

AMENDMENT NO. _____ Calendar No. _____

Purpose: To provide a complete substitute.

IN THE SENATE OF THE UNITED STATES—109th Cong., 1st Sess.

S. 1789

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.

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended to be proposed by _____

Viz:

1 Strike all after the enacting clause and insert the fol-

2 lowing:

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 2005”.

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

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. 321. Notice to individuals.

Sec. 322. Exemptions.

Sec. 323. Methods of notice.

Sec. 324. Content of notification.

Sec. 325. Coordination of notification with credit reporting agencies.

Sec. 326. Notice to law enforcement.

Sec. 327. Enforcement.

Sec. 328. Enforcement by State attorneys general.

Sec. 329. Effect on Federal and State law.

Sec. 330. Authorization of appropriations.

Sec. 331. Reporting on risk assessment exemptions.

Sec. 332. 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 not
9 otherwise subject to confidentiality or non-
10 disclosure requirements.

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

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

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

22 (ii) Any 2 of the following:

23 (I) Home address or telephone
24 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 money,
20 goods, services or any other thing of value.

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 Data Privacy and Security Act of 2005,”
14 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 **“SEC. 1039. CONCEALMENT OF SECURITY BREACHES IN-**
22 **VOLVING SENSITIVE PERSONALLY IDENTIFI-**
23 **ABLE INFORMATION.**

24 “(a) Whoever, having knowledge of a security breach
25 and of the obligation either individually or collectively to

1 provide notice of such breach to individuals under title IV
2 of the Personal Data Privacy and Security Act of 2005,
3 and having not otherwise qualified for an exemption from
4 providing notice under section 422 of such Act, inten-
5 tionally and willfully conceals the fact of such security
6 breach and which breach causes economic damage to 1
7 or more persons, shall be fined under this title or impris-
8 oned not more than 5 years, or both.

9 “(b) For purposes of subsection (a), the term ‘person’
10 has the same meaning as in section 1030(e)(12) of title
11 18, United States Code.”.

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

“1039. Concealment of security breaches involving personally identifiable
information.”.

16 (c) ENFORCEMENT AUTHORITY.—

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

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

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

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

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

17 (2) any other relevant provision.

18 (b) REQUIREMENTS.—In carrying out the require-
19 ments of this section, the United States Sentencing Com-
20 mission shall—

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

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

25 (B) the growing incidences of theft and
26 misuse of digitized or electronic personally iden-

1 tifiable information, including identity theft;
2 and

3 (C) the need to deter, prevent, and punish
4 such offenses;

5 (2) consider the extent to which the Federal
6 sentencing guidelines (including its policy state-
7 ments) adequately address violations of the sections
8 amended by this Act to—

9 (A) sufficiently deter and punish such of-
10 fenses; and

11 (B) adequately reflect the enhanced pen-
12 alties established under this Act;

13 (3) maintain reasonable consistency with other
14 relevant directives and sentencing guidelines;

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

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

21 (A) the online sale of fraudulently obtained
22 or stolen personally identifiable information;

23 (B) the sale of fraudulently obtained or
24 stolen personally identifiable information to an
25 individual who is engaged in terrorist activity or

1 aiding other individuals engaged in terrorist ac-
2 tivity; or

3 (C) the sale of fraudulently obtained or
4 stolen personally identifiable information to fi-
5 nance terrorist activity or other criminal activi-
6 ties;

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

14 (7) ensure that the Federal sentencing guide-
15 lines adequately meet the purposes of sentencing
16 under section 3553(a)(2) of title 18, United States
17 Code.

18 (c) EMERGENCY AUTHORITY TO SENTENCING COM-
19 MISSION.—The United States Sentencing Commission
20 may, as soon as practicable, promulgate amendments
21 under this section in accordance with procedures estab-
22 lished in section 21(a) of the Sentencing Act of 1987 (28
23 U.S.C. 994 note) as though the authority under that Act
24 had not expired.

1 **TITLE II—DATA BROKERS**

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

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

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

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

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

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

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

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

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

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

16 (c) DISCLOSURES TO INDIVIDUALS.—

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

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

5 (d) ACCURACY RESOLUTION PROCESS.—

6 (1) INFORMATION FROM A PUBLIC RECORD OR
7 LICENSOR.—

8 (A) IN GENERAL.—If an individual notifies
9 a data broker of a dispute as to the complete-
10 ness or accuracy of information disclosed to
11 such individual under subsection (c) that is de-
12 rived from a public record source or pursuant
13 to a license agreement, such data broker shall
14 determine within 30 days whether the informa-
15 tion in its system accurately and completely
16 records the information available from the pub-
17 lic record source or licensor.

18 (B) DATA BROKER ACTIONS.—If a data
19 broker determines under subparagraph (A) that
20 the information in its systems does not accu-
21 rately and completely record the information
22 available from a public record source or licen-
23 sor, the data broker shall —

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

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

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

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

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

22 (3) EXTENSION OF REVIEW PERIOD.—The 30-
23 day period described in paragraph (1) may be ex-
24 tended for not more than 30 additional days if a
25 data broker receives information from the individual

1 during the initial 30-day period that is relevant to
2 the completeness or accuracy of any disputed infor-
3 mation.

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

12 (5) DETERMINATION THAT DISPUTE IS FRIVO-
13 LOUS OR IRRELEVANT.—

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

21 (B) NOTICE.—A data broker shall notify
22 an individual of a determination under subpara-
23 graph (A) within a reasonable time by any
24 means available to such data broker.

1 **SEC. 202. ENFORCEMENT.**

2 (a) CIVIL PENALTIES.—

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

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

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

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

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

25 (c) STATE ENFORCEMENT.—

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

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

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

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

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

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

25 (C) file petitions for appeal.

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

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

15 (A) conduct investigations;

16 (B) administer oaths and affirmations; or

17 (C) compel the attendance of witnesses or
18 the production of documentary and other evi-
19 dence.

20 (6) VENUE; SERVICE OF PROCESS.—

21 (A) VENUE.—Any action brought under
22 this subsection may be brought in the district
23 court of the United States that meets applicable
24 requirements relating to venue under section
25 1931 of title 28, United States Code.

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

4 (i) is an inhabitant; or

5 (ii) may be found.

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

9 (e) IMPLEMENTATION TIME LINE.—Not later than
10 1 year after the date of enactment of this Act, a business
11 entity subject to the provisions of this title shall implement
12 a data privacy and security program pursuant to this title.

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

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

19 **SEC. 204. EFFECTIVE DATE.**

20 This title shall take effect 180 days after the date
21 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 (d) SAFE HARBORS.—

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

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

20 **SEC. 302. REQUIREMENTS FOR A PERSONAL DATA PRIVACY**
21 **AND SECURITY PROGRAM.**

22 (a) PERSONAL DATA PRIVACY AND SECURITY PRO-
23 GRAM.—A business entity subject to this subtitle shall
24 comply with the following safeguards and any other ad-
25 ministrative, technical, or physical safeguards identified by

1 the Federal Trade Commission in a rulemaking process
2 pursuant to section 553 of title 5, United States Code,
3 for the protection of sensitive personally identifiable infor-
4 mation:

5 (1) SCOPE.—A business entity shall implement
6 a comprehensive personal data privacy and security
7 program that includes administrative, technical, and
8 physical safeguards appropriate to the size and com-
9 plexity of the business entity and the nature and
10 scope of its activities.

11 (2) DESIGN.—The personal data privacy and
12 security program shall be designed to—

13 (A) ensure the privacy, security, and con-
14 fidentiality of personal electronic records;

15 (B) protect against any anticipated
16 vulnerabilities to the privacy, security, or integ-
17 rity of sensitive personally identifying informa-
18 tion; and

19 (C) protect against unauthorized access to
20 use of sensitive personally identifying informa-
21 tion that could result in substantial harm or in-
22 convenience to any individual.

23 (3) RISK ASSESSMENT.—A business entity
24 shall—

1 (A) identify reasonably foreseeable internal
2 and external vulnerabilities that could result in
3 unauthorized access, disclosure, use, or alter-
4 ation of sensitive personally identifiable infor-
5 mation or systems containing sensitive person-
6 ally identifiable information;

7 (B) assess the likelihood of and potential
8 damage from unauthorized access, disclosure,
9 use, or alteration of sensitive personally identifi-
10 able information;

11 (C) assess the sufficiency of its policies,
12 technologies, and safeguards in place to control
13 and minimize risks from unauthorized access,
14 disclosure, use, or alteration of sensitive person-
15 ally identifiable information; and

16 (D) assess the vulnerability of sensitive
17 personally identifiable information during de-
18 struction and disposal of such information, in-
19 cluding through the disposal or retirement of
20 hardware.

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

23 (A) design its personal data privacy and
24 security program to control the risks identified
25 under paragraph (3); and

1 (B) adopt measures commensurate with
2 the sensitivity of the data as well as the size,
3 complexity, and scope of the activities of the
4 business entity that—

5 (i) control access to systems and fa-
6 cilities containing sensitive personally iden-
7 tifiable information, including controls to
8 authenticate and permit access only to au-
9 thorized individuals;

10 (ii) detect actual and attempted
11 fraudulent, unlawful, or unauthorized ac-
12 cess, disclosure, use, or alteration of sen-
13 sitive personally identifiable information,
14 including by employees and other individ-
15 uals otherwise authorized to have access;

16 (iii) protect sensitive personally identi-
17 fiable information during use, trans-
18 mission, storage, and disposal by
19 encryption or other reasonable means (in-
20 cluding as directed for disposal of records
21 under section 628 of the Fair Credit Re-
22 porting Act (15 U.S.C. 1681w) and the
23 implementing regulations of such Act as
24 set forth in section 682 of title 16, Code
25 of Federal Regulations); and

1 (iv) ensure that sensitive personally
2 identifiable information is properly de-
3 stroyed and disposed of, including during
4 the destruction of computers, diskettes,
5 and other electronic media that contain
6 sensitive personally identifiable informa-
7 tion.

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

12 (c) VULNERABILITY TESTING.—

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

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

23 (d) RELATIONSHIP TO SERVICE PROVIDERS.—In the
24 event a business entity subject to this subtitle engages

1 service providers not subject to this subtitle, such business
2 entity shall—

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

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

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

22 (1) technology;

23 (2) the sensitivity of personally identifiable in-
24 formation;

1 (3) internal or external threats to personally
2 identifiable information; and

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

5 (A) mergers and acquisitions;

6 (B) alliances and joint ventures;

7 (C) outsourcing arrangements;

8 (D) bankruptcy; and

9 (E) changes to sensitive personally identi-
10 fiable information systems.

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

16 **SEC. 303. ENFORCEMENT.**

17 (a) CIVIL PENALTIES.—

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

23 (2) INTENTIONAL OR WILLFUL VIOLATION.—A
24 business entity that intentionally or willfully violates
25 the provisions of sections 301 or 302 shall be subject

1 to additional penalties in the amount of \$5,000 per
2 violation per day while such a violation exists, with
3 a maximum of an additional \$500,000 per violation.

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

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

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

15 (c) **STATE ENFORCEMENT.**—

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

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

9 (2) NOTICE.—

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

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

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

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

24 (C) NOTIFICATION WHEN PRACTICABLE.—

25 In an action described under subparagraph (B),

1 the Attorney General of a State shall provide
2 the written notice and the copy of the complaint
3 to the Federal Trade Commission as soon after
4 the filing of the complaint as practicable.

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

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

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

14 (C) file petitions for appeal.

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

24 (5) RULE OF CONSTRUCTION.—For purposes of
25 bringing any civil action under paragraph (1) noth-

1 ing in this title shall be construed to prevent an at-
2 torney general of a State from exercising the powers
3 conferred on the attorney general by the laws of that
4 State to—

5 (A) conduct investigations;

6 (B) administer oaths and affirmations; or

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

10 (6) VENUE; SERVICE OF PROCESS.—

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

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

19 (i) is an inhabitant; or

20 (ii) may be found.

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

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

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

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

11 **Subtitle B—Security Breach**
12 **Notification**

13 **SEC. 321. NOTICE TO INDIVIDUALS.**

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

22 (b) OBLIGATION OF OWNER OR LICENSEE.—

23 (1) NOTICE TO OWNER OR LICENSEE.—Any
24 agency, or business entity engaged in interstate com-
25 merce, that uses, accesses, transmits, stores, dis-
26 poses of, or collects sensitive personally identifiable

1 information that the agency or business entity does
2 not own or license shall notify the owner or licensee
3 of the information following the discovery of a secu-
4 rity breach involving such information.

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

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

21 (c) TIMELINESS OF NOTIFICATION.—

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

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

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

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

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

22 (2) EXTENDED DELAY OF NOTIFICATION.—If
23 the notification required under subsection (a) is de-
24 layed pursuant to paragraph (1), an agency or busi-
25 ness entity shall give notice 30 days after the day

1 such law enforcement delay was invoked unless a
2 Federal law enforcement agency provides written no-
3 tification that further delay is necessary.

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

9 **SEC. 322. EXEMPTIONS.**

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

12 (1) IN GENERAL.—Section 321 shall not apply
13 to an agency if the agency certifies, in writing, that
14 notification of the security breach as required by
15 section 321 reasonably could be expected to—

16 (A) cause damage to the national security;

17 or

18 (B) hinder a law enforcement investigation
19 or the ability of the agency to conduct law en-
20 forcement investigations.

21 (2) LIMITS ON CERTIFICATIONS.—An agency
22 may not execute a certification under paragraph (1)
23 to—

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

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

3 (C) restrain competition.

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

9 (b) SAFE HARBOR.—An agency or business entity
10 will be exempt from the notice requirements under section
11 321, if—

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

17 (2) without unreasonable delay, but not later
18 than 45 days after the discovery of a security
19 breach, unless extended by the United States Secret
20 Service, the agency or business entity notifies the
21 United States Secret Service, in writing, of—

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

23 (B) its decision to invoke the risk assess-
24 ment exemption; and

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

4 (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

5 (1) IN GENERAL.—A business entity will be ex-
6 empt from the notice requirement under section 321
7 if the business entity utilizes or participates in a se-
8 curity program that—

9 (A) is designed to block the use of the sen-
10 sitive personally identifiable information to ini-
11 tiate unauthorized financial transactions before
12 they are charged to the account of the indi-
13 vidual; and

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

17 (2) LIMITATION.—The exemption by this sub-
18 section does not apply if the information subject to
19 the security breach includes sensitive personally
20 identifiable information in addition to the sensitive
21 personally identifiable information identified in sec-
22 tion 3.

23 **SEC. 323. METHODS OF NOTICE.**

24 An agency, or business entity shall be in compliance
25 with section 321 if it provides both:

1 (1) INDIVIDUAL NOTICE.—

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

5 (B) Telephone notice to the individual per-
6 sonally; or

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

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

19 **SEC. 324. CONTENT OF NOTIFICATION.**

20 (a) IN GENERAL.—Regardless of the method by
21 which notice is provided to individuals under section 323,
22 such notice shall include, to the extent possible—

23 (1) a description of the categories of sensitive
24 personally identifiable information that was, or is

1 reasonably believed to have been, acquired by an un-
2 authorized person;

3 (2) a toll-free number—

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

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

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

13 (b) **ADDITIONAL CONTENT.**—Notwithstanding sec-
14 tion 329, a State may require that a notice under sub-
15 section (a) shall also include information regarding victim
16 protection assistance provided for by that State.

17 **SEC. 325. COORDINATION OF NOTIFICATION WITH CREDIT**
18 **REPORTING AGENCIES.**

19 If an agency or business entity is required to provide
20 notification to more than 1,000 individuals under section
21 321(a), the agency or business entity shall also notify,
22 without unreasonable delay, all consumer reporting agen-
23 cies that compile and maintain files on consumers on a
24 nationwide basis (as defined in section 603(p) of the Fair

1 Credit Reporting Act (15 U.S.C. 1681a(p)) of the timing
2 and distribution of the notices.

3 **SEC. 326. NOTICE TO LAW ENFORCEMENT.**

4 (a) SECRET SERVICE.—Any business entity or agen-
5 cy shall give notice of a security breach to the United
6 States Secret Service if—

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

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

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

18 (4) the security breach involves primarily sen-
19 sitive personally identifiable information of employ-
20 ees and contractors of the Federal Government in-
21 volved in national security or law enforcement.

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

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

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

13 (3) the attorney general of each State affected
14 by the security breach.

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

20 **SEC. 327. ENFORCEMENT.**

21 (a) CIVIL ACTIONS BY THE ATTORNEY GENERAL.—
22 The Attorney General may bring a civil action in the ap-
23 propriate United States district court against any business
24 entity that engages in conduct constituting a violation of
25 this subtitle and, upon proof of such conduct by a prepon-

1 derance of the evidence, such business entity shall be sub-
2 ject to a civil penalty of not more than \$1,000 per day
3 per individual whose sensitive personally identifiable infor-
4 mation was, or is reasonably believed to have been,
5 accessed or acquired by an unauthorized person, up to a
6 maximum of \$50,000 per person.

7 (b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-
8 ERAL.—

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

14 (A) enjoining such act or practice; or

15 (B) enforcing compliance with this subtitle.

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

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

24 (d) FRAUD ALERT.—Section 605A(b)(1) of the Fair
25 Credit Reporting Act (15 U.S.C. 1681c–1(b)(1)) is

1 amended by inserting “, or evidence that the consumer
2 has received notice that the consumer’s financial informa-
3 tion has or may have been compromised,” after “identity
4 theft report”.

5 **SEC. 328. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

6 (a) IN GENERAL.—

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

22 (A) enjoin that practice;

23 (B) enforce compliance with this subtitle;

24 or

1 (C) civil penalties of not more than \$1,000
2 per day per individual whose sensitive person-
3 ally identifiable information was, or is reason-
4 ably believed to have been, accessed or acquired
5 by an unauthorized person, up to a maximum
6 of \$50,000 per day.

7 (2) NOTICE.—

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

12 (i) written notice of the action; and

13 (ii) a copy of the complaint for the ac-
14 tion.

15 (B) EXEMPTION.—

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

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

1 of the complaint to the Attorney General
2 at the time the State attorney general files
3 the action.

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

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

10 (2) initiate an action in the appropriate United
11 States district court under section 327 and move to
12 consolidate all pending actions, including State ac-
13 tions, in such court;

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

16 (4) file petitions for appeal.

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

1 (d) CONSTRUCTION.—For purposes of bringing any
2 civil action under subsection (a), nothing in this subtitle
3 regarding notification shall be construed to prevent an at-
4 torney general of a State from exercising the powers con-
5 ferred on such attorney general by the laws of that State
6 to—

- 7 (1) conduct investigations;
- 8 (2) administer oaths or affirmations; or
- 9 (3) compel the attendance of witnesses or the
10 production of documentary and other evidence.

11 (e) VENUE; SERVICE OF PROCESS.—

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

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

18 (B) another court of competent jurisdic-
19 tion.

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

23 (A) is an inhabitant; or

24 (B) may be found.

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

5 **SEC. 329. EFFECT ON FEDERAL AND STATE LAW.**

6 (a) IN GENERAL.—The provisions of this subtitle
7 shall supersede any other provision of Federal law or any
8 provision of law of any State relating to notification of
9 a security breach, except as provided in section 324(b).

10 (b) GRAMM-LEACH-BLILEY.—This subtitle shall not
11 preclude any operation permitted under section 507 of the
12 Gramm-Leach-Bliley Act (15 U.S.C. 6807).

13 **SEC. 330. AUTHORIZATION OF APPROPRIATIONS.**

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

19 **SEC. 331. REPORTING ON RISK ASSESSMENT EXEMPTIONS.**

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

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

1 ness entities invoking the risk assessment exemption
2 under section 322(b) of this Act and the response of
3 the United States Secret Service to such notices;
4 and

5 (2) the number and nature of security breaches
6 subject to the national security and law enforcement
7 exemptions under section 322(a) of this Act.

8 **SEC. 332. EFFECTIVE DATE.**

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

12 **TITLE IV—GOVERNMENT AC-**
13 **CESS TO AND USE OF COM-**
14 **MERCIAL DATA**

15 **SEC. 401. GENERAL SERVICES ADMINISTRATION REVIEW**
16 **OF CONTRACTS.**

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

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

1 es privacy and security threats created by malicious
2 software or code, or the use of peer-to-peer file shar-
3 ing software;

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

6 (3) the extent to which the databases and sys-
7 tems containing personally identifiable information
8 of a data broker have been compromised by security
9 breaches; and

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

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

21 (c) PENALTIES.—In awarding contracts with data
22 brokers for products or services related to access, use,
23 compilation, distribution, processing, analyzing, or evalu-
24 ating personally identifiable information, the Adminis-
25 trator of the General Services Administration shall—

1 (1) include monetary or other penalties—

2 (A) for failure to comply with subtitles A
3 and B of title IV of this Act; or

4 (B) if a contractor knows or has reason to
5 know that the personally identifiable informa-
6 tion being provided is inaccurate, and provides
7 such inaccurate information; and

8 (2) require a data broker that engages service
9 providers not subject to subtitle A of title IV for re-
10 sponsibilities related to sensitive personally identifi-
11 able information to—

12 (A) exercise appropriate due diligence in
13 selecting those service providers for responsibil-
14 ities related to personally identifiable informa-
15 tion;

16 (B) take reasonable steps to select and re-
17 tain service providers that are capable of main-
18 taining appropriate safeguards for the security,
19 privacy, and integrity of the personally identifi-
20 able information at issue; and

21 (C) require such service providers, by con-
22 tract, to implement and maintain appropriate
23 measures designed to meet the objectives and
24 requirements in title IV.

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

5 **SEC. 402. REQUIREMENT TO AUDIT INFORMATION SECU-**
6 **RITY PRACTICES OF CONTRACTORS AND**
7 **THIRD PARTY BUSINESS ENTITIES.**

8 Section 3544(b) of title 44, United States Code, is
9 amended—

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

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

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

15 “(9) procedures for evaluating and auditing the
16 information security practices of contractors or third
17 party business entities supporting the information
18 systems or operations of the agency involving per-
19 sonally identifiable information (as that term is de-
20 fined in section 3 of the Personal Data Privacy and
21 Security Act of 2005) and ensuring remedial action
22 to address any significant deficiencies.”.

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

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

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

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

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

12 “(iii) purchasing or subscribing for a
13 fee to personally identifiable information
14 from a data broker (as such terms are de-
15 fined in section 3 of the Personal Data
16 Privacy and Security Act of 2005).”.

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

25 (1) completes a privacy impact assessment
26 under section 208 of the E-Government Act of 2002

1 (44 U.S.C. 3501 note), which shall subject to the
2 provision in that Act pertaining to sensitive informa-
3 tion, include a description of—

4 (A) such database;

5 (B) the name of the data broker from
6 whom it is obtained; and

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

8 (2) adopts regulations that specify—

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

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

13 (C) any standards used to ensure that the
14 personally identifiable information accessed,
15 analyzed, or used is the minimum necessary to
16 accomplish the intended legitimate purpose of
17 the Federal agency;

18 (D) standards limiting the retention and
19 redisclosure of personally identifiable informa-
20 tion obtained from such databases;

21 (E) procedures ensuring that such data
22 meet standards of accuracy, relevance, com-
23 pleteness, and timeliness;

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

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

8 (H) mechanisms, if any, for the enforce-
9 ment and independent oversight of existing or
10 planned procedures, policies, or guidelines; and

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

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

18 (A) providing for penalties—

19 (i) for failure to comply with title IV
20 of this Act; or

21 (ii) if the entity knows or has reason
22 to know that the personally identifiable in-
23 formation being provided to the Federal
24 department or agency is inaccurate, and
25 provides such inaccurate information; and

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

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

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

15 (iii) require such service providers, by
16 contract, to implement and maintain appro-
17 priate measures designed to meet the ob-
18 jectives and requirements in title IV.

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

23 (d) STUDY OF GOVERNMENT USE.—

24 (1) SCOPE OF STUDY.—Not later than 180
25 days after the date of enactment of this Act, the

1 Comptroller General of the United States shall con-
2 duct a study and audit and prepare a report on Fed-
3 eral agency use of data brokers or commercial data-
4 bases containing personally identifiable information,
5 including the impact on privacy and security, and
6 the extent to which Federal contracts include suffi-
7 cient provisions to ensure privacy and security pro-
8 tections, and penalties for failures in privacy and se-
9 curity practices.

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

12 **SEC. 404. IMPLEMENTATION OF CHIEF PRIVACY OFFICER**
13 **REQUIREMENTS.**

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

1 (b) DUTIES AND RESPONSIBILITIES OF CHIEF PRI-
2 VACY OFFICER.—In addition to the duties and responsibil-
3 ities outlined under section 522 of the Transportation,
4 Treasury, Independent Agencies, and General Government
5 Appropriations Act, 2005 (division H of Public Law 108–
6 447; 118 Stat. 3199), the Department of Justice Chief
7 Privacy Officer shall—

8 (1) oversee the Department of Justice’s imple-
9 mentation of the requirements under section 603 to
10 conduct privacy impact assessments of the use of
11 commercial data containing personally identifiable
12 information by the Department; and

13 (2) coordinate with the Privacy and Civil Lib-
14 erties Oversight Board, established in the Intel-
15 ligence Reform and Terrorism Prevention Act of
16 2004 (Public Law 108–458), in implementing this
17 section.