fair Credit Reporting Act (15 U.S.C. 1681a(p))
 10 of the timing and distribution of the notices. *Such notice*
 11 *shall be given to the consumer credit reporting agencies*
 12 *without unreasonable delay and, if it will not delay notice*
 13 *to the affected individuals, prior to the distribution of no-*
 14 *tices to the affected individuals.*

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

16 (a) SECRET SERVICE.—Any business entity or agen-
 17 cy shall ~~give notice of a security breach to the United~~
 18 ~~States Secret Service~~ *notify the United States Secret Serv-*
 19 *ice of the fact that a security breach has occurred if—*

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

24 (2) the security breach involves a database,
 25 networked or integrated databases, or other data
 26 system containing the sensitive personally identifi-

1 able information of more than 1,000,000 individuals
2 nationwide;

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

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

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

14 (1) the Federal Bureau of Investigation, if the
15 security breach involves espionage, foreign counter-
16 intelligence, information protected against unauthor-
17 ized disclosure for reasons of national defense or for-
18 eign relations, or Restricted Data (as that term is
19 defined in section 11y of the Atomic Energy Act of
20 1954 (42 U.S.C. 2014(y)), except for offenses af-
21 fecting the duties of the United States Secret Serv-
22 ice under section 3056(a) of title 18, United States
23 Code;

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

1 (3) the attorney general of each State affected
2 by the security breach.

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

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

10 (1) *Notice under subsection (a) shall be delivered*
11 *as promptly as possible, but not later than 14 days*
12 *after discovery of the events requiring notice.*

13 (2) *Notice under subsection (b) shall be delivered*
14 *not later than 14 days after the Service receives notice*
15 *of a security breach from an agency or business enti-*
16 *ty.*

17 **SEC. 317. ENFORCEMENT.**

18 (a) **CIVIL ACTIONS BY THE ATTORNEY GENERAL.—**
19 The Attorney General may bring a civil action in the ap-
20 propriate United States district court against any business
21 entity that engages in conduct constituting a violation of
22 this subtitle and, upon proof of such conduct by a prepon-
23 derance of the evidence, such business entity shall be sub-
24 ject to a civil penalty of not more than \$1,000 per day
25 per individual whose sensitive personally identifiable infor-

1 mation was, or is reasonably believed to have been,
2 accessed or acquired by an unauthorized person, up to a
3 maximum of \$1,000,000 per violation, unless such conduct
4 is found to be willful or intentional.

5 (b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-
6 ERAL.—

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

12 (A) enjoining such act or practice; or

13 (B) enforcing compliance with this subtitle.

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

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

22 (d) FRAUD ALERT.—Section 605A(b)(1) of the Fair
23 Credit Reporting Act (15 U.S.C. 1681e–1(b)(1)) is
24 amended by inserting “, or evidence that the consumer
25 has received notice that the consumer’s financial informa-

1 tion has or may have been compromised,” after “identity
2 theft report”.

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

4 (a) IN GENERAL.—

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 engage-
12 ment of a business entity in a practice that is pro-
13 hibited under this subtitle, the State or the State or
14 local law enforcement agency on behalf of the resi-
15 dents of the agency’s jurisdiction, may bring a civil
16 action on behalf of the residents of the State or ju-
17 risdiction in a district court of the United States of
18 appropriate jurisdiction or any other court of com-
19 petent jurisdiction, including a State court, to—

20 (A) enjoin that practice;

21 (B) enforce compliance with this subtitle;

22 or

23 (C) civil penalties of not more than \$1,000
24 per day per individual whose sensitive person-
25 ally identifiable information was, or is reason-

1 ably believed to have been, accessed or acquired
2 by an unauthorized person, up to a maximum
3 of \$1,000,000 per violation, unless such con-
4 duct is found to be willful or intentional.

5 (2) NOTICE.—

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

10 (i) written notice of the action; and

11 (ii) a copy of the complaint for the ac-
12 tion.

13 (B) EXEMPTION.—

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

21 (ii) NOTIFICATION.—In an action de-
22 scribed in clause (i), the attorney general
23 of a State shall provide notice and a copy
24 of the complaint to the Attorney General

1 at the time the State attorney general files
2 the action.

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

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

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

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

15 (4) file petitions for appeal.

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

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

1 regarding notification shall be construed to prevent an at-
2 torney general of a State from exercising the powers con-
3 ferred on such attorney general by the laws of that State
4 to—

5 (1) conduct investigations;

6 (2) administer oaths or affirmations; or

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

9 (e) VENUE; SERVICE OF PROCESS.—

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

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

16 (B) another court of competent jurisdic-
17 tion.

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

21 (A) is an inhabitant; or

22 (B) may be found.

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

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

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

4 The provisions of this subtitle shall supersede any
5 other provision of Federal law or any provision of law of
6 any State relating to notification *by a business entity en-*
7 *gaged in interstate commerce or an agency* of a security
8 breach, except as provided in section 314(b).

9 **SEC. 320. AUTHORIZATION OF APPROPRIATIONS.**

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

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

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

20 (1) the number and nature of the security
21 breaches described in the notices filed by those busi-
22 ness entities invoking the risk assessment exemption
23 under section 312(b) and the response of the United
24 States Secret Service to such notices; and

1 (2) the number and nature of security breaches
2 subject to the national security and law enforcement
3 exemptions under section 312(a), provided that such
4 report may not disclose the contents of any risk as-
5 sessment provided to the United States Secret Serv-
6 ice pursuant to this subtitle.

7 **SEC. 322. EFFECTIVE DATE.**

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

11 ***Subtitle C—Office of Federal***
12 ***Identity Protection***

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

14 (a) *ESTABLISHMENT.*—*There is established in the Fed-*
15 *eral Trade Commission an Office of Federal Identity Pro-*
16 *tection.*

17 (b) *DUTIES.*—*The Office of Federal Identity Protection*
18 *shall be responsible for assisting each consumer with—*

19 (1) *addressing the consequences of the theft or*
20 *compromise of the personally identifiable information*
21 *of that consumer;*

22 (2) *accessing remedies provided under Federal*
23 *law and providing information about remedies avail-*
24 *able under State law;*

25 (3) *restoring the accuracy of—*

1 (A) the personally identifiable information
2 of that consumer; and

3 (B) records containing the personally iden-
4 tifiable information of that consumer that were
5 stolen or compromised; and

6 (4) retrieving any stolen or compromised person-
7 ally identifiable information of that consumer.

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

11 (1) Establish a website, easily and conspicuously
12 accessible from *ftc.gov*, dedicated to assisting con-
13 sumers with the retrieval of the stolen or compromised
14 personally identifiable information of the consumer.

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

18 (3) Establish online and offline consumer-service
19 teams to assist consumers seeking the retrieval of the
20 personally identifiable information of the consumer.

21 (4) Provide guidance and information to service
22 organizations or pro bono legal services programs that
23 offer individualized assistance or counseling to vic-
24 tims of identity theft.

1 (5) *Establish a reasonable standard for deter-*
2 *mining when an individual becomes a victim of iden-*
3 *tity theft.*

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

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

9 (A) *in all Federal, State, and local jurisdic-*
10 *tions, in lieu of a police report or any other doc-*
11 *ument required by State or local law, as a pre-*
12 *requisite to accessing business records of trans-*
13 *actions done by someone claiming to be the indi-*
14 *vidual; and*

15 (B) *to establish the eligibility of that indi-*
16 *vidual for—*

17 (i) *the fraud alert protections under*
18 *section 605A of the Fair Credit Reporting*
19 *Act (15 U.S.C. 1681c–1); and*

20 (ii) *the reporting protections under sec-*
21 *tion 605B(a) of the Fair Credit Reporting*
22 *Act (15 U.S.C. 1681c–2(a)).*

23 (8) *Coordinate, as the Office determines nec-*
24 *essary, with the designated Chief Privacy Officer of*
25 *each Federal agency, or any other designated senior*

1 *official in such agency in charge of privacy, in order*
 2 *to meet the duties of assisting consumers as required*
 3 *under subsection (b).*

4 *(9) In addition to the requirements in para-*
 5 *graphs (1) through (7), the Federal Trade Commis-*
 6 *sion shall promulgate regulations that enable the Of-*
 7 *fice of Federal Identity Protection to help consumers*
 8 *restore their stolen or otherwise compromised person-*
 9 *ally identifiable information quickly and inexpen-*
 10 *sively.*

11 *(d) AUTHORIZATION OF APPROPRIATIONS.—There are*
 12 *authorized to be appropriated for the Office of Federal Iden-*
 13 *tity Protection such sums as are necessary for fiscal year*
 14 *2008 and each of the 4 succeeding fiscal years.*

15 **TITLE IV—GOVERNMENT AC-**
 16 **CESS TO AND USE OF COM-**
 17 **MERCIAL DATA**

18 **SEC. 401. GENERAL SERVICES ADMINISTRATION REVIEW**
 19 **OF CONTRACTS.**

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

1 (1) the data privacy and security program of a
2 data broker to ensure the privacy and security of
3 data containing personally identifiable information,
4 including whether such program adequately address-
5 es privacy and security threats created by malicious
6 software or code, or the use of peer-to-peer file shar-
7 ing software;

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

10 (3) the extent to which the databases and sys-
11 tems containing personally identifiable information
12 of a data broker have been compromised by security
13 breaches; and

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

17 (b) COMPLIANCE SAFE HARBOR.—The data privacy
18 and security program of a data broker shall be deemed
19 sufficient for the purposes of subsection (a), if the data
20 broker complies with or provides protection equal to indus-
21 try standards, as identified by the Federal Trade Commis-
22 sion, that are applicable to the type of personally identifi-
23 able information involved in the ordinary course of busi-
24 ness of such data broker.

1 (c) PENALTIES.—In awarding contracts with data
2 brokers for products or services related to access, use,
3 compilation, distribution, processing, analyzing, or evalu-
4 ating personally identifiable information, the Adminis-
5 trator of the General Services Administration shall—

6 (1) include monetary or other penalties—

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

9 (B) if a contractor knows or has reason to
10 know that the personally identifiable informa-
11 tion being provided is inaccurate, and provides
12 such inaccurate information; and

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

17 (A) exercise appropriate due diligence in
18 selecting those service providers for responsibil-
19 ities related to personally identifiable informa-
20 tion;

21 (B) take reasonable steps to select and re-
22 tain service providers that are capable of main-
23 taining appropriate safeguards for the security,
24 privacy, and integrity of the personally identifi-
25 able information at issue; and

1 (C) require such service providers, by con-
2 tract, to implement and maintain appropriate
3 measures designed to meet the objectives and
4 requirements in title III.

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

9 **SEC. 402. REQUIREMENT TO AUDIT INFORMATION SECU-**
10 **RITY PRACTICES OF CONTRACTORS AND**
11 **THIRD PARTY BUSINESS ENTITIES.**

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

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

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

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

19 “(9) procedures for evaluating and auditing the
20 information security practices of contractors or third
21 party business entities supporting the information
22 systems or operations of the agency involving per-
23 sonally identifiable information (as that term is de-
24 fined in section 3 of the Personal Data Privacy and

1 Security Act of 2007) and ensuring remedial action
2 to address any significant deficiencies.”.

3 **SEC. 403. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT**
4 **USE OF COMMERCIAL INFORMATION SERV-**
5 **ICES CONTAINING PERSONALLY IDENTIFI-**
6 **ABLE INFORMATION.**

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

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

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

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

14 “(iii) purchasing or subscribing for a
15 fee to personally identifiable information
16 from a data broker (as such terms are de-
17 fined in section 3 of the Personal Data
18 Privacy and Security Act of 2007).”.

19 (b) LIMITATION.—Notwithstanding any other provi-
20 sion of law, commencing 1 year after the date of enact-
21 ment of this Act, no Federal agency may enter into a con-
22 tract with a data broker to access for a fee any database
23 consisting primarily of personally identifiable information
24 concerning United States persons (other than news report-

1 ing or telephone directories) unless the head of such de-
2 partment or agency—

3 (1) completes a privacy impact assessment
4 under section 208 of the E-Government Act of 2002
5 (44 U.S.C. 3501 note), which shall subject to the
6 provision in that Act pertaining to sensitive informa-
7 tion, include a description of—

8 (A) such database;

9 (B) the name of the data broker from
10 whom it is obtained; and

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

12 (2) adopts regulations that specify—

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

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

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

22 (D) standards limiting the retention and
23 redisclosure of personally identifiable informa-
24 tion obtained from such databases;

1 (E) procedures ensuring that such data
2 meet standards of accuracy, relevance, com-
3 pleteness, and timeliness;

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

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

11 (H) mechanisms, if any, for the enforce-
12 ment and independent oversight of existing or
13 planned procedures, policies, or guidelines; and

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

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

21 (A) providing for penalties—

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

24 (ii) if the entity knows or has reason
25 to know that the personally identifiable in-

1 formation being provided to the Federal
2 department or agency is inaccurate, and
3 provides such inaccurate information; and

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

8 (i) exercise appropriate due diligence
9 in selecting those service providers for re-
10 sponsibilities related to personally identifi-
11 able information;

12 (ii) take reasonable steps to select and
13 retain service providers that are capable of
14 maintaining appropriate safeguards for the
15 security, privacy, and integrity of the per-
16 sonally identifiable information at issue;
17 and

18 (iii) require such service providers, by
19 contract, to implement and maintain ap-
20 propriate measures designed to meet the
21 objectives and requirements in title III.

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

1 (d) STUDY OF GOVERNMENT USE.—

2 (1) SCOPE OF STUDY.—Not later than 180
3 days after the date of enactment of this Act, the
4 Comptroller General of the United States shall con-
5 duct a study and audit and prepare a report on Fed-
6 eral agency use of data brokers or commercial data-
7 bases containing personally identifiable information,
8 including the impact on privacy and security, and
9 the extent to which Federal contracts include suffi-
10 cient provisions to ensure privacy and security pro-
11 tections, and penalties for failures in privacy and se-
12 curity practices.

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

15 (d) STUDY OF GOVERNMENT USE.—

16 (1) SCOPE OF STUDY.—*Not later than 180 days*
17 *after the date of enactment of this Act, the Comp-*
18 *troller General of the United States shall conduct a*
19 *study and audit and prepare a report on Federal*
20 *agency actions to address the recommendations in the*
21 *Government Accountability Office’s April 2006 report*
22 *on agency adherence to key privacy principles in*
23 *using data brokers or commercial databases con-*
24 *taining personally identifiable information.*

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

3 **SEC. 404. IMPLEMENTATION OF CHIEF PRIVACY OFFICER**
4 **REQUIREMENTS.**

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

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

23 (1) oversee the Department of Justice’s imple-
24 mentation of the requirements under section 403 to
25 conduct privacy impact assessments of the use of

1 commercial data containing personally identifiable
2 information by the Department; and

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

Calendar No. 168

110TH CONGRESS
1ST Session

S. 495

[Report No. 110-70]

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.

MAY 23, 2007

Reported with amendments