

112TH CONGRESS  
1ST SESSION

# S. 1151

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

JUNE 7, 2011

Mr. LEAHY (for himself, Mr. SCHUMER, Mr. CARDIN, and Mr. FRANKEN) 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 2011”.

6 (b) TABLE OF CONTENTS.—The table of contents of  
7 this Act is as follows:

- Sec. 1. Short title; table of contents.
- Sec. 2. Findings.
- Sec. 3. Definitions.

TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND  
OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY

- Sec. 101. Organized criminal activity in connection with unauthorized access to personally identifiable information.
- Sec. 102. Concealment of security breaches involving sensitive personally identifiable information.
- Sec. 103. Penalties for fraud and related activity in connection with computers.

TITLE II—DATA BROKERS

- Sec. 201. Transparency and accuracy of data collection.
- Sec. 202. Enforcement.
- Sec. 203. Relation to State laws.
- Sec. 204. Effective date.

TITLE III—PRIVACY AND SECURITY OF PERSONALLY  
IDENTIFIABLE INFORMATION

Subtitle A—A Data Privacy and Security Program

- Sec. 301. Purpose and applicability of data privacy and security program.
- Sec. 302. Requirements for a personal data privacy and security program.
- Sec. 303. Enforcement.
- Sec. 304. Relation to other laws.

Subtitle B—Security Breach Notification

- Sec. 311. Notice to individuals.
- Sec. 312. Exemptions.
- Sec. 313. Methods of notice.
- Sec. 314. Content of notification.
- Sec. 315. Coordination of notification with credit reporting agencies.
- Sec. 316. Notice to law enforcement.
- Sec. 317. Enforcement.
- Sec. 318. Enforcement by State attorneys general.
- Sec. 319. Effect on Federal and State law.
- Sec. 320. Authorization of appropriations.
- Sec. 321. Reporting on risk assessment exemptions.
- Sec. 322. Effective date.

TITLE IV—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL  
DATA

- Sec. 401. General services administration review of contracts.
- Sec. 402. Requirement to audit information security practices of contractors and third party business entities.
- Sec. 403. Privacy impact assessment of government use of commercial information services containing personally identifiable information.

TITLE V—COMPLIANCE WITH STATUTORY PAY-AS-YOU-GO ACT

- Sec. 501. Budget compliance.

1 **SEC. 2. FINDINGS.**

2 Congress finds that—

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

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

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

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

17 (5) it is important for business entities that  
18 own, use, or license personally identifiable informa-  
19 tion to adopt reasonable procedures to ensure the se-  
20 curity, privacy, and confidentiality of that personally  
21 identifiable information;

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

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

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

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

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

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

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

1 **SEC. 3. DEFINITIONS.**

2 In this Act, the following definitions shall apply:

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

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

9 (3) BUSINESS ENTITY.—The term “business  
10 entity” means any organization, corporation, trust,  
11 partnership, sole proprietorship, unincorporated as-  
12 sociation, or venture established to make a profit, or  
13 nonprofit.

14 (4) IDENTITY THEFT.—The term “identity  
15 theft” means a violation of section 1028(a)(7) of  
16 title 18, United States Code.

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

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

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

7           (A) means the protection of data in elec-  
8 tronic form, in storage or in transit, using an  
9 encryption technology that has been adopted by  
10 a widely accepted standards setting body or,  
11 has been widely accepted as an effective indus-  
12 try practice which renders such data indecipher-  
13 able in the absence of associated cryptographic  
14 keys necessary to enable decryption of such  
15 data; and

16           (B) includes appropriate management and  
17 safeguards of such cryptographic keys so as to  
18 protect the integrity of the encryption.

19           (8) PERSONAL ELECTRONIC RECORD.—

20           (A) IN GENERAL.—The term “personal  
21 electronic record” means data associated with  
22 an individual contained in a database,  
23 networked or integrated databases, or other  
24 data system that is provided by a data broker  
25 to nonaffiliated third parties and includes per-

1           sonally identifiable information about that indi-  
2           vidual.

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

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

7                   (ii) any proprietary assessment or  
8                   evaluation of an individual or any propri-  
9                   etary assessment or evaluation of informa-  
10                  tion about an individual.

11           (9) PERSONALLY IDENTIFIABLE INFORMA-  
12           TION.—The term “personally identifiable informa-  
13           tion” means any information, or compilation of in-  
14           formation, in electronic or digital form that is a  
15           means of identification, as defined by section  
16           1028(d)(7) of title 18, United State Code.

17           (10) PUBLIC RECORD SOURCE.—The term  
18           “public record source” means the Congress, any  
19           agency, any State or local government agency, the  
20           government of the District of Columbia and govern-  
21           ments of the territories or possessions of the United  
22           States, and Federal, State or local courts, courts  
23           martial and military commissions, that maintain  
24           personally identifiable information in records avail-  
25           able to the public.

1 (11) SECURITY BREACH.—

2 (A) IN GENERAL.—The term “security  
3 breach” means compromise of the security, con-  
4 fidentiality, or integrity of computerized data  
5 through misrepresentation or actions—

6 (i) that result in, or that there is a  
7 reasonable basis to conclude has resulted  
8 in—

9 (I) the unauthorized acquisition  
10 of sensitive personally identifiable in-  
11 formation; and

12 (II) access to sensitive personally  
13 identifiable information that is for an  
14 unauthorized purpose, or in excess of  
15 authorization; and

16 (ii) which present a significant risk of  
17 harm or fraud to any individual.

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

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



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

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

6                   (iii) any lawfully authorized investiga-  
7                   tive, protective, or intelligence activity of a  
8                   law enforcement or intelligence agency of  
9                   the United States.

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

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

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

21                   (ii) Any 2 of the following:

22                   (I) Home address or telephone  
23                   number.

24                   (II) Mother’s maiden name.

1 (III) Month, day, and year of  
2 birth.

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

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

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

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

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

9 Section 1961(1) of title 18, United States Code, is  
10 amended by inserting “section 1030 (relating to fraud and  
11 related activity in connection with computers) if the act  
12 is a felony,” before “section 1084”.

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

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

19 **“§ 1041. Concealment of security breaches involving**  
20 **sensitive personally identifiable informa-**  
21 **tion**

22 “(a) Whoever, having knowledge of a security breach  
23 and having the obligation to provide notice of such breach  
24 to individuals under title III of the Personal Data Privacy  
25 and Security Act of 2011, and having not otherwise quali-

1 fined for an exemption from providing notice under section  
 2 312 of such Act, intentionally and willfully conceals the  
 3 fact of such security breach and which breach causes eco-  
 4 nomic damage to 1 or more persons, shall be fined under  
 5 this title or imprisoned not more than 5 years, or both.

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

9 “(c) Any person seeking an exemption under section  
 10 312(b) of the Personal Data Privacy and Security Act of  
 11 2011 shall be immune from prosecution under this section  
 12 if the United States Secret Service does not indicate, in  
 13 writing, that such notice be given under section 312(b)(3)  
 14 of such Act.”.

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

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

19 (c) ENFORCEMENT AUTHORITY.—

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



1 (ii) by striking “in the case of—” and  
2 all that follows through “an offense under  
3 subsection (a)(5)(B)” and inserting “in the  
4 case of an offense, or an attempt or con-  
5 spiracy to commit an offense, under sub-  
6 section (a)(5)(B)”;

7 (iii) by inserting “or conspiracy” after  
8 “if the offense”;

9 (iv) by redesignating subclauses (I)  
10 through (VI) as clauses (i) through (vi),  
11 respectively, and adjusting the margin ac-  
12 cordingly; and

13 (v) in clause (vi), as so redesignated,  
14 by striking “; or” and inserting a semi-  
15 colon;

16 (B) in subparagraph (B)—

17 (i) by striking clause (ii);

18 (ii) by striking “in the case of—” and  
19 all that follows through “an offense under  
20 subsection (a)(5)(A)” and inserting “in the  
21 case of an offense, or an attempt or con-  
22 spiracy to commit an offense, under sub-  
23 section (a)(5)(A)”;

24 (iii) by inserting “or conspiracy” after  
25 “if the offense”; and

1 (iv) by striking “; or” and inserting a  
2 semicolon;

3 (C) in subparagraph (C)—

4 (i) by striking clause (ii);

5 (ii) by striking “in the case of—” and  
6 all that follows through “an offense or an  
7 attempt to commit an offense” and insert-  
8 ing “in the case of an offense, or an at-  
9 tempt or conspiracy to commit an of-  
10 fense,”; and

11 (iii) by striking “; or” and inserting a  
12 semicolon;

13 (D) in subparagraph (D)—

14 (i) by striking clause (ii);

15 (ii) by striking “in the case of—” and  
16 all that follows through “an offense or an  
17 attempt to commit an offense” and insert-  
18 ing “in the case of an offense, or an at-  
19 tempt or conspiracy to commit an of-  
20 fense,”; and

21 (iii) by striking “; or” and inserting a  
22 semicolon;

23 (E) in subparagraph (E), by inserting “or  
24 conspires” after “offender attempts”;

1 (F) in subparagraph (F), by inserting “or  
2 conspires” after “offender attempts”; and

3 (G) in subparagraph (G)(ii), by inserting  
4 “or conspiracy” after “an attempt”.

## 5 **TITLE II—DATA BROKERS**

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

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

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

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

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

24 (3) any data broker currently subject to and in  
25 compliance with the data security requirements for



1 such entities under the Health Insurance Portability  
2 and Accountability Act (Public Law 104–191), and  
3 its implementing regulations;

4 (4) any data broker subject to, and in compli-  
5 ance with, the privacy and data security require-  
6 ments under sections 13401 and 13404 of division  
7 A of the American Reinvestment and Recovery Act  
8 of 2009 (42 U.S.C. 17931 and 17934) and imple-  
9 menting regulations promulgated under such sec-  
10 tions;

11 (5) information in a personal electronic record  
12 that—

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

18 (B) is not maintained primarily for the  
19 purpose of transmitting or otherwise providing  
20 that information, or assessments based on that  
21 information, to nonaffiliated third parties;

22 (6) information concerning proprietary meth-  
23 odologies, techniques, scores, or algorithms relating  
24 to fraud prevention not normally provided to third  
25 parties in the ordinary course of business; and

1 (7) information that is used for legitimate gov-  
2 ernmental or fraud prevention purposes that would  
3 be compromised by disclosure to the individual.

4 (c) DISCLOSURES TO INDIVIDUALS.—

5 (1) IN GENERAL.—A data broker shall, upon  
6 the request of an individual, disclose to such indi-  
7 vidual for a reasonable fee all personal electronic  
8 records pertaining to that individual maintained or  
9 accessed by the data broker specifically for disclo-  
10 sure to third parties that request information on  
11 that individual in the ordinary course of business in  
12 the databases or systems of the data broker at the  
13 time of such request.

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

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

20 (1) IN GENERAL.—If a person takes any ad-  
21 verse action with respect to any individual that is  
22 based, in whole or in part, on any information con-  
23 tained in a personal electronic record, the person, at  
24 no cost to the affected individual, shall provide—

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

3 (B) to the individual, in writing or elec-  
4 tronically, the name, address, and telephone  
5 number of the data broker (including a toll-free  
6 telephone number established by the data  
7 broker, if the data broker complies and main-  
8 tains data on individuals on a nationwide basis)  
9 that furnished the information to the person;

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

12 (D) information to the individual on the  
13 procedures for correcting any inaccuracies in  
14 such information.

15 (2) ACCEPTED METHODS OF NOTICE.—A per-  
16 son shall be in compliance with the notice require-  
17 ments under paragraph (1) if such person provides  
18 written or electronic notice in the same manner and  
19 using the same methods as are required under sec-  
20 tion 313(1) of this Act.

21 (e) ACCURACY RESOLUTION PROCESS.—

22 (1) INFORMATION FROM A PUBLIC RECORD OR  
23 LICENSOR.—

24 (A) IN GENERAL.—If an individual notifies  
25 a data broker of a dispute as to the complete-

1           ness or accuracy of information disclosed to  
2           such individual under subsection (c) that is ob-  
3           tained from a public record source or a license  
4           agreement, such data broker shall determine  
5           within 30 days whether the information in its  
6           system accurately and completely records the  
7           information available from the licensor or public  
8           record source.

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

15               (i) correct any inaccuracies or incom-  
16               pleteness, and provide to such individual  
17               written notice of such changes; and

18               (ii) provide such individual with the  
19               contact information of the public record or  
20               licensor.

21          (2) INFORMATION NOT FROM A PUBLIC RECORD  
22          SOURCE OR LICENSOR.—If an individual notifies a  
23          data broker of a dispute as to the completeness or  
24          accuracy of information not from a public record or  
25          licensor that was disclosed to the individual under

1 subsection (c), the data broker shall, within 30 days  
2 of receiving notice of such dispute—

3 (A) review and consider free of charge any  
4 information submitted by such individual that is  
5 relevant to the completeness or accuracy of the  
6 disputed information; and

7 (B) correct any information found to be in-  
8 complete or inaccurate and provide notice to  
9 such individual of whether and what informa-  
10 tion was corrected, if any.

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

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

1           (5) DETERMINATION THAT DISPUTE IS FRIVO-  
2 LOUS OR IRRELEVANT.—

3           (A) IN GENERAL.—Notwithstanding para-  
4 graphs (1) through (3), a data broker may de-  
5 cline to investigate or terminate a review of in-  
6 formation disputed by an individual under those  
7 paragraphs if the data broker reasonably deter-  
8 mines that the dispute by the individual is friv-  
9 ous or intended to perpetrate fraud.

10           (B) NOTICE.—A data broker shall notify  
11 an individual of a determination under subpara-  
12 graph (A) within a reasonable time by any  
13 means available to such data broker.

14 **SEC. 202. ENFORCEMENT.**

15           (a) CIVIL PENALTIES.—

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

21           (2) INTENTIONAL OR WILLFUL VIOLATION.—A  
22 data broker that intentionally or willfully violates the  
23 provisions of section 201 shall be subject to addi-  
24 tional penalties in the amount of \$1,000 per viola-

1       tion per day, to a maximum of an additional  
2       \$250,000 per violation, while such violations persist.

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

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

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

14      (c) **STATE ENFORCEMENT.**—

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

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

3 (A) enjoin that act or practice;

4 (B) enforce compliance with this title; or

5 (C) obtain civil penalties of not more than  
6 \$1,000 per violation per day while such viola-  
7 tions persist, up to a maximum of \$250,000 per  
8 violation.

9 (2) NOTICE.—

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

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

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

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

24 (C) NOTIFICATION WHEN PRACTICABLE.—

25 In an action described under subparagraph (B),



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

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

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

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

14                  (C) file petitions for appeal.

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

23           (5) RULE OF CONSTRUCTION.—For purposes of  
24           bringing any civil action under paragraph (1), noth-  
25           ing in this title shall be construed to prevent an at-

1       torney general of a State from exercising the powers  
2       conferred on the attorney general by the laws of that  
3       State to—

4               (A) conduct investigations;

5               (B) administer oaths and affirmations; or

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

9       (6) VENUE; SERVICE OF PROCESS.—

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

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

18                   (i) is an inhabitant; or

19                   (ii) may be found.

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

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

24       No requirement or prohibition may be imposed under  
25       the laws of any State with respect to any subject matter

1 regulated under section 201, relating to individual access  
2 to, and correction of, personal electronic records held by  
3 data brokers.

4 **SEC. 204. EFFECTIVE DATE.**

5 This title shall take effect 180 days after the date  
6 of enactment of this Act.

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

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

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

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

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

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

3 (1) FINANCIAL INSTITUTIONS.—Financial insti-  
4 tutions—

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

9 (B) subject to—

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

16 (ii) compliance with part 314 of title  
17 16, Code of Federal Regulations.

18 (2) HIPPA REGULATED ENTITIES.—

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

1 (B) BUSINESS ENTITIES.—A Business en-  
2 tity shall be deemed in compliance with this Act  
3 if the business entity—

4 (i) is acting as a business associate,  
5 as that term is defined under the Health  
6 Insurance Portability and Accountability  
7 Act of 1996 (42 U.S.C. 1301 et seq.) and  
8 is in compliance with the requirements im-  
9 posed under that Act and implementing  
10 regulations promulgated under that Act;  
11 and

12 (ii) is subject to, and currently in  
13 compliance, with the privacy and data se-  
14 curity requirements under sections 13401  
15 and 13404 of division A of the American  
16 Reinvestment and Recovery Act of 2009  
17 (42 U.S.C. 17931 and 17934) and imple-  
18 menting regulations promulgated under  
19 such sections.

20 (3) PUBLIC RECORDS.—Public records not oth-  
21 erwise subject to a confidentiality or nondisclosure  
22 requirement, or information obtained from a news  
23 report or periodical.

24 (d) SAFE HARBORS.—

1           (1) IN GENERAL.—A business entity shall be  
2           deemed in compliance with the privacy and security  
3           program requirements under section 302 if the busi-  
4           ness entity complies with or provides protection  
5           equal to industry standards or standards widely ac-  
6           cepted as an effective industry practice, as identified  
7           by the Federal Trade Commission, that are applica-  
8           ble to the type of sensitive personally identifiable in-  
9           formation involved in the ordinary course of business  
10          of such business entity.

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

18 **SEC. 302. REQUIREMENTS FOR A PERSONAL DATA PRIVACY**

19 **AND SECURITY PROGRAM.**

20          (a) PERSONAL DATA PRIVACY AND SECURITY PRO-  
21          GRAM.—A business entity subject to this subtitle shall  
22          comply with the following safeguards and any other ad-  
23          ministrative, technical, or physical safeguards identified by  
24          the Federal Trade Commission in a rulemaking process  
25          pursuant to section 553 of title 5, United States Code,

1 for the protection of sensitive personally identifiable infor-  
2 mation:

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

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

11 (A) ensure the privacy, security, and con-  
12 fidentiality of sensitive personally identifying in-  
13 formation;

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

18 (C) protect against unauthorized access to  
19 use of sensitive personally identifying informa-  
20 tion that could create a significant risk of harm  
21 or fraud to any individual.

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

24 (A) identify reasonably foreseeable internal  
25 and external vulnerabilities that could result in

1 unauthorized access, disclosure, use, or alter-  
2 ation of sensitive personally identifiable infor-  
3 mation or systems containing sensitive person-  
4 ally identifiable information;

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

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

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

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

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

24 (B) adopt measures commensurate with  
25 the sensitivity of the data as well as the size,



1 complexity, and scope of the activities of the  
2 business entity that—

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

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

15 (iii) protect sensitive personally identi-  
16 fiable information during use, trans-  
17 mission, storage, and disposal by  
18 encryption, redaction, or access controls  
19 that are widely accepted as an effective in-  
20 dustry practice or industry standard, or  
21 other reasonable means (including as di-  
22 rected for disposal of records under section  
23 628 of the Fair Credit Reporting Act (15  
24 U.S.C. 1681w) and the implementing regu-  
25 lations of such Act as set forth in section

1 682 of title 16, Code of Federal Regula-  
2 tions);

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

10 (v) trace access to records containing  
11 sensitive personally identifiable information  
12 so that the business entity can determine  
13 who accessed or acquired such sensitive  
14 personally identifiable information per-  
15 taining to specific individuals; and

16 (vi) ensure that no third party or cus-  
17 tomer of the business entity is authorized  
18 to access or acquire sensitive personally  
19 identifiable information without the busi-  
20 ness entity first performing sufficient due  
21 diligence to ascertain, with reasonable cer-  
22 tainty, that such information is being  
23 sought for a valid legal purpose.

24 (b) TRAINING.—Each business entity subject to this  
25 subtitle shall take steps to ensure employee training and

1 supervision for implementation of the data security pro-  
2 gram of the business entity.

3 (c) VULNERABILITY TESTING.—

4 (1) IN GENERAL.—Each business entity subject  
5 to this subtitle shall take steps to ensure regular  
6 testing of key controls, systems, and procedures of  
7 the personal data privacy and security program to  
8 detect, prevent, and respond to attacks or intrusions,  
9 or other system failures.

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

14 (d) RELATIONSHIP TO SERVICE PROVIDERS.—In the  
15 event a business entity subject to this subtitle engages  
16 service providers not subject to this subtitle, such business  
17 entity shall—

18 (1) exercise appropriate due diligence in select-  
19 ing those service providers for responsibilities related  
20 to sensitive personally identifiable information, and  
21 take reasonable steps to select and retain service  
22 providers that are capable of maintaining appro-  
23 priate safeguards for the security, privacy, and in-  
24 tegrity of the sensitive personally identifiable infor-  
25 mation at issue; and

1           (2) require those service providers by contract  
2           to implement and maintain appropriate measures de-  
3           signed to meet the objectives and requirements gov-  
4           erning entities subject to section 301, this section,  
5           and subtitle B.

6           (e) PERIODIC ASSESSMENT AND PERSONAL DATA  
7           PRIVACY AND SECURITY MODERNIZATION.—Each busi-  
8           ness entity subject to this subtitle shall on a regular basis  
9           monitor, evaluate, and adjust, as appropriate its data pri-  
10          vacy and security program in light of any relevant changes  
11          in—

12                 (1) technology;

13                 (2) the sensitivity of personally identifiable in-  
14          formation;

15                 (3) internal or external threats to personally  
16          identifiable information; and

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

19                         (A) mergers and acquisitions;

20                         (B) alliances and joint ventures;

21                         (C) outsourcing arrangements;

22                         (D) bankruptcy; and

23                         (E) changes to sensitive personally identifi-  
24          able information systems.

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

6 **SEC. 303. ENFORCEMENT.**

7 (a) CIVIL PENALTIES.—

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

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

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

23 (4) OTHER RIGHTS AND REMEDIES.—The  
24 rights and remedies available under this section are

1 cumulative and shall not affect any other rights and  
2 remedies available under law.

3 (b) FEDERAL TRADE COMMISSION AUTHORITY.—

4 Any business entity shall have the provisions of this sub-  
5 title enforced against it by the Federal Trade Commission.

6 (c) STATE ENFORCEMENT.—

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

19 (A) enjoin that act or practice;

20 (B) enforce compliance with this subtitle;

21 or

22 (C) obtain civil penalties of not more than  
23 \$5,000 per violation per day while such viola-  
24 tions persist, up to a maximum of \$500,000 per  
25 violation.

1 (2) NOTICE.—

2 (A) IN GENERAL.—Before filing an action  
3 under this subsection, the attorney general of  
4 the State involved shall provide to the Federal  
5 Trade Commission—

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

7 (ii) a copy of the complaint for that  
8 action.

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

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

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

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

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

6           (C) file petitions for appeal.

7           (4) PENDING PROCEEDINGS.—If the Federal  
8           Trade Commission has instituted a proceeding or ac-  
9           tion for a violation of this subtitle or any regulations  
10          thereunder, no attorney general of a State may, dur-  
11          ing the pendency of such proceeding or action, bring  
12          an action under this subsection against any defend-  
13          ant named in such criminal proceeding or civil ac-  
14          tion for any violation that is alleged in that pro-  
15          ceeding or action.

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

22                 (A) conduct investigations;

23                 (B) administer oaths and affirmations; or



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

4 (6) VENUE; SERVICE OF PROCESS.—

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

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

13 (i) is an inhabitant; or

14 (ii) may be found.

15 (d) NO PRIVATE CAUSE OF ACTION.—Nothing in  
16 this subtitle establishes a private cause of action against  
17 a business entity for violation of any provision of this sub-  
18 title.

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

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

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

5 **Subtitle B—Security Breach**  
6 **Notification**

7 **SEC. 311. NOTICE TO INDIVIDUALS.**

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

16 (b) OBLIGATION OF OWNER OR LICENSEE.—

17 (1) NOTICE TO OWNER OR LICENSEE.—Any  
18 agency, or business entity engaged in interstate com-  
19 merce, that uses, accesses, transmits, stores, dis-  
20 poses of, or collects sensitive personally identifiable  
21 information that the agency or business entity does  
22 not own or license shall notify the owner or licensee  
23 of the information following the discovery of a secu-  
24 rity breach involving such information.

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

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

17           (c) TIMELINESS OF NOTIFICATION.—

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

22           (2) REASONABLE DELAY.—Reasonable delay  
23           under this subsection may include any time nec-  
24           essary to determine the scope of the security breach,  
25           prevent further disclosures, conduct the risk assess-

1 ment described in section 302(a)(3), and restore the  
2 reasonable integrity of the data system and provide  
3 notice to law enforcement when required.

4 (3) BURDEN OF PRODUCTION.—The agency,  
5 business entity, owner, or licensee required to pro-  
6 vide notice under this subtitle shall, upon the re-  
7 quest of the Attorney General, provide records or  
8 other evidence of the notifications required under  
9 this subtitle, including to the extent applicable, the  
10 reasons for any delay of notification.

11 (d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW  
12 ENFORCEMENT PURPOSES.—

13 (1) IN GENERAL.—If a Federal law enforce-  
14 ment or intelligence agency determines that the noti-  
15 fication required under this section would impede a  
16 criminal investigation, such notification shall be de-  
17 layed upon written notice from such Federal law en-  
18 forcement or intelligence agency to the agency or  
19 business entity that experienced the breach.

20 (2) EXTENDED DELAY OF NOTIFICATION.—If  
21 the notification required under subsection (a) is de-  
22 layed pursuant to paragraph (1), an agency or busi-  
23 ness entity shall give notice 30 days after the day  
24 such law enforcement delay was invoked unless a  
25 Federal law enforcement or intelligence agency pro-

1       vides written notification that further delay is nec-  
2       essary.

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

8   **SEC. 312. EXEMPTIONS.**

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

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

16                   (A) cause damage to the national security;

17                   or

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

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

24                   (A) conceal violations of law, inefficiency,

25                   or administrative error;

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

3 (C) restrain competition.

4 (3) NOTICE.—In every case in which an agency  
5 or business agency issues a certification under para-  
6 graph (1), the certification, accompanied by a de-  
7 scription of the factual basis for the certification,  
8 shall be immediately provided to the United States  
9 Secret Service and the Federal Bureau of Investiga-  
10 tion.

11 (4) SECRET SERVICE AND FBI REVIEW OF CER-  
12 TIFICATIONS.—

13 (A) IN GENERAL.—The United States Se-  
14 cret Service or the Federal Bureau of Investiga-  
15 tion may review a certification provided by an  
16 agency under paragraph (3), and shall review a  
17 certification provided by a business entity under  
18 paragraph (3), to determine whether an exemp-  
19 tion under paragraph (1) is merited. Such re-  
20 view shall be completed not later than 10 busi-  
21 ness days after the date of receipt of the certifi-  
22 cation, except as provided in paragraph (5)(C).

23 (B) NOTICE.—Upon completing a review  
24 under subparagraph (A) the United States Se-  
25 cret Service or the Federal Bureau of Investiga-

1           tion shall immediately notify the agency or  
2           business entity, in writing, of its determination  
3           of whether an exemption under paragraph (1)  
4           is merited.

5           (C) EXEMPTION.—The exemption under  
6           paragraph (1) shall not apply if the United  
7           States Secret Service or the Federal Bureau of  
8           Investigation determines under this paragraph  
9           that the exemption is not merited.

10          (5) ADDITIONAL AUTHORITY OF THE SECRET  
11          SERVICE AND FBI.—

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

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

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

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

13           (1) a risk assessment concludes that—

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

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



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

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

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

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

18 (3) the United States Secret Service or the  
19 Federal Bureau of Investigation does not indicate, in  
20 writing, within 10 business days from receipt of the  
21 decision, that notice should be given.

22 (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

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

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

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

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

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

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

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

22 **SEC. 313. METHODS OF NOTICE.**

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

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

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

6                   (B) Telephone notice to the individual per-  
7                   sonally.

8                   (C) 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.—Notice to major media  
15           outlets serving a State or jurisdiction, if the number  
16           of residents of such State whose sensitive personally  
17           identifiable information was, or is reasonably be-  
18           lieved to have been, accessed or acquired by an un-  
19           authorized person exceeds 5,000.

20 **SEC. 314. CONTENT OF NOTIFICATION.**

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

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

1 reasonably believed to have been, accessed or ac-  
2 quired by an unauthorized person;

3 (2) a toll-free number—

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

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

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

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

17 **SEC. 315. COORDINATION OF NOTIFICATION WITH CREDIT**  
18 **REPORTING AGENCIES.**

19 If an agency or business entity is required to provide  
20 notification to more than 5,000 individuals under section  
21 311(a), the agency or business entity shall also notify all  
22 consumer reporting agencies that compile and maintain  
23 files on consumers on a nationwide basis (as defined in  
24 section 603(p) of the Fair Credit Reporting Act (15  
25 U.S.C. 1681a(p)) of the timing and distribution of the no-

1 tices. Such notice shall be given to the consumer credit  
2 reporting agencies without unreasonable delay and, if it  
3 will not delay notice to the affected individuals, prior to  
4 the distribution of notices to the affected individuals.

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

6 (a) SECRET SERVICE AND FBI.—Any business entity  
7 or agency shall notify the United States Secret Service  
8 and the Federal Bureau of Investigation of the fact that  
9 a security breach has occurred if—

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

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

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

21 (4) the security breach involves primarily sen-  
22 sitive personally identifiable information of individ-  
23 uals known to the agency or business entity to be  
24 employees and contractors of the Federal Govern-

1           ment involved in national security or law enforce-  
2           ment.

3           (b) FTC REVIEW OF THRESHOLDS.—The Federal  
4 Trade Commission may review and adjust the thresholds  
5 for notice to law enforcement under subsection (a), after  
6 notice and the opportunity for public comment, in a man-  
7 ner consistent with this section.

8           (c) ADVANCE NOTICE TO LAW ENFORCEMENT.—Not  
9 later than 48 hours before notifying an individual of a se-  
10 curity breach under section 311, a business entity or agen-  
11 cy that is required to provide notice under this section  
12 shall notify the United States Secret Service and the Fed-  
13 eral Bureau of Investigation of the fact that the business  
14 entity or agency intends to provide the notice.

15           (d) NOTICE TO OTHER LAW ENFORCEMENT AGEN-  
16 CIES.—The United States Secret Service and the Federal  
17 Bureau of Investigation shall be responsible for noti-  
18 fying—

19                   (1) the United States Postal Inspection Service,  
20           if the security breach involves mail fraud;

21                   (2) the attorney general of each State affected  
22           by the security breach; and

23                   (3) the Federal Trade Commission, if the secu-  
24           rity breach involves consumer reporting agencies

1 subject to the Fair Credit Reporting Act (15 U.S.C.  
2 1681 et seq.), or anticompetitive conduct.

3 (e) **TIMING OF NOTICES.**—The notices required  
4 under this section shall be delivered as follows:

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

8 (2) Notice under subsection (d) shall be deliv-  
9 ered not later than 14 days after the Service receives  
10 notice of a security breach from an agency or busi-  
11 ness entity.

12 **SEC. 317. ENFORCEMENT.**

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

1 shall take into account the degree of culpability of the  
2 business entity, any prior violations of this subtitle by the  
3 business entity, the ability of the business entity to pay,  
4 the effect on the ability of the business entity to continue  
5 to do business, and such other matters as justice may re-  
6 quire.

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

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

14 (A) enjoining such act or practice; or

15 (B) enforcing compliance with this subtitle.

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

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

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



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

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

6 (a) IN GENERAL.—

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

22 (A) enjoin that practice;

23 (B) enforce compliance with this subtitle;

24 or

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

8 (2) NOTICE.—

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

13 (i) written notice of the action; and

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

16 (B) EXEMPTION.—

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

24 (ii) NOTIFICATION.—In an action de-  
25 scribed in clause (i), the attorney general

1 of a State shall provide notice and a copy  
2 of the complaint to the Attorney General  
3 at the time the State attorney general files  
4 the action.

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

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

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

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

17 (4) file petitions for appeal.

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

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

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

11 (e) VENUE; SERVICE OF PROCESS.—

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

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

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

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

23 (A) is an inhabitant; or

24 (B) may be found.

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

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

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

11 **SEC. 320. AUTHORIZATION OF APPROPRIATIONS.**

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

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

18 The United States Secret Service and the Federal  
19 Bureau of Investigation shall report to Congress not later  
20 than 18 months after the date of enactment of this Act,  
21 and upon the request by Congress thereafter, on—

22 (1) the number and nature of the security  
23 breaches described in the notices filed by those busi-  
24 ness entities invoking the risk assessment exemption  
25 under section 312(b) and the response of the United

1 States Secret Service and the Federal Bureau of In-  
2 vestigation to such notices; and

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

10 **SEC. 322. EFFECTIVE DATE.**

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

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

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

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

24 (1) the data privacy and security program of a  
25 data broker to ensure the privacy and security of

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

6 (2) the compliance of a data broker with such  
7 program;

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

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

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

23 (c) PENALTIES.—In awarding contracts with data  
24 brokers for products or services related to access, use,  
25 compilation, distribution, processing, analyzing, or evalu-

1 ating personally identifiable information, the Adminis-  
2 trator of the General Services Administration shall—

3 (1) include monetary or other penalties—

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

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

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

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

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

23 (C) require such service providers, by con-  
24 tract, to implement and maintain appropriate



1           measures designed to meet the objectives and  
2           requirements in title III.

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

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

10          Section 3544(b) of title 44, United States Code, is  
11 amended—

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

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

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

17           “(9) procedures for evaluating and auditing the  
18 information security practices of contractors or third  
19 party business entities supporting the information  
20 systems or operations of the agency involving per-  
21 sonally identifiable information (as that term is de-  
22 fined in section 3 of the Personal Data Privacy and  
23 Security Act of 2011) and ensuring remedial action  
24 to address any significant deficiencies.”.

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

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

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

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

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

12 “(iii) purchasing or subscribing for a  
13 fee to personally identifiable information  
14 from a data broker (as such terms are de-  
15 fined in section 3 of the Personal Data  
16 Privacy and Security Act of 2011).”.

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

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

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

4 (A) such database;

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

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

8 (2) adopts regulations that specify—

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

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

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

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

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

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

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

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

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

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

18 (A) providing for penalties—

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

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

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

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

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

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

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

23 (d) STUDY OF GOVERNMENT USE.—

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

1 Comptroller General of the United States shall con-  
2 duct a study and audit and prepare a report on Fed-  
3 eral agency actions to address the recommendations  
4 in the Government Accountability Office’s April  
5 2006 report on agency adherence to key privacy  
6 principles in using data brokers or commercial data-  
7 bases containing personally identifiable information.

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

10 **TITLE V—COMPLIANCE WITH**  
11 **STATUTORY PAY-AS-YOU-GO ACT**

12 **SEC. 501. BUDGET COMPLIANCE.**

13 The budgetary effects of this Act, for the purpose of  
14 complying with the Statutory Pay-As-You-Go Act of 2010,  
15 shall be determined by reference to the latest statement  
16 titled “Budgetary Effects of PAYGO Legislation” for this  
17 Act, submitted for printing in the Congressional Record  
18 by the Chairman of the Senate Budget Committee, pro-  
19 vided that such statement has been submitted prior to the  
20 vote on passage.

○