

109TH CONGRESS  
1ST SESSION

# 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.

---

## IN THE SENATE OF THE UNITED STATES

SEPTEMBER 29, 2005

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

---

## A BILL

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

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

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

4 (a) SHORT TITLE.—This Act may be cited as the  
5 “Personal Data Privacy and Security Act of 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. Fraud and related criminal activity in connection with unauthorized access to personally identifiable information.
- Sec. 102. Organized criminal activity in connection with unauthorized access to personally identifiable information.
- Sec. 103. Concealment of security breaches involving sensitive personally identifiable information.
- Sec. 104. Aggravated fraud in connection with computers.
- Sec. 105. Review and amendment of Federal sentencing guidelines related to fraudulent access to or misuse of digitized or electronic personally identifiable information.

TITLE II—ASSISTANCE FOR STATE AND LOCAL LAW ENFORCEMENT  
COMBATING CRIMES RELATED TO FRAUDULENT, UNAUTHORIZED, OR OTHER CRIMINAL USE OF PERSONALLY IDENTIFIABLE INFORMATION

- Sec. 201. Grants for State and local enforcement.
- Sec. 202. Authorization of appropriations.

TITLE III—DATA BROKERS

- Sec. 301. Transparency and accuracy of data collection.
- Sec. 302. Enforcement.
- Sec. 303. Relation to State laws.
- Sec. 304. Effective date.

TITLE IV—PRIVACY AND SECURITY OF PERSONALLY  
IDENTIFIABLE INFORMATION

Subtitle A—Data Privacy and Security Program

- Sec. 401. Purpose and applicability of data privacy and security program.
- Sec. 402. Requirements for a personal data privacy and security program.
- Sec. 403. Enforcement.
- Sec. 404. Relation to State laws.

Subtitle B—Security Breach Notification

- Sec. 421. Right to notice of security breach.
- Sec. 422. Notice procedures.
- Sec. 423. Content of notice.
- Sec. 424. Risk assessment and fraud prevention notice exemptions.
- Sec. 425. Victim protection assistance.
- Sec. 426. Enforcement.
- Sec. 427. Relation to State laws.
- Sec. 428. Study on securing personally identifiable information in the digital era.
- Sec. 429. Reporting on risk assessment exemption.
- Sec. 430. Authorization of appropriations.
- Sec. 431. Reporting on risk assessment exemption.
- Sec. 432. Effective date.

TITLE V—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL  
DATA

Sec. 501. General Services Administration review of contracts.

Sec. 502. Requirement to audit information security practices of contractors and third party business entities.

Sec. 503. Privacy impact assessment of government use of commercial information services containing personally identifiable information.

Sec. 504. 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;

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

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

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

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

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

24          (11) because government use of commercial  
25          data containing personal information potentially af-

1       fects individual privacy, and law enforcement and  
2       national security operations, there is a need for Con-  
3       gress to exercise oversight over government use of  
4       commercial data.

5 **SEC. 3. DEFINITIONS.**

6       In this Act:

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

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

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

20          (4) IDENTITY THEFT.—The term “identity  
21       theft” means a violation of section 1028 of title 18,  
22       United States Code, or any other similar provision  
23       of applicable State law.

24          (5) DATA BROKER.—The term “data broker”  
25       means a business entity which for monetary fees,

1 dues, or on a cooperative nonprofit basis, currently  
2 or regularly engages, in whole or in part, in the  
3 practice of collecting, transmitting, or providing ac-  
4 cess to sensitive personally identifiable information  
5 primarily for the purposes of providing such infor-  
6 mation to nonaffiliated third parties on a nationwide  
7 basis on more than 5,000 individuals who are not  
8 the customers or employees of the business entity or  
9 affiliate.

10 (6) DATA FURNISHER.—The term “data fur-  
11 nisher” means any agency, governmental entity, or-  
12 ganization, corporation, trust, partnership, sole pro-  
13 prietorship, unincorporated association, venture es-  
14 tablished to make a profit, or nonprofit, and any  
15 contractor, subcontractor, affiliate, or licensee there-  
16 of, that serves as a source of information for a data  
17 broker.

18 (7) PERSONAL ELECTRONIC RECORD.—The  
19 term “personal electronic record” means data associ-  
20 ated with an individual contained in a database,  
21 networked or integrated databases, or other data  
22 system that holds sensitive personally identifiable in-  
23 formation of that individual and is provided to non-  
24 affiliated third parties.

1           (8) PERSONALLY IDENTIFIABLE INFORMA-  
2           TION.—The term “personally identifiable informa-  
3           tion” means any information, or compilation of in-  
4           formation, in electronic or digital form serving as a  
5           means of identification, as defined by section  
6           1028(d)(7) of title 18, United State Code.

7           (9) PUBLIC RECORD SOURCE.—The term “pub-  
8           lic record source” means any agency, Federal court,  
9           or State court that maintains personally identifiable  
10          information in records available to the public.

11          (10) SECURITY BREACH.—

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

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

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

1 the sensitive personally identifiable infor-  
2 mation is not subject to further unauthor-  
3 ized disclosure; or

4 (ii) the release of a public record not  
5 otherwise subject to confidentiality or non-  
6 disclosure requirements.

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

12 (A) An individual’s name in combination  
13 with any 1 of the following data elements:

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

17 (ii) Any 2 of the following:

18 (I) Information that relates to—

19 (aa) the past, present, or fu-  
20 ture physical or mental health or  
21 condition of an individual;

22 (bb) the provision of health  
23 care to an individual; or

1 (cc) the past, present, or fu-  
2 ture payment for the provision of  
3 health care to an individual.

4 (II) Home address or telephone  
5 number.

6 (III) Mother's maiden name, if  
7 identified as such.

8 (IV) Month, day, and year of  
9 birth.

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

14 (iv) A unique electronic identification  
15 number, user name, or routing code in  
16 combination with the associated security  
17 code, access code, or password.

18 (v) Any other information regarding  
19 an individual determined appropriate by  
20 the Federal Trade Commission.

21 (B) A financial account number or credit  
22 or debit card number in combination with the  
23 required security code, access code, or pass-  
24 word.

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. FRAUD AND RELATED CRIMINAL ACTIVITY IN**  
7 **CONNECTION WITH UNAUTHORIZED ACCESS**  
8 **TO PERSONALLY IDENTIFIABLE INFORMA-**  
9 **TION.**

10 Section 1030(a)(2) of title 18, United States Code,  
11 is amended—

12 (1) in subparagraph (B), by striking “or” after  
13 the semicolon;

14 (2) in subparagraph (C), by inserting “or” after  
15 the semicolon; and

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

17 “(D) information contained in the data-  
18 bases or systems of a data broker, or in other  
19 personal electronic records, as such terms are  
20 defined in section 3 of the Personal Data Pri-  
21 vacy and Security Act of 2005;”.

1 **SEC. 102. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION**  
2 **WITH UNAUTHORIZED ACCESS TO PERSON-**  
3 **ALLY IDENTIFIABLE INFORMATION.**

4 Section 1961(1) of title 18, United States Code, is  
5 amended by inserting “section 1030(a)(2)(D)(relating to  
6 fraud and related activity in connection with unauthorized  
7 access to personally identifiable information,” before “sec-  
8 tion 1084”.

9 **SEC. 103. CONCEALMENT OF SECURITY BREACHES INVOLV-**  
10 **ING SENSITIVE PERSONALLY IDENTIFIABLE**  
11 **INFORMATION.**

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

15 **“§ 1039. Concealment of security breaches involving**  
16 **sensitive personally identifiable informa-**  
17 **tion**

18 “(a) Whoever, having knowledge of a security breach  
19 and the obligation to provide notice of such breach to indi-  
20 viduals under title IV of the Personal Data Privacy and  
21 Security Act of 2005, and having not otherwise qualified  
22 for an exemption from providing notice under section 422  
23 of such Act, intentionally and willfully conceals the fact  
24 of such security breach which causes economic damages  
25 to 1 or more persons, shall be fined under this title or  
26 imprisoned not more than 5 years, or both.

1       “(b) For purposes of subsection (a), the term ‘person’  
 2 means any individual, corporation, company, association,  
 3 firm, partnership, society, or joint stock company.”.

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

“1039. Concealment of security breaches involving personally identifiable infor-  
 mation.”.

8       (c) ENFORCEMENT AUTHORITY.—The United States  
 9 Secret Service shall have the authority to investigate of-  
 10 fenses under this section.

11 **SEC. 104. AGGRAVATED FRAUD IN CONNECTION WITH COM-**  
 12 **PUTERS.**

13       (a) IN GENERAL.—Chapter 47 of title 18, United  
 14 States Code, is amended by adding after section 1030 the  
 15 following:

16 **“§ 1030A. Aggravated fraud in connection with com-**  
 17 **puters**

18       “(a) IN GENERAL.—Whoever, during and in relation  
 19 to any felony violation enumerated in subsection (c),  
 20 knowingly obtains, accesses, or transmits, without lawful  
 21 authority, a means of identification of another person  
 22 may, in addition to the punishment provided for such fel-  
 23 ony, be sentenced to a term of imprisonment of up to 2  
 24 years.

1       “(b) CONSECUTIVE SENTENCES.—Notwithstanding  
2 any other provision of law, should a court in its discretion  
3 impose an additional sentence under subsection (a)—

4           “(1) no term of imprisonment imposed on a  
5 person under this section shall run concurrently, ex-  
6 cept as provided in paragraph (3), with any other  
7 term of imprisonment imposed on such person under  
8 any other provision of law, including any term of im-  
9 prisonment imposed for the felony during which the  
10 means of identifications was obtained, accessed, or  
11 transmitted;

12           “(2) in determining any term of imprisonment  
13 to be imposed for the felony during which the means  
14 of identification was obtained, accessed, or trans-  
15 mitted, a court shall not in any way reduce the term  
16 to be imposed for such crime so as to compensate  
17 for, or otherwise take into account, any separate  
18 term of imprisonment imposed or to be imposed for  
19 a violation of this section; and

20           “(3) a term of imprisonment imposed on a per-  
21 son for a violation of this section may, in the discre-  
22 tion of the court, run concurrently, in whole or in  
23 part, only with another term of imprisonment that  
24 is imposed by the court at the same time on that  
25 person for an additional violation of this section.

1       “(c) DEFINITION.—For purposes of this section, the  
 2 term ‘felony violation enumerated in subsection (c)’ means  
 3 any offense that is a felony violation of paragraphs (2)  
 4 through (7) of section 1030(a).”.

5       (b) CONFORMING AND TECHNICAL AMENDMENTS.—  
 6 The table of sections for chapter 47 of title 18, United  
 7 States Code, is amended by inserting after the item relat-  
 8 ing to section 1030 the following new item:

“1030A. Aggravated fraud in connection with computers.”.

9       **SEC. 105. REVIEW AND AMENDMENT OF FEDERAL SEN-**  
 10                               **TENCING GUIDELINES RELATED TO FRAUDU-**  
 11                               **LENT ACCESS TO OR MISUSE OF DIGITIZED**  
 12                               **OR ELECTRONIC PERSONALLY IDENTIFIABLE**  
 13                               **INFORMATION.**

14       (a) REVIEW AND AMENDMENT.—Not later than 180  
 15 days after the date of enactment of this Act, the United  
 16 States Sentencing Commission, pursuant to its authority  
 17 under section 994 of title 28, United States Code, and  
 18 in accordance with this section, shall review and, if appro-  
 19 priate, amend the Federal sentencing guidelines (including  
 20 its policy statements) applicable to persons convicted of  
 21 using fraud to access, or misuse of, digitized or electronic  
 22 personally identifiable information, including identity theft  
 23 or any offense under—

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

1 (2) any other relevant provision.

2 (b) REQUIREMENTS.—In carrying out the require-  
3 ments of this section, the United States Sentencing Com-  
4 mission shall—

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

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

9 (B) the growing incidences of theft and  
10 misuse of digitized or electronic personally iden-  
11 tifiable information, including identity theft;  
12 and

13 (C) the need to deter, prevent, and punish  
14 such offenses;

15 (2) consider the extent to which the Federal  
16 sentencing guidelines (including its policy state-  
17 ments) adequately address violations of the sections  
18 amended by this Act to—

19 (A) sufficiently deter and punish such of-  
20 fenses; and

21 (B) adequately reflect the enhanced pen-  
22 alties established under this Act;

23 (3) maintain reasonable consistency with other  
24 relevant directives and sentencing guidelines;

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

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

7                 (A) the online sale of fraudulently obtained  
8 or stolen personally identifiable information;

9                 (B) the sale of fraudulently obtained or  
10 stolen personally identifiable information to an  
11 individual who is engaged in terrorist activity or  
12 aiding other individuals engaged in terrorist ac-  
13 tivity; or

14                 (C) the sale of fraudulently obtained or  
15 stolen personally identifiable information to fi-  
16 nance terrorist activity or other criminal activi-  
17 ties;

18           (6) make any necessary conforming changes to  
19 the Federal sentencing guidelines to ensure that  
20 such guidelines (including its policy statements) as  
21 described in subsection (a) are sufficiently stringent  
22 to deter, and adequately reflect crimes related to  
23 fraudulent access to, or misuse of, personally identi-  
24 fiable information; and

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

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

12 **TITLE II—ASSISTANCE FOR**  
13 **STATE AND LOCAL LAW EN-**  
14 **FORCEMENT COMBATING**  
15 **CRIMES RELATED TO FRAUD-**  
16 **ULENT, UNAUTHORIZED, OR**  
17 **OTHER CRIMINAL USE OF**  
18 **PERSONALLY IDENTIFIABLE**  
19 **INFORMATION**

20 **SEC. 201. GRANTS FOR STATE AND LOCAL ENFORCEMENT.**

21           (a) IN GENERAL.—Subject to the availability of  
22 amounts provided in advance in appropriations Acts, the  
23 Assistant Attorney General for the Office of Justice Pro-  
24 grams of the Department of Justice may award a grant  
25 to a State to establish and develop programs to increase

1 and enhance enforcement against crimes related to fraud-  
2 ulent, unauthorized, or other criminal use of personally  
3 identifiable information.

4 (b) APPLICATION.—A State seeking a grant under  
5 subsection (a) shall submit an application to the Assistant  
6 Attorney General for the Office of Justice Programs of  
7 the Department of Justice at such time, in such manner,  
8 and containing such information as the Assistant Attorney  
9 General may require.

10 (c) USE OF GRANT AMOUNTS.—A grant awarded to  
11 a State under subsection (a) shall be used by a State, in  
12 conjunction with units of local government within that  
13 State, State and local courts, other States, or combina-  
14 tions thereof, to establish and develop programs to—

15 (1) assist State and local law enforcement agen-  
16 cies in enforcing State and local criminal laws relat-  
17 ing to crimes involving the fraudulent, unauthorized,  
18 or other criminal use of personally identifiable infor-  
19 mation;

20 (2) assist State and local law enforcement agen-  
21 cies in educating the public to prevent and identify  
22 crimes involving the fraudulent, unauthorized, or  
23 other criminal use of personally identifiable informa-  
24 tion;

1           (3) educate and train State and local law en-  
2           forcement officers and prosecutors to conduct inves-  
3           tigations and forensic analyses of evidence and pros-  
4           ecutions of crimes involving the fraudulent, unau-  
5           thorized, or other criminal use of personally identifi-  
6           able information;

7           (4) assist State and local law enforcement offi-  
8           cers and prosecutors in acquiring computer and  
9           other equipment to conduct investigations and foren-  
10          sic analysis of evidence of crimes involving the  
11          fraudulent, unauthorized, or other criminal use of  
12          personally identifiable information; and

13          (5) facilitate and promote the sharing of Fed-  
14          eral law enforcement expertise and information  
15          about the investigation, analysis, and prosecution of  
16          crimes involving the fraudulent, unauthorized, or  
17          other criminal use of personally identifiable informa-  
18          tion with State and local law enforcement officers  
19          and prosecutors, including the use of multi-jurisdic-  
20          tional task forces.

21          (d) ASSURANCES AND ELIGIBILITY.—To be eligible  
22          to receive a grant under subsection (a), a State shall pro-  
23          vide assurances to the Attorney General that the State—

24                (1) has in effect laws that penalize crimes in-  
25                volving the fraudulent, unauthorized, or other crimi-

1       nal use of personally identifiable information, such  
2       as penal laws prohibiting—

3               (A) fraudulent schemes executed to obtain  
4       personally identifiable information;

5               (B) schemes executed to sell or use fraudu-  
6       lently obtained personally identifiable informa-  
7       tion; and

8               (C) online sales of personally identifiable  
9       information obtained fraudulently or by other  
10       illegal means;

11       (2) will provide an assessment of the resource  
12       needs of the State and units of local government  
13       within that State, including criminal justice re-  
14       sources being devoted to the investigation and en-  
15       forcement of laws related to crimes involving the  
16       fraudulent, unauthorized, or other criminal use of  
17       personally identifiable information; and

18       (3) will develop a plan for coordinating the pro-  
19       grams funded under this section with other federally  
20       funded technical assistant and training programs,  
21       including directly funded local programs such as the  
22       Local Law Enforcement Block Grant program (de-  
23       scribed under the heading “Violent Crime Reduction  
24       Programs, State and Local Law Enforcement As-  
25       sistance” of the Departments of Commerce, Justice,

1 and State, the Judiciary, and Related Agencies Ap-  
2 propriations Act, 1998 (Public Law 105–119)).

3 (e) **MATCHING FUNDS.**—The Federal share of a  
4 grant received under this section may not exceed 90 per-  
5 cent of the total cost of a program or proposal funded  
6 under this section unless the Attorney General waives,  
7 wholly or in part, the requirements of this subsection.

8 **SEC. 202. AUTHORIZATION OF APPROPRIATIONS.**

9 (a) **IN GENERAL.**—There is authorized to be appro-  
10 priated to carry out this title \$25,000,000 for each of fis-  
11 cal years 2006 through 2009.

12 (b) **LIMITATIONS.**—Of the amount made available to  
13 carry out this title in any fiscal year not more than 3 per-  
14 cent may be used by the Attorney General for salaries and  
15 administrative expenses.

16 (c) **MINIMUM AMOUNT.**—Unless all eligible applica-  
17 tions submitted by a State or units of local government  
18 within a State for a grant under this title have been fund-  
19 ed, the State, together with grantees within the State  
20 (other than Indian tribes), shall be allocated in each fiscal  
21 year under this title not less than 0.75 percent of the total  
22 amount appropriated in the fiscal year for grants pursuant  
23 to this title, except that the United States Virgin Islands,  
24 American Samoa, Guam, and the Northern Mariana Is-  
25 lands each shall be allocated 0.25 percent.

1 (d) GRANTS TO INDIAN TRIBES.—Notwithstanding  
2 any other provision of this title, the Attorney General may  
3 use amounts made available under this title to make  
4 grants to Indian tribes for use in accordance with this  
5 title.

## 6 **TITLE III—DATA BROKERS**

### 7 **SEC. 301. TRANSPARENCY AND ACCURACY OF DATA COL-** 8 **LECTION.**

9 (a) IN GENERAL.—Data brokers engaging in inter-  
10 state commerce are subject to the requirements of this  
11 title for any product or service offered to third parties that  
12 allows access, use, compilation, distribution, processing,  
13 analyzing, or evaluation of sensitive personally identifiable  
14 information.

15 (b) LIMITATION.—Notwithstanding any other para-  
16 graph of this title, this section shall not apply to—

17 (1) data brokers engaging in interstate com-  
18 merce for any offered product or service currently  
19 subject to, and in compliance with, access and accu-  
20 racy protections similar to those under subsections  
21 (c) through (f) of this section under the Fair Credit  
22 Reporting Act (Public Law 91–508), or the Gramm-  
23 Leach Bliley Act (Public Law 106–102);

24 (2) data brokers engaging in interstate com-  
25 merce for any offered product or service currently in

1 compliance with the requirements for such entities  
2 under the Health Insurance Portability and Ac-  
3 countability Act (Public Law 104–191), and imple-  
4 menting regulations;

5 (3) information in a personal electronic record  
6 held by a data broker if—

7 (A) the data broker maintains such infor-  
8 mation solely pursuant to a license agreement  
9 with another business entity; and

10 (B) the business entity providing such in-  
11 formation to the data broker pursuant to a li-  
12 cense agreement either complies with the provi-  
13 sions of this section or qualifies for this exemp-  
14 tion; and

15 (4) information in a personal record that—

16 (A) the data broker has identified as inac-  
17 curate, but maintains for the purpose of aiding  
18 the data broker in preventing inaccurate infor-  
19 mation from entering an individual’s personal  
20 electronic record; and

21 (B) is not maintained primarily for the  
22 purpose of transmitting or otherwise providing  
23 that information, or assessments based on that  
24 information, to non-affiliated third parties.

25 (c) DISCLOSURES TO INDIVIDUALS.—

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

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 the processes and procedures for demonstrating  
13          and correcting any inaccuracies.

14          (d) CREATION OF AN ACCURACY RESOLUTION PROC-  
15          ESS.—A data broker shall develop and publish on its  
16          website timely and fair processes and procedures for re-  
17          sponding to claims of inaccuracies, including procedures  
18          for correcting inaccurate information in the personal elec-  
19          tronic records it maintains on individuals.

20          (e) ACCURACY RESOLUTION PROCESS.—

21                 (1) INFORMATION FROM A PUBLIC RECORD  
22                 SOURCE.—

23                         (A) IN GENERAL.—If an individual notifies  
24                         a data broker of a dispute as to the complete-  
25                         ness or accuracy of information, and the data

1 broker determines that such information is de-  
2 rived from a public record source, the data  
3 broker shall determine within 30 days whether  
4 the information in its system accurately and  
5 completely records the information offered by  
6 the public record source.

7 (B) DATA BROKER ACTIONS.—If a data  
8 broker determines under subparagraph (A) that  
9 the information in its systems—

10 (i) does not accurately and completely  
11 record the information offered by a public  
12 record source, the data broker shall correct  
13 any inaccuracies or incompleteness, and  
14 provide to such individual written notice of  
15 such changes; and

16 (ii) does accurately and completely  
17 record the information offered by a public  
18 record source, the data broker shall—

19 (I) provide such individual with  
20 the name, address, and telephone con-  
21 tact information of the public record  
22 source; and

23 (II) notify such individual of the  
24 right to add for a period of 90 days  
25 to the personal electronic record of

1                   the individual maintained by the data  
2                   broker notice of the dispute under  
3                   subsection (f).

4                   (2) INVESTIGATION OF DISPUTED INFORMATION  
5                   NOT FROM A PUBLIC RECORD SOURCE.—If the com-  
6                   pleteness or accuracy of any nonpublic record source  
7                   disclosed to an individual under subsection (c) is dis-  
8                   puted by the individual and such individual notifies  
9                   the data broker directly of such dispute, the data  
10                  broker shall, before the end of the 30-day period be-  
11                  ginning on the date on which the data broker re-  
12                  ceives the notice of the dispute—

13                   (A) investigate free of charge and record  
14                   the current status of the disputed information;  
15                   or

16                   (B) delete the item from the individuals  
17                   data file in accordance with paragraph (8).

18                   (3) EXTENSION OF PERIOD TO INVESTIGATE.—  
19                   Except as provided in paragraph (4), the 30-day pe-  
20                   riod described in paragraph (1) may be extended for  
21                   not more than 15 additional days if a data broker  
22                   receives information from the individual during that  
23                   30-day period that is relevant to the investigation.

24                   (4) LIMITATIONS ON EXTENSION OF PERIOD TO  
25                   INVESTIGATE.—Paragraph (3) shall not apply to any

1 investigation in which, during the 30-day period de-  
2 scribed in paragraph (1), the information that is the  
3 subject of the investigation is found to be inaccurate  
4 or incomplete or a data broker determines that the  
5 information cannot be verified.

6 (5) NOTICE IDENTIFYING THE DATA FUR-  
7 NISHER.—If the completeness or accuracy of any in-  
8 formation disclosed to an individual under sub-  
9 section (c) is disputed by the individual, a data  
10 broker shall provide upon the request of the indi-  
11 vidual, the name, business address, and telephone  
12 contact information of any data furnisher who pro-  
13 vided an item of information in dispute.

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

16 (A) IN GENERAL.—Notwithstanding para-  
17 graphs (1) through (4), a data broker may de-  
18 cline to investigate or terminate an investiga-  
19 tion of information disputed by an individual  
20 under those paragraphs if the data broker rea-  
21 sonably determines that the dispute by the indi-  
22 vidual is frivolous or irrelevant, including by  
23 reason of a failure by the individual to provide  
24 sufficient information to investigate the dis-  
25 puted information.

1 (B) NOTICE.—Not later than 5 business  
2 days after making any determination in accord-  
3 ance with subparagraph (A) that a dispute is  
4 frivolous or irrelevant, a data broker shall no-  
5 tify the individual of such determination by  
6 mail, or if authorized by the individual, by any  
7 other means available to the data broker.

8 (C) CONTENTS OF NOTICE.—A notice  
9 under subparagraph (B) shall include—

10 (i) the reasons for the determination  
11 under subparagraph (A); and

12 (ii) identification of any information  
13 required to investigate the disputed infor-  
14 mation, which may consist of a standard-  
15 ized form describing the general nature of  
16 such information.

17 (7) CONSIDERATION OF INDIVIDUAL INFORMA-  
18 TION.—In conducting any investigation with respect  
19 to disputed information in the personal electronic  
20 record of any individual, a data broker shall review  
21 and consider all relevant information submitted by  
22 the individual in the period described in paragraph  
23 (2) with respect to such disputed information.

24 (8) TREATMENT OF INACCURATE OR UNVERIFI-  
25 ABLE INFORMATION.—

1           (A) IN GENERAL.—If, after any review of  
2 public record information under paragraph (1)  
3 or any investigation of any information disputed  
4 by an individual under paragraphs (2) through  
5 (4), an item of information is found to be inac-  
6 curate or incomplete or cannot be verified, a  
7 data broker shall promptly delete that item of  
8 information from the individual’s personal elec-  
9 tronic record or modify that item of informa-  
10 tion, as appropriate, based on the results of the  
11 investigation.

12           (B) NOTICE TO INDIVIDUALS OF REINSER-  
13 TION OF PREVIOUSLY DELETED INFORMA-  
14 TION.—If any information that has been de-  
15 leted from an individual’s personal electronic  
16 record pursuant to subparagraph (A) is re-  
17 inserted in the personal electronic record of the  
18 individual, a data broker shall, not later than 5  
19 days after reinsertion, notify the individual of  
20 the reinsertion and identify any data furnisher  
21 not previously disclosed in writing, or if author-  
22 ized by the individual for that purpose, by any  
23 other means available to the data broker, unless  
24 such notification has been previously given  
25 under this subsection.

1 (C) NOTICE OF RESULTS OF INVESTIGA-  
2 TION OF DISPUTED INFORMATION FROM A NON-  
3 PUBLIC RECORD SOURCE.—

4 (i) IN GENERAL.—Not later than 5  
5 business days after the completion of an  
6 investigation under paragraph (2), a data  
7 broker shall provide written notice to an  
8 individual of the results of the investiga-  
9 tion, by mail or, if authorized by the indi-  
10 vidual for that purpose, by other means  
11 available to the data broker.

12 (ii) ADDITIONAL REQUIREMENT.—Be-  
13 fore the expiration of the 5-day period, as  
14 part of, or in addition to such notice, a  
15 data broker shall, in writing, provide to an  
16 individual—

17 (I) a statement that the inves-  
18 tigation is completed;

19 (II) a report that is based upon  
20 the personal electronic record of such  
21 individual as that personal electronic  
22 record is revised as a result of the in-  
23 vestigation;

24 (III) a notice that, if requested  
25 by the individual, a description of the

1 procedures used to determine the ac-  
2 curacy and completeness of the infor-  
3 mation shall be provided to the indi-  
4 vidual by the data broker, including  
5 the business name, address, and tele-  
6 phone number of any data furnisher  
7 of information contacted in connection  
8 with such information; and

9 (IV) a notice that the individual  
10 has the right to request notifications  
11 under subsection (f).

12 (D) DESCRIPTION OF INVESTIGATION PRO-  
13 CEDURES.—Not later than 15 days after receiv-  
14 ing a request from an individual for a descrip-  
15 tion referred to in subparagraph (C)(ii)(III), a  
16 data broker shall provide to the individual such  
17 a description.

18 (E) EXPEDITED DISPUTE RESOLUTION.—  
19 If by no later than 3 business days after the  
20 date on which a data broker receives notice of  
21 a dispute from an individual of information in  
22 the personal electronic record of such individual  
23 in accordance with paragraph (2), a data  
24 broker resolves such dispute in accordance with  
25 subparagraph (A) by the deletion of the dis-

1           puted information, then the data broker shall  
2           not be required to comply with subsections (e)  
3           and (f) with respect to that dispute if the data  
4           broker provides to the individual, by telephone  
5           or other means authorized by the individual,  
6           prompt notice of the deletion.

7           (f) NOTICE OF DISPUTE.—

8           (1) IN GENERAL.—If the completeness or accu-  
9           racy of any information disclosed to an individual  
10          under subsection (c) is disputed and unless there is  
11          a reasonable ground to believe that such dispute is  
12          frivolous or irrelevant, an individual may request  
13          that the data broker indicate notice of the dispute  
14          for a period of—

15                (A) 30 days for information from a non-  
16                public record source; and

17                (B) 90 days for information from a public  
18                record source.

19          (2) COMPLIANCE.—A data broker shall be  
20          deemed in compliance with the requirements under  
21          paragraph (1) by either—

22                (A) allowing the individual to file a brief  
23                statement setting forth the nature of the dis-  
24                pute under paragraph (3); or

1 (B) using an alternative notice method  
2 that—

3 (i) clearly flags the disputed informa-  
4 tion for third parties accessing the infor-  
5 mation; and

6 (ii) provides a means for third parties  
7 to obtain further information regarding the  
8 nature of the dispute.

9 (3) CONTENTS OF STATEMENT.—A data broker  
10 may limit statements made under paragraph (2)(A)  
11 to not more than 100 words if it provides an indi-  
12 vidual with assistance in writing a clear summary of  
13 the dispute or until the dispute is resolved.

14 (g) ADDITIONAL REQUIREMENTS.—The Federal  
15 Trade Commission may exempt certain classes of data  
16 brokers from this title in a rulemaking process pursuant  
17 to section 553 of title 5, United States Code.

18 **SEC. 302. ENFORCEMENT.**

19 (a) CIVIL PENALTIES.—

20 (1) PENALTIES.—Any data broker that violates  
21 the provisions of section 301 shall be subject to civil  
22 penalties of not more than \$1,000 per violation per  
23 day, with a maximum of \$15,000 per day, while  
24 such violations persist.

1           (2) INTENTIONAL OR WILLFUL VIOLATION.—A  
2 data broker that intentionally or willfully violates the  
3 provisions of section 301 shall be subject to addi-  
4 tional penalties in the amount of \$1,000 per viola-  
5 tion per day, with a maximum of an additional  
6 \$15,000 per day, while such violations persist.

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

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

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

17           (1) IN GENERAL.—Whenever it appears that a  
18 data broker to which this title applies has engaged,  
19 is engaged, or is about to engage, in any act or prac-  
20 tice constituting a violation of this title, the Attorney  
21 General may bring a civil action in an appropriate  
22 district court of the United States to—

23                   (A) enjoin such act or practice;

24                   (B) enforce compliance with this title;

25                   (C) obtain damages—

1 (i) in the sum of actual damages, res-  
2 titution, and other compensation on behalf  
3 of the affected residents of a State; and

4 (ii) punitive damages, if the violation  
5 is willful or intentional; and

6 (D) obtain such other relief as the court  
7 determines to be appropriate.

8 (2) OTHER INJUNCTIVE RELIEF.—Upon a  
9 proper showing in the action under paragraph (1),  
10 the court shall grant a permanent injunction or a  
11 temporary restraining order without bond.

12 (c) STATE ENFORCEMENT.—

13 (1) CIVIL ACTIONS.—In any case in which the  
14 attorney general of a State has reason to believe  
15 that an interest of the residents of that State has  
16 been or is threatened or adversely affected by an act  
17 or practice that violates this title, the State may  
18 bring a civil action on behalf of the residents of that  
19 State in a district court of the United States of ap-  
20 propriate jurisdiction, or any other court of com-  
21 petent jurisdiction, to—

22 (A) enjoin that act or practice;

23 (B) enforce compliance with this title;

24 (C) obtain—

1 (i) damages in the sum of actual dam-  
2 ages, restitution, or other compensation on  
3 behalf of affected residents of the State;  
4 and

5 (ii) punitive damages, if the violation  
6 is willful or intentional; or

7 (D) obtain such other legal and equitable  
8 relief as the court may consider to be appro-  
9 priate.

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 Attorney  
14 General—

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 Attorney General as soon after the filing of  
6 the complaint as practicable.

7 (3) ATTORNEY GENERAL AUTHORITY.—Upon  
8 receiving notice under paragraph (2), the Attorney  
9 General shall have the right to—

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

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

15 (C) file petitions for appeal.

16 (4) PENDING PROCEEDINGS.—If the Attorney  
17 General has instituted a proceeding or action for a  
18 violation of this title or any regulations thereunder,  
19 no attorney general of a State may, during the pend-  
20 ency of such proceeding or action, bring an action  
21 under this subsection against any defendant named  
22 in such criminal proceeding or civil action for any  
23 violation that is alleged in that proceeding 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 1931 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 title establishes a private cause of action against a  
23 data broker for violation of any provision of this title.

1 **SEC. 303. RELATION TO STATE LAWS.**

2 No requirement or prohibition may be imposed under  
3 the laws of any State with respect to any subject matter  
4 regulated under section 301, relating to individual access  
5 to, and correction of, personal electronic records held by  
6 databrokers.

7 **SEC. 304. EFFECTIVE DATE.**

8 This title shall take effect 180 days after the date  
9 of enactment of this Act and shall be implemented pursu-  
10 ant to a State by State rollout schedule set by the Federal  
11 Trade Commission, but in no case shall full implementa-  
12 tion and effect of this title occur later than 1 year and  
13 180 days after the date of enactment of this Act.

14 **TITLE IV—PRIVACY AND SECURITY**  
15 **OF PERSONALLY IDENTIFIABLE INFORMATION**  
16 **Subtitle A—Data Privacy and**  
17 **Security Program**  
18

19 **SEC. 401. PURPOSE AND APPLICABILITY OF DATA PRIVACY**  
20 **AND SECURITY PROGRAM.**

21 (a) PURPOSE.—The purpose of this subtitle is to en-  
22 sure standards for developing and implementing adminis-  
23 trative, technical, and physical safeguards to protect the  
24 privacy, security, confidentiality, integrity, storage, and  
25 disposal of sensitive personally identifiable information.

1 (b) IN GENERAL.—A business entity engaging in  
2 interstate commerce that involves collecting, accessing,  
3 transmitting, using, storing, or disposing of sensitive per-  
4 sonally identifiable information in electronic or digital  
5 form on 10,000 or more United States persons is subject  
6 to the requirements for a data privacy and security pro-  
7 gram under section 402 for protecting sensitive personally  
8 identifiable information.

9 (c) LIMITATIONS.—Notwithstanding any other obli-  
10 gation under this subtitle, this subtitle does not apply to—

11 (1) financial institutions—

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

16 (B) subject to—

17 (i) examinations for compliance with  
18 the requirements of this Act by 1 or more  
19 Federal or State functional regulators (as  
20 defined in section 509 of the Gramm-  
21 Leach-Bliley Act (15 U.S.C. 6809)); or

22 (ii) compliance with part 314 of title  
23 16, Code of Federal Regulations; or

24 (2) “covered entities” subject to the Health In-  
25 surance Portability and Accountability Act of 1996

1 (42 U.S.C. 1301 et seq.), including the data security  
2 requirements and implementing regulations of that  
3 Act.

4 (d) SAFE HARBOR.—A business entity shall be  
5 deemed in compliance with the privacy and security pro-  
6 gram requirements under section 402 if the business enti-  
7 ty complies with or provides protection equal to industry  
8 standards, as identified by the Federal Trade Commission,  
9 that are applicable to the type of sensitive personally iden-  
10 tifiable information involved in the ordinary course of  
11 business of such business entity.

12 **SEC. 402. REQUIREMENTS FOR A PERSONAL DATA PRIVACY**  
13 **AND SECURITY PROGRAM.**

14 (a) PERSONAL DATA PRIVACY AND SECURITY PRO-  
15 GRAM.—Unless otherwise limited under section 401(c), a  
16 business entity subject to this subtitle shall comply with  
17 the following safeguards and any others identified by the  
18 Federal Trade Commission in a rulemaking process pursu-  
19 ant to section 553 of title 5, United States Code, to pro-  
20 tect the privacy and security of sensitive personally identi-  
21 fiable information:

22 (1) SCOPE.—A business entity shall implement  
23 a comprehensive personal data privacy and security  
24 program that includes administrative, technical, and  
25 physical safeguards appropriate to the size and com-

1       plexity of the business entity and the nature and  
2       scope of its activities.

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

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

7           (B) protect against any anticipated  
8       vulnerabilities to the privacy, security, or integ-  
9       rity of personal electronic records; and

10          (C) protect against unauthorized access to  
11       use of personal electronic records that could re-  
12       sult in substantial harm or inconvenience to any  
13       individual.

14          (3) RISK ASSESSMENT.—A business entity  
15       shall—

16          (A) identify reasonably foreseeable internal  
17       and external vulnerabilities that could result in  
18       unauthorized access, disclosure, use, or alter-  
19       ation of sensitive personally identifiable infor-  
20       mation or systems containing sensitive person-  
21       ally identifiable information;

22          (B) assess the likelihood of and potential  
23       damage from unauthorized access, disclosure,  
24       use, or alteration of sensitive personally identifi-  
25       able information; and

1 (C) assess the sufficiency of its policies,  
2 technologies, and safeguards in place to control  
3 and minimize risks from unauthorized access,  
4 disclosure, use, or alteration of sensitive person-  
5 ally identifiable information.

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

8 (A) design its personal data privacy and  
9 security program to control the risks identified  
10 under paragraph (3); and

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

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

20 (ii) detect actual and attempted  
21 fraudulent, unlawful, or unauthorized ac-  
22 cess, disclosure, use, or alteration of sen-  
23 sitive personally identifiable information,  
24 including by employees and other individ-

1 uals otherwise authorized to have access;  
2 and

3 (iii) protect sensitive personally identi-  
4 fiable information during use, trans-  
5 mission, storage, and disposal by  
6 encryption or other reasonable means (in-  
7 cluding as directed for disposal of records  
8 under section 628 of the Fair Credit Re-  
9 porting Act (15 U.S.C. 1681w) and the  
10 implementing regulations of such Act as  
11 set forth in section 682 of title 16, Code  
12 of Federal Regulations).

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

17 (c) VULNERABILITY TESTING.—

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

24 (2) FREQUENCY.—The frequency and nature of  
25 the tests required under paragraph (1) shall be de-

1       terminated by the risk assessment of the business enti-  
2       ty under subsection (a)(3).

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

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

15          (2) require those service providers by contract  
16      to implement and maintain appropriate measures de-  
17      signed to meet the objectives and requirements gov-  
18      erning entities subject to this section, section 401,  
19      and subtitle B.

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

- 1 (1) technology;
- 2 (2) the sensitivity of personally identifiable in-  
3 formation;
- 4 (3) internal or external threats to personally  
5 identifiable information; and
- 6 (4) the changing business arrangements of the  
7 business entity, such as—
  - 8 (A) mergers and acquisitions;
  - 9 (B) alliances and joint ventures;
  - 10 (C) outsourcing arrangements;
  - 11 (D) bankruptcy; and
  - 12 (E) changes to sensitive personally identifi-  
13 able information systems.

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

19 **SEC. 403. ENFORCEMENT.**

20 (a) CIVIL PENALTIES.—

21 (1) IN GENERAL.—Any business entity that vio-  
22 lates the provisions of sections 401 or 402 shall be  
23 subject to civil penalties of not more than \$5,000  
24 per violation per day, with a maximum of \$35,000  
25 per day, while such violations persist.

1           (2) INTENTIONAL OR WILLFUL VIOLATION.—A  
2 business entity that intentionally or willfully violates  
3 the provisions of sections 401 or 402 shall be subject  
4 to additional penalties in the amount of \$5,000 per  
5 violation per day, with a maximum of an additional  
6 \$35,000 per day, while such violations persist.

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

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

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

17           (1) IN GENERAL.—Whenever it appears that a  
18 business entity or agency to which this subtitle ap-  
19 plies has engaged, is engaged, or is about to engage,  
20 in any act or practice constituting a violation of this  
21 subtitle, the Attorney General may bring a civil ac-  
22 tion in an appropriate district court of the United  
23 States to—

24                   (A) enjoin such act or practice;

1 (B) enforce compliance with this subtitle;

2 and

3 (C) obtain damages—

4 (i) in the sum of actual damages, res-  
5 titution, and other compensation on behalf  
6 of the affected residents of a State; and

7 (ii) punitive damages, if the violation  
8 is willful or intentional; and

9 (D) obtain such other relief as the court  
10 determines to be appropriate.

11 (2) OTHER INJUNCTIVE RELIEF.—Upon a  
12 proper showing in the action under paragraph (1),  
13 the court shall grant a permanent injunction or a  
14 temporary restraining order without bond.

15 (c) STATE ENFORCEMENT.—

16 (1) CIVIL ACTIONS.—In any case in which the  
17 attorney general of a State has reason to believe  
18 that an interest of the residents of that State has  
19 been or is threatened or adversely affected by an act  
20 or practice that violates this subtitle, the State may  
21 bring a civil action on behalf of the residents of that  
22 State in a district court of the United States of ap-  
23 propriate jurisdiction, or any other court of com-  
24 petent jurisdiction, to—

25 (A) enjoin that act or practice;

1 (B) enforce compliance with this subtitle;

2 (C) obtain—

3 (i) damages in the sum of actual dam-  
4 ages, restitution, or other compensation on  
5 behalf of affected residents of the State;  
6 and

7 (ii) punitive damages, if the violation  
8 is willful or intentional; or

9 (D) obtain such other legal and equitable  
10 relief as the court may consider to be appro-  
11 priate.

12 (2) NOTICE.—

13 (A) IN GENERAL.—Before filing an action  
14 under this subsection, the attorney general of  
15 the State involved shall provide to the Attorney  
16 General—

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

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

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

1 notice described in this subparagraph before the  
2 filing of the action.

3 (C) NOTIFICATION WHEN PRACTICABLE.—

4 In an action described under subparagraph (B),  
5 the attorney general of a State shall provide the  
6 written notice and the copy of the complaint to  
7 the Attorney General as soon after the filing of  
8 the complaint as practicable.

9 (3) ATTORNEY GENERAL AUTHORITY.—Upon  
10 receiving notice under paragraph (2), the Attorney  
11 General shall have the right to—

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

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

17 (C) file petitions for appeal.

18 (4) PENDING PROCEEDINGS.—If the Attorney  
19 General has instituted a proceeding or action for a  
20 violation of this title or any regulations thereunder,  
21 no attorney general of a State may, during the pend-  
22 ency of such proceeding or action, bring an action  
23 under this subsection against any defendant named  
24 in such criminal proceeding or civil action for any  
25 violation that is alleged in that proceeding or action.

1           (5) RULE OF CONSTRUCTION.—For purposes of  
2 bringing any civil action under paragraph (1) noth-  
3 ing in this title shall be construed to prevent an at-  
4 torney general of a State from exercising the powers  
5 conferred on the attorney general by the laws of that  
6 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 1931 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 title establishes a private cause of action against a

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

3 **SEC. 404. RELATION TO STATE LAWS.**

4 (a) IN GENERAL.—No State may—

5 (1) require an entity described in section 401(c)  
6 to comply with this subtitle or any regulation pro-  
7 mulgated thereunder; and

8 (2) require an entity in compliance with the  
9 safe harbor established under section 401(d), to  
10 comply with any other provision of this subtitle.

11 (b) EFFECT OF SUBTITLE A.—Except as provided in  
12 subsection (a), this subtitle does not annul, alter, affect,  
13 or exempt any person subject to the provisions of this sub-  
14 title from complying with the laws of any State with re-  
15 spect to security programs for sensitive personally identifi-  
16 able information, except to the extent that those laws are  
17 inconsistent with any provisions of this subtitle, and then  
18 only to the extent of such inconsistency.

19 **Subtitle B—Security Breach**  
20 **Notification**

21 **SEC. 421. NOTICE TO INDIVIDUALS.**

22 (a) IN GENERAL.—Any agency, or business entity en-  
23 gaged in interstate commerce, that uses, accesses, trans-  
24 mits, stores, disposes of or collects sensitive personally  
25 identifiable information shall, following the discovery of a

1 security breach maintained by the agency or business enti-  
2 ty that contains such information, notify any resident of  
3 the United States whose sensitive personally identifiable  
4 information was subject to the security breach.

5 (b) OBLIGATION OF OWNER OR LICENSEE.—

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

14 (2) NOTICE BY OWNER, LICENSEE OR OTHER  
15 DESIGNATED THIRD PARTY.—Noting in this subtitle  
16 shall prevent or abrogate an agreement between an  
17 agency or business entity required to give notice  
18 under this section and a designated third party, in-  
19 cluding an owner or licensee of the sensitive person-  
20 ally identifiable information subject to the security  
21 breach, to provide the notifications required under  
22 subsection (a).

23 (3) BUSINESS ENTITY RELIEVED FROM GIVING  
24 NOTICE.—A business entity obligated to give notice  
25 under subsection (a) shall be relieved of such obliga-

1       tion if an owner or licensee of the sensitive person-  
2       ally identifiable information subject to the security  
3       breach, or other designated third party, provides  
4       such notification.

5       (c) TIMELINESS OF NOTIFICATION.—

6           (1) IN GENERAL.—All notifications required  
7       under this section shall be made without unreason-  
8       able delay following—

9           (A) the discovery by the agency or business  
10       entity of a security breach; and

11          (B) any measures necessary to determine  
12       the scope of the breach, prevent further disclo-  
13       sures, and restore the reasonable integrity of  
14       the data system.

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

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

23          (1) IN GENERAL.—If a law enforcement agency  
24       determines that the notification required under this  
25       section would impede a criminal investigation, such

1 notification may be delayed upon the written request  
2 of the law enforcement agency.

3 (2) EXTENDED DELAY OF NOTIFICATION.—If  
4 the notification required under subsection (a) is de-  
5 layed pursuant to paragraph (1), an agency or busi-  
6 ness entity shall give notice 30 days after the day  
7 such law enforcement delay was invoked unless a law  
8 enforcement agency provides written notification  
9 that further delay is necessary.

10 **SEC. 422. EXEMPTIONS.**

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

13 (1) IN GENERAL.—Section 421 shall not apply  
14 to an agency if the head of the agency certifies, in  
15 writing, that notification of the security breach as  
16 required by section 421 reasonably could be expected  
17 to—

18 (A) cause damage to the national security;

19 or

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

23 (2) LIMITS ON CERTIFICATIONS.—The head of  
24 an agency may not execute a certification under  
25 paragraph (1) to—

1 (A) conceal violations of law, inefficiency,  
2 or administrative error;

3 (B) prevent embarrassment to a business  
4 entity, organization, or agency; or

5 (C) restrain competition.

6 (3) NOTICE.—In every case in which a head of  
7 an agency issues a certification under paragraph (1),  
8 the certification, accompanied by a concise descrip-  
9 tion of the factual basis for the certification, shall be  
10 immediately provided to the Congress.

11 (b) RISK ASSESSMENT EXEMPTION.—An agency or  
12 business entity will be exempt from the notice require-  
13 ments under section 421, if—

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

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

24 (A) the results of the risk assessment;

1 (B) its decision to invoke the risk assess-  
2 ment exemption; and

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

6 (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

7 (1) IN GENERAL.—A business entity will be ex-  
8 empt from the notice requirement under section 421  
9 if the business entity utilizes or participates in a se-  
10 curity program that—

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

16 (B) provides for notice after a security  
17 breach that has resulted in fraud or unauthor-  
18 ized transactions.

19 (2) LIMITATION.—The exemption by this sub-  
20 section does not apply if the information subject to  
21 the security breach includes, in addition to an ac-  
22 count number, sensitive personally identifiable infor-  
23 mation.

1 **SEC. 423. METHODS OF NOTICE.**

2 An agency, or business entity shall be in compliance  
3 with section 421 if it provides:

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; or

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

14 (2) MEDIA NOTICE.—If more than 5,000 resi-  
15 dents of a State or jurisdiction are impacted, notice  
16 to major media outlets serving that State or jurisdic-  
17 tion.

18 **SEC. 424. CONTENT OF NOTIFICATION.**

19 (a) IN GENERAL.—Regardless of the method by  
20 which notice is provided to individuals under section 423,  
21 such notice shall include, to the extent possible—

22 (1) a description of the categories of sensitive  
23 personally identifiable information that was, or is  
24 reasonably believed to have been, acquired by an un-  
25 authorized person;

26 (2) a toll-free number—

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

4 (B) from which the individual may learn—

5 (i) what types of sensitive personally  
6 identifiable information the agency or busi-  
7 ness entity maintained about that indi-  
8 vidual or about individuals in general; and

9 (ii) whether or not the agency or busi-  
10 ness entity maintained sensitive personally  
11 identifiable information about that indi-  
12 vidual; and

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

15 (b) **ADDITIONAL CONTENT.**—Notwithstanding sec-  
16 tion 429, a State may require that a notice under sub-  
17 section (a) shall also include information regarding victim  
18 protection assistance provided for by that State.

19 **SEC. 425. COORDINATION OF NOTIFICATION WITH CREDIT**  
20 **REPORTING AGENCIES.**

21 If an agency or business entity is required to provide  
22 notification to more than 1,000 individuals under section  
23 421(a), the agency or business entity shall also notify,  
24 without unreasonable delay, all consumer reporting agen-  
25 cies that compile and maintain files on consumers on a

1 nationwide basis (as defined in section 603(p) of the Fair  
2 Credit Reporting Act (15 U.S.C. 1681a(p)) of the timing  
3 and distribution of the notices.

4 **SEC. 426. NOTICE TO LAW ENFORCEMENT.**

5 (a) SECRET SERVICE.—Any business entity or agen-  
6 cy required to give notice under section 421 shall also give  
7 notice to the United States Secret Service if the security  
8 breach impacts—

9 (1) more than 10,000 individuals nationwide;

10 (2) a database, networked or integrated data-  
11 bases, or other data system associated with the sen-  
12 sitive personally identifiable information on more  
13 than 1,000,000 individuals nationwide;

14 (3) databases owned by the Federal Govern-  
15 ment; or

16 (4) primarily sensitive personally identifiable in-  
17 formation of employees and contractors of the Fed-  
18 eral Government involved in national security or law  
19 enforcement.

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

23 (1)(A) the Federal Bureau of Investigation, if  
24 the security breach involves espionage, foreign coun-  
25 terintelligence, information protected against unau-

1       thorized disclosure for reasons of national defense or  
2       foreign relations, or Restricted Data (as that term  
3       is defined in section 11y of the Atomic Energy Act  
4       of 1954 (42 U.S.C. 2014(y)), except for offenses af-  
5       fecting the duties of the United States Secret Serv-  
6       ice under section 3056(a) of title 18, United States  
7       Code; and

8               (B) the United States Postal Inspection Serv-  
9       ice, if the security breach involves mail fraud; and

10              (2) the attorney general of each State affected  
11       by the security breach.

12       (c) 30-DAY RULE.—The notices to Federal law en-  
13       forcement and the attorney general of each State affected  
14       by a security breach required under this section shall be  
15       delivered without unreasonable delay, but not later than  
16       30 days after discovery of the events requiring notice.

17       **SEC. 427. CIVIL REMEDIES.**

18       (a) PENALTIES.—Any agency, or business entity en-  
19       gaged in interstate commerce, that violates this subtitle  
20       shall be subject to a fine of—

21              (1) not more than \$1,000 per individual per  
22       day whose sensitive personally identity information  
23       was, or is reasonably believed to have been, acquired  
24       by an unauthorized person; or

1           (2) not more than \$50,000 per day while the  
2 failure to give notice under this subtitle persists.

3           (b) **EQUITABLE RELIEF.**—Any agency or business  
4 entity that violates, proposes to violate, or has violated this  
5 subtitle may be enjoined from further violations by a court  
6 of competent jurisdiction.

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

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

17          (e) **INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-**  
18 **ERAL.**—Whenever it appears that a business entity or  
19 agency to which this subtitle applies has engaged, is en-  
20 gaged, or is about to engage, in any act or practice consti-  
21 tuting a violation of this subtitle, the Attorney General  
22 may bring a civil action in an appropriate district court  
23 of the United States to—

24           (1) enjoin such act or practice;

25           (2) enforce compliance with this subtitle;

1 (3) obtain damages—

2 (A) in the sum of actual damages, restitu-  
3 tion, and other compensation on behalf of the  
4 affected residents of a State; and

5 (B) punitive damages, if the violation is  
6 willful or intentional; and

7 (4) obtain such other relief as the court deter-  
8 mines to be appropriate.

9 **SEC. 428. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

10 (a) IN GENERAL.—

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 engage-  
18 ment of any agency or business entity in a practice  
19 that is prohibited under this subtitle, the State, as  
20 *parens patriae* on behalf of the residents of the  
21 State, or the State or local law enforcement agency  
22 on behalf of the residents of the agency's jurisdic-  
23 tion, may bring a civil action on behalf of the resi-  
24 dents of the State or jurisdiction in a district court  
25 of the United States of appropriate jurisdiction or

1 any other court of competent jurisdiction, including  
2 a State court, to—

3 (A) enjoin that practice;

4 (B) enforce compliance with this subtitle;

5 (C) obtain damages, restitution, or other  
6 compensation on behalf of residents of the  
7 State; or

8 (D) obtain such other relief as the court  
9 may consider to be appropriate.

10 (2) NOTICE.—

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

15 (i) written notice of the action; and

16 (ii) a copy of the complaint for the ac-  
17 tion.

18 (B) EXEMPTION.—

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

1                   (ii) NOTIFICATION.—In an action de-  
2                   scribed in clause (i), the attorney general  
3                   of a State shall provide notice and a copy  
4                   of the complaint to the Attorney General  
5                   at the time the State attorney general files  
6                   the action.

7           (b) FEDERAL PROCEEDINGS.—Upon receiving notice  
8           under subsection (a)(2), the Attorney General shall have  
9           the right to—

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

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

15                   (3) 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 data  
25 broker for violation of any provision of this subtitle.

1 **SEC. 429. EFFECT ON FEDERAL AND STATE LAW.**

2 The provisions of this subtitle shall supersede any  
3 other provision of Federal law or any provision of law of  
4 any State relating to notification of a security breach, ex-  
5 cept as provided in section 424(b).

6 **SEC. 430. AUTHORIZATION OF APPROPRIATIONS.**

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

12 **SEC. 431. REPORTING ON RISK ASSESSMENT EXEMPTION.**

13 The United States Secret Service shall report to Con-  
14 gress not later than 18 months after the date of enactment  
15 of this Act, and upon the request by Congress thereafter,  
16 on the number and nature of the security breaches de-  
17 scribed in the notices filed by those business entities invok-  
18 ing the risk assessment exemption under section 422(b)  
19 and the response of the United States Secret Service to  
20 those notices.

21 **SEC. 432. EFFECTIVE DATE.**

22 This subtitle shall take effect on the expiration of the  
23 date which is 90 days after the date of enactment of this  
24 Act.

1 **TITLE V—GOVERNMENT ACCESS**  
2 **TO AND USE OF COMMERCIAL**  
3 **DATA**

4 **SEC. 501. GENERAL SERVICES ADMINISTRATION REVIEW**  
5 **OF CONTRACTS.**

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

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

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

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

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

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

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

17                (1) include monetary or other penalties—

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

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

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

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

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

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

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

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

20      **SEC. 502. REQUIREMENT TO AUDIT INFORMATION SECU-**  
21                      **RITY PRACTICES OF CONTRACTORS AND**  
22                      **THIRD PARTY BUSINESS ENTITIES.**

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

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

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

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

6 “(9) procedures for evaluating and auditing the  
7 information security practices of contractors or third  
8 party business entities supporting the information  
9 systems or operations of the agency involving per-  
10 sonally identifiable information (as that term is de-  
11 fined in section 3 of the Personal Data Privacy and  
12 Security Act of 2005) and ensuring remedial action  
13 to address any significant deficiencies.”.

14 **SEC. 503. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT**  
15 **USE OF COMMERCIAL INFORMATION SERV-**  
16 **ICES CONTAINING PERSONALLY IDENTIFI-**  
17 **ABLE INFORMATION.**

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

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

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

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

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

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

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

19                           (A) such database;

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

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

23           (2) adopts regulations that specify—

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

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

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

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

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

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

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

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

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

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

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

6 (A) providing for penalties—

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

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

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

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

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

1           sonally identifiable information at issue;  
2           and

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

7           (c) LIMITATION ON PENALTIES.—The penalties  
8           under paragraph (3)(A) shall not apply to a data broker  
9           providing information that is accurately and completely re-  
10          corded from a public record source.

11          (d) INDIVIDUAL SCREENING PROGRAMS.—

12                   (1) IN GENERAL.—Notwithstanding any other  
13           provision of law, commencing one year after the date  
14           of enactment of this Act, no Federal department or  
15           agency may use commercial databases or contract  
16           with a data broker to implement an individual  
17           screening program unless such program is—

18                           (A) congressionally authorized; and

19                           (B) subject to regulations developed by no-  
20           tice and comment that—

21                                   (i) establish a procedure to enable in-  
22           dividuals, who suffer an adverse con-  
23           sequence because the screening system de-  
24           termined that they might pose a security  
25           threat, to appeal such determination and

1 correct information contained in the sys-  
2 tem;

3 (ii) ensure that Federal and commer-  
4 cial databases that will be used to establish  
5 the identity of individuals or otherwise  
6 make assessments of individuals under the  
7 system will not produce a large number of  
8 false positives or unjustified adverse con-  
9 sequences;

10 (iii) ensure the efficacy and accuracy  
11 of all of the search tools that will be used  
12 and ensure that the department or agency  
13 can make an accurate predictive assess-  
14 ment of those who may constitute a threat;

15 (iv) establish an internal oversight  
16 board to oversee and monitor the manner  
17 in which the system is being implemented;

18 (v) establish sufficient operational  
19 safeguards to reduce the opportunities for  
20 abuse;

21 (vi) implement substantial security  
22 measures to protect the system from unau-  
23 thorized access;

1 (vii) adopt policies establishing the ef-  
2 fective oversight of the use and operation  
3 of the system; and

4 (viii) ensure that there are no specific  
5 privacy concerns with the technological ar-  
6 chitecture of the system; and

7 (C) coordinated with the Terrorist Screen-  
8 ing Center or any such successor organization.

9 (2) DEFINITION.—As used in this subsection,  
10 the term “individual screening program”—

11 (A) means a system that relies on person-  
12 ally identifiable information from commercial  
13 databases to—

14 (i) evaluate all or most individuals  
15 seeking to exercise a particular right or  
16 privilege under Federal law; and

17 (ii) determine whether such individ-  
18 uals are on a terrorist watch list or other-  
19 wise pose a security threat; and

20 (B) does not include any program or sys-  
21 tem to grant security clearances.

22 (e) STUDY OF GOVERNMENT USE.—

23 (1) SCOPE OF STUDY.—Not later than 180  
24 days after the date of enactment of this Act, the  
25 Comptroller General of the United States shall con-

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

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

11 **SEC. 504. IMPLEMENTATION OF CHIEF PRIVACY OFFICER**  
12 **REQUIREMENTS.**

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

24       (b) DUTIES AND RESPONSIBILITIES OF CHIEF PRI-  
25 VACY OFFICER.—In addition to the duties and responsibil-

1 ities outlined under section 522 of the Transportation,  
2 Treasury, Independent Agencies, and General Government  
3 Appropriations Act, 2005 (division H of Public Law 108–  
4 447; 118 Stat. 3199), the Department of Justice Chief  
5 Privacy Officer shall—

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

11          (2) promote the use of law enforcement tech-  
12          nologies that sustain privacy protections, and assure  
13          that the implementation of such technologies relat-  
14          ing to the use, collection, and disclosure of person-  
15          ally identifiable information preserve the privacy and  
16          security of such information; and

17          (3) coordinate with the Privacy and Civil Lib-  
18          erties Oversight Board, established in the Intel-  
19          ligence Reform and Terrorism Prevention Act of  
20          2004 (Public Law 108–458), in implementing para-  
21          graphs (1) and (2) of this subsection.

○