

AMENDMENT NO. \_\_\_\_\_ Calendar No. \_\_\_\_\_

Purpose: In the nature of a substitute.

**IN THE SENATE OF THE UNITED STATES—112th Cong., 1st Sess.**

**S. 1535**

To protect consumers by mitigating the vulnerability of personally identifiable information to theft through a security breach, providing notice and remedies to consumers in the wake of such a breach, holding companies accountable for preventable breaches, facilitating the sharing of post-breach technical information between companies, and enhancing criminal and civil penalties and other protections against the unauthorized collection or use of personally identifiable information.

Referred to the Committee on \_\_\_\_\_ and  
ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended  
to be proposed by Mr. BLUMENTHAL

Viz:

1 Strike all after the enacting clause and insert the fol-  
2 lowing:

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

4 (a) SHORT TITLE.—This Act may be cited as the  
5 “Personal Data Protection and Breach Accountability Act  
6 of 2011”.

7 (b) TABLE OF CONTENTS.—The table of contents of  
8 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. Concealment of security breaches involving sensitive personally identifiable information.
- Sec. 102. Unauthorized manipulation of Internet traffic on a user's computer.

TITLE II—PRIVACY AND SECURITY OF SENSITIVE PERSONALLY  
IDENTIFIABLE INFORMATION

Subtitle A—A Data Privacy and Security Program

- Sec. 201. Purpose and applicability of data privacy and security program.
- Sec. 202. Requirements for a personal data privacy and security program.
- Sec. 203. Federal enforcement.
- Sec. 204. Enforcement by State Attorneys General.
- Sec. 205. Supplemental enforcement by individuals.

Subtitle B—Security Breach Notification

- Sec. 211. Notice to individuals.
- Sec. 212. Exemptions from notice to individuals.
- Sec. 213. Methods of notice to individuals.
- Sec. 214. Content of notice to individuals.
- Sec. 215. Remedies for security breach.
- Sec. 216. Notice to credit reporting agencies.
- Sec. 217. Notice to law enforcement.
- Sec. 218. Federal enforcement.
- Sec. 219. Enforcement by State attorneys general.
- Sec. 220. Supplemental enforcement by individuals.
- Sec. 221. Relation to other laws.
- Sec. 222. Authorization of appropriations.
- Sec. 223. Reporting on risk assessment exemptions.

Subtitle C—Post-Breach Technical Information Clearinghouse

- Sec. 230. Clearinghouse information collection, maintenance, and access.
- Sec. 231. Protections for clearinghouse participants.
- Sec. 232. Effective date.

TITLE III—ACCESS TO AND USE OF COMMERCIAL DATA

- Sec. 301. General services administration review of contracts.
- Sec. 302. Requirement to audit information security practices of contractors and third party business entities.
- Sec. 303. Privacy impact assessment of government use of commercial information services containing sensitive personally identifiable information.
- Sec. 304. FBI report on reported breaches and compliance.
- Sec. 305. Department of Justice report on enforcement actions.
- Sec. 306. Report on notification effectiveness.

## TITLE IV—COMPLIANCE WITH STATUTORY PAY-AS-YOU-GO ACT

Sec. 401. 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

1 and assistance to mitigate their damages and to re-  
2 store the integrity of their personal information and  
3 identities;

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

9 (8) there is a need to ensure that data brokers  
10 conduct their operations in a manner that prioritizes  
11 fairness, transparency, accuracy, and respect for the  
12 privacy of consumers;

13 (9) government access to commercial data can  
14 potentially improve safety, law enforcement, and na-  
15 tional security;

16 (10) because government use of commercial  
17 data containing personal information potentially af-  
18 fects individual privacy, and law enforcement and  
19 national security operations, there is a need for Con-  
20 gress to exercise oversight over government use of  
21 commercial data;

22 (11) over 22,960,000 cases of data breaches in-  
23 volving personally identifiable information were re-  
24 ported through July of 2011, and in 2009 through

1       2010, over 230,900,000 cases of personal data  
2       breaches were reported;

3           (12) facilitating information sharing among  
4       business entities and across sectors in the event of  
5       a breach can assist in remediating the breach and  
6       preventing similar breaches in the future;

7           (13) because the Federal Government has lim-  
8       ited resources, consumers themselves play a vital  
9       and complementary role in facilitating prompt notifi-  
10      cation and protecting against future breaches of se-  
11      curity;

12          (14) in addition to the immediate damages  
13      caused by security breaches, the lack of basic reme-  
14      dial requirements often forces individuals whose sen-  
15      sitive personally identifiable information is com-  
16      promised as a result of a security breach to incur  
17      the economic costs of litigation to seek remedies, and  
18      the economic costs of fees required in many States  
19      to freeze compromised accounts; and

20          (15) victims of personal data breaches may suf-  
21      fer debilitating emotional and physical effects and  
22      become depressed or anxious, especially in cases of  
23      repeated or unresolved instances of data breaches.

1 **SEC. 3. DEFINITIONS.**

2 (a) IN GENERAL.—In this Act, the following defini-  
3 tions shall apply:

4 (1) AFFILIATE.—The term “affiliate” means  
5 persons related by common ownership or by cor-  
6 porate control.

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

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

15 (4) CREDIT RATING AGENCY.—The term “cred-  
16 it rating agency” has the meaning given such term  
17 in section 3(a)(61) of the Securities Exchange Act  
18 of 1934 (12 U.S.C. 78c(a)(61)).

19 (5) CREDIT REPORT.—The term “credit report”  
20 means a consumer report, as that term is defined in  
21 section 603 of the Fair Credit Reporting Act (15  
22 U.S.C. 1681a).

23 (6) DATA BROKER.—The term “data broker”  
24 means a business entity which for monetary fees or  
25 dues regularly engages in the practice of collecting,  
26 transmitting, or providing access to sensitive person-

1       ally identifiable information on more than 5,000 in-  
2       dividuals who are not the customers or employees of  
3       that business entity or affiliate primarily for the  
4       purposes of providing such information to non-  
5       affiliated third parties on an interstate basis.

6           (7) DESIGNATED ENTITY.—The term “des-  
7       ignated entity” means the Federal Government enti-  
8       ty designated under section 217(a).

9           (8) ENCRYPTION.—The term “encryption”—

10           (A) means the protection of data in elec-  
11       tronic form, in storage or in transit, using an  
12       encryption technology that has been generally  
13       accepted by experts in the field of information  
14       security that renders such data indecipherable  
15       in the absence of associated cryptographic keys  
16       necessary to enable decryption of such data;  
17       and

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

21           (9) IDENTITY THEFT.—The term “identity  
22       theft” means a violation of section 1028(a)(7) of  
23       title 18, United States Code.

24           (10) INTELLIGENCE COMMUNITY.—The term  
25       “intelligence community” includes the following:

1 (A) The Office of the Director of National  
2 Intelligence.

3 (B) The Central Intelligence Agency.

4 (C) The National Security Agency.

5 (D) The Defense Intelligence Agency.

6 (E) The National Geospatial-Intelligence  
7 Agency.

8 (F) The National Reconnaissance Office.

9 (G) Other offices within the Department of  
10 Defense for the collection of specialized national  
11 intelligence through reconnaissance programs.

12 (H) The intelligence elements of the Army,  
13 the Navy, the Air Force, the Marine Corps, the  
14 Federal Bureau of Investigation, and the De-  
15 partment of Energy.

16 (I) The Bureau of Intelligence and Re-  
17 search of the Department of State.

18 (J) The Office of Intelligence and Analysis  
19 of the Department of the Treasury.

20 (K) The elements of the Department of  
21 Homeland Security concerned with the analysis  
22 of intelligence information, including the Office  
23 of Intelligence of the Coast Guard.

24 (L) Such other elements of any other de-  
25 partment or agency as may be designated by

1           the President, or designated jointly by the Di-  
2           rector of National Intelligence and the head of  
3           the department or agency concerned, as an ele-  
4           ment of the intelligence community.

5           (11) PREDISPUTE ARBITRATION AGREEMENT.—

6           The term “predispute arbitration agreement” means  
7           any agreement to arbitrate a dispute that had not  
8           yet arisen at the time of the making of the agree-  
9           ment.

10          (12) PUBLIC RECORD SOURCE.—The term

11          “public record source” means the Congress, any  
12          agency, any State or local government agency, the  
13          government of the District of Columbia and govern-  
14          ments of the territories or possessions of the United  
15          States, and Federal, State or local courts, courts  
16          martial and military commissions, that maintain  
17          personally identifiable information in records avail-  
18          able to the public.

19          (13) SECURITY BREACH.—

20          (A) IN GENERAL.—The term “security  
21          breach” means compromise of the security, con-  
22          fidentiality, or integrity of, or the loss of, com-  
23          puterized data through misrepresentation or ac-  
24          tions that result in, or that there is a reason-  
25          able basis to conclude has resulted in—

1 (i) the unauthorized acquisition of  
2 sensitive personally identifiable informa-  
3 tion; or

4 (ii) access to sensitive personally iden-  
5 tifiable information that is for an unau-  
6 thorized purpose, or in excess of authoriza-  
7 tion.

8 (B) EXCLUSION.—The term “security  
9 breach” does not include—

10 (i) a good faith acquisition of sensitive  
11 personally identifiable information by a  
12 business entity or agency, or an employee  
13 or agent of a business entity or agency, if  
14 the sensitive personally identifiable infor-  
15 mation is not subject to further unauthor-  
16 ized disclosure;

17 (ii) the release of a public record not  
18 otherwise subject to confidentiality or non-  
19 disclosure requirements or the release of  
20 information obtained from a public record;  
21 or

22 (iii) any lawfully authorized criminal  
23 investigation or authorized investigative,  
24 protective, or intelligence activities that are  
25 carried out by or on behalf of any element

1 of the intelligence community and con-  
2 ducted in accordance with the United  
3 States laws, authorities, and regulations  
4 governing such intelligence activities.

5 (14) SECURITY FREEZE.—The term “security  
6 freeze” means a notice, at the request of the con-  
7 sumer and subject to exceptions in section 215(b),  
8 that prohibits the consumer reporting agency from  
9 releasing all or any part of the consumer’s credit re-  
10 port or any information derived from it without the  
11 express authorization of the consumer.

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

17 (A) An individual’s first and last name or  
18 first initial and last name in combination with  
19 any 2 of the following data elements:

- 20 (i) Home address.  
21 (ii) Telephone number of the indi-  
22 vidual.  
23 (iii) Mother’s maiden name.  
24 (iv) Month, day, and year of birth.

1 (B) A non-truncated social security num-  
2 ber, driver's license number, passport number,  
3 or alien registration number or other govern-  
4 ment-issued unique identification number.

5 (C) Information about an individual's geo-  
6 graphic location that is in whole or in part gen-  
7 erated by or derived from that individual's use  
8 of a wireless communication device or other  
9 electronic device, excluding telephone and in-  
10 strument numbers and network or Internet  
11 Protocol addresses.

12 (D) Unique biometric data such as a finger  
13 print, voice print, face print, a retina or iris  
14 image, or any other unique physical representa-  
15 tion.

16 (E) A unique account identifier, including  
17 a financial account number or credit or debit  
18 card number, electronic identification number,  
19 user name, health insurance policy or subscriber  
20 identification number, or routing code.

21 (F) Not less than 2 of the following data  
22 elements:

23 (i) An individual's first and last name  
24 or first initial and last name.

1           (ii) A unique account identifier, in-  
2           cluding a financial account number or  
3           credit or debit card number, electronic  
4           identification number, user name, or rout-  
5           ing code.

6           (iii) Any security code, access code, or  
7           password, or source code that could be  
8           used to generate such codes and pass-  
9           words.

10          (iv) Information regarding an individ-  
11          ual's medical history, mental or physical  
12          medical condition, or medical treatment or  
13          diagnosis by a health care professional.

14          (G) Any other combination of data ele-  
15          ments that could allow unauthorized access to  
16          or acquisition of the information described in  
17          subparagraph (A), (B), (C), (D), (E), or (F),  
18          including—

19               (i) a unique account identifier;

20               (ii) an electronic identification num-  
21               ber;

22               (iii) a user name;

23               (iv) a routing code; or

24               (v) any associated security code, ac-  
25               cess code, or password or any associated

1 security questions and answers that could  
2 allow unauthorized access to the account.

3 (16) SERVICE PROVIDER.—

4 (A) IN GENERAL.—The term “service pro-  
5 vider” means a business entity that—

6 (i) provides electronic data trans-  
7 mission, routing, intermediate and tran-  
8 sient storage, or connections to the system  
9 or network of the business entity;

10 (ii) is not the sender or the intended  
11 recipient of the data;

12 (iii) is not ordinarily expected to select  
13 or modify the content of the electronic  
14 data; and

15 (iv) transmits, routes, stores, or pro-  
16 vides connections for personal information  
17 in a manner that personal information is  
18 undifferentiated from other types of data  
19 that such business entity transmits, routes,  
20 stores, or provides connections.

21 (B) SAVINGS CLAUSE.—Any such business  
22 entity shall be treated as a service provider  
23 under this Act only to the extent that the busi-  
24 ness entity is engaged in the provision of the  
25 transmission, routing, intermediate and tran-

1           sient storage or connections described in sub-  
2           paragraph (A).

3           (b) MODIFIED DEFINITION BY RULEMAKING.—The  
4 Federal Trade Commission may, by rule promulgated  
5 under section 553 of title 5, United States Code, modify  
6 the definition of “sensitive personally identifiable informa-  
7 tion” in a manner consistent with the purposes of this Act  
8 and to the extent that such modification will not unreason-  
9 ably impede interstate commerce.

10 **TITLE I—ENHANCING PUNISH-**  
11 **MENT FOR IDENTITY THEFT**  
12 **AND OTHER VIOLATIONS OF**  
13 **DATA PRIVACY AND SECUR-**  
14 **ITY**

15 **SEC. 101. CONCEALMENT OF SECURITY BREACHES INVOLV-**  
16 **ING SENSITIVE PERSONALLY IDENTIFIABLE**  
17 **INFORMATION.**

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

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

24           “(a) Whoever, having knowledge of a security breach  
25 and of the fact that notice of such security breach is re-

1 quired under title II of the Personal Data Protection and  
2 Breach Accountability Act of 2011, intentionally or will-  
3 fully conceals the fact of such security breach and which  
4 breach, shall, in the event that such security breach results  
5 in economic harm or substantial emotional distress to 1  
6 or more persons, shall be fined under this title or impris-  
7 oned not more than 5 years, or both.

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

11 “(c) Any person seeking an exemption under section  
12 212(b) of the Personal Data Protection and Breach Ac-  
13 countability Act of 2011 shall be immune from prosecution  
14 under this section if the United States Secret Service does  
15 not indicate, in writing, that such notice be given under  
16 section 212(b)(1)(B) of the Personal Data Protection and  
17 Breach Accountability Act of 2011.”.

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

“1041. Concealment of security breaches involving sensitive personally identifi-  
able information.”.

22 (c) ENFORCEMENT AUTHORITY.—

23 (1) IN GENERAL.—The United States Secret  
24 Service and the Federal Bureau of Investigation

1 shall have the authority to investigate offenses under  
2 this section.

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

6 **SEC. 102. UNAUTHORIZED MANIPULATION OF INTERNET**  
7 **TRAFFIC ON A USER'S COMPUTER.**

8 (a) DEFINITION.—In this section, the term “pro-  
9 tected computer” has the meaning given the term in sec-  
10 tion 1030(e)(2) of title 18, United States Code.

11 (b) PROHIBITION.—

12 (1) IN GENERAL.—Unless a service provider  
13 provides a clear and conspicuous disclosure of data  
14 collected in the process of intercepting a web search  
15 or query entered by an authorized user of a pro-  
16 tected computer, and obtains the consent of an au-  
17 thorized user of the protected computer prior to any  
18 such action, it shall be unlawful for a service pro-  
19 vider to knowingly or intentionally—

20 (A) bypass the display of search engine re-  
21 sults and redirect web searches or queries en-  
22 tered by an authorized user of a protected com-  
23 puter directly to a commercial website, counter-  
24 feit web page, or targeted advertisement and

1           derive an economic benefit from such activity;

2           or

3                   (B) monitor, manipulate, aggregate, and  
4           market the data collected in the process of  
5           intercepting a web search or query entered by  
6           an authorized user of a protected computer and  
7           derive an economic benefit from such activity.

8           (2) CONSENT.—A service provider may not re-  
9           quire consent to perform the collection of data de-  
10          scribed in paragraph (1) as a condition of providing  
11          service to an authorized user of the protected com-  
12          puter.

13          (c) LIMITATIONS ON LIABILITY.—The restrictions  
14          imposed under this section do not apply to any monitoring  
15          of, or interaction with, a subscriber’s Internet or other  
16          network connection or service, or a protected computer,  
17          by or at the direction of a telecommunications carrier,  
18          cable operator, computer hardware or software provider,  
19          financial institution or provider of information services or  
20          interactive computer service for—

21                   (1) network or computer security purposes;

22                   (2) diagnostics;

23                   (3) technical support;

24                   (4) repair;

25                   (5) network management;

1           (6) authorized updates of software or system  
2           firmware;

3           (7) authorized remote system management;

4           (8) authorized provision of protection for users  
5           of the computer from objectionable content;

6           (9) authorized scanning for computer software  
7           used in violation of this section for removal by an  
8           authorized user; or

9           (10) detection or prevention of fraud.

10          (d) ENFORCEMENT BY THE ATTORNEY GENERAL.—

11           (1) LIABILITY AND PENALTY FOR VIOLA-  
12           TIONS.—Any person who engages in an activity in  
13           violation of this section shall be fined not more than  
14           \$500,000.

15           (2) ENHANCED LIABILITY AND PENALTIES FOR  
16           PATTERN OR PRACTICE OF VIOLATIONS.—

17           (A) IN GENERAL.—Any person who en-  
18           gages in a pattern or practice of activity that  
19           violates the provisions of this section shall be  
20           fined not more than \$1,000,000.

21           (B) TREATMENT OF SINGLE ACTION OR  
22           CONDUCT.—For purposes of subparagraph (A),  
23           any single action or conduct that violates this  
24           section with respect to multiple protected com-  
25           puters shall be construed as a single violation.

1           (3) CONSIDERATIONS.—In determining the  
2 amount of any penalty under paragraph (1) or (2),  
3 the court shall take into account—

4           (A) the degree of culpability of the defend-  
5 ant;

6           (B) any history of prior such conduct;

7           (C) the ability of the defendant to pay any  
8 fine imposed;

9           (D) the effect on the ability of the defend-  
10 ant to continue to do business; and

11           (E) such other matters as justice may re-  
12 quire.

13 **TITLE II—PRIVACY AND SECUR-**  
14 **ITY OF SENSITIVE PERSON-**  
15 **ALLY IDENTIFIABLE INFOR-**  
16 **MATION**

17 **Subtitle A—A Data Privacy and**  
18 **Security Program**

19 **SEC. 201. 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 security 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 202 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 the following:

12 (1) FINANCIAL INSTITUTIONS.—A financial in-  
13 stitution subject to the data security requirements  
14 and standards under 501(b) of the Gramm-Leach-  
15 Bliley Act (15 U.S.C. 6801(b)) and subject to the  
16 jurisdiction of an agency or authority described in  
17 section 505(a) of the Gramm-Leach-Bliley Act (15  
18 U.S.C. 6805(a)), if the Federal functional regulator  
19 (as defined in section 509 of the Gramm-Leach-Bli-  
20 ley Act (15 U.S.C. 6809)) with jurisdiction over that  
21 financial institution has issued a regulation under  
22 title V of the Gramm-Leach-Bliley Act (15 U.S.C.  
23 6801 et seq.) that requires financial institutions  
24 within its jurisdiction to provide notification to indi-  
25 viduals following a breach of security.

1 (2) HIPAA REGULATED ENTITIES.—

2 (A) COVERED ENTITIES.—A business enti-  
3 ty subject to the Health Insurance Portability  
4 and Accountability Act of 1996 (42 U.S.C.  
5 1301 et seq.), including the data security re-  
6 quirements and implementing regulations of  
7 that Act.

8 (B) COMPLIANCE.—A business entity  
9 that—

10 (i) is acting as a business associate,  
11 as that term is defined under the Health  
12 Insurance Portability and Accountability  
13 Act of 1996 (42 U.S.C. 1301 et seq.) and  
14 is in compliance with the requirements im-  
15 posed under that Act and implementing  
16 regulations promulgated under that Act;  
17 and

18 (ii) is subject to, and currently in  
19 compliance, with the privacy and data se-  
20 curity requirements under sections 13401  
21 and 13404 of division A of the American  
22 Reinvestment and Recovery Act of 2009  
23 (42 U.S.C. 17931 and 17934) and imple-  
24 menting regulations promulgated under  
25 such sections.



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 identifiable  
13 information;

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

18 (C) protect against unauthorized access to  
19 or use of sensitive personally identifiable infor-  
20 mation that could create a significant risk of  
21 harm 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;

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; and

24 (vii) minimize the amount of personal  
25 information maintained by the business en-

1                   tity, providing for the retention of such  
2                   personal information only as reasonably  
3                   needed for the business purposes of the  
4                   business entity or as necessary to comply  
5                   with any other provision of law.

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

10          (c) VULNERABILITY TESTING.—

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

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

21          (d) CERTAIN RELATIONSHIP TO PROVIDERS OF  
22 SERVICES.—In the event a business entity subject to this  
23 subtitle engages a person or entity not subject to this sub-  
24 title (other than a service provider) to receive sensitive  
25 personally identifiable information in performing services

1 or functions (other than the services or functions provided  
2 by a service provider) on behalf of and under the instruc-  
3 tion of such business entity, such business entity shall—

4           (1) exercise appropriate due diligence in select-  
5           ing the person or entity for responsibilities related to  
6           sensitive personally identifiable information, and  
7           take reasonable steps to select and retain a person  
8           or entity that is capable of maintaining appropriate  
9           safeguards for the security, privacy, and integrity of  
10          the sensitive personally identifiable information at  
11          issue; and

12          (2) require the person or entity by contract to  
13          implement and maintain appropriate measures de-  
14          signed to meet the objectives and requirements gov-  
15          erning entities subject to section 201, this section,  
16          and subtitle B.

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

23                 (1) technology;

24                 (2) the sensitivity of sensitive personally identi-  
25          fiable information;

1           (3) internal or external threats to sensitive per-  
2           sonally identifiable information; and

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

5                   (A) mergers and acquisitions;

6                   (B) alliances and joint ventures;

7                   (C) outsourcing arrangements;

8                   (D) bankruptcy; and

9                   (E) changes to sensitive personally identifi-  
10           able information systems.

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

16   **SEC. 203. FEDERAL ENFORCEMENT.**

17           (a) CIVIL PENALTIES.—

18                   (1) IN GENERAL.—The Attorney General may  
19           bring a civil action in the appropriate United States  
20           district court against any business entity that en-  
21           gages in conduct constituting a violation of this sub-  
22           title and, upon proof of such conduct by a prepon-  
23           derance of the evidence, such business entity shall be  
24           subject to a civil penalty of not more than \$5,000  
25           per violation per day while such a violation exists,

1 with a maximum of \$20,000,000 per violation, un-  
2 less such conduct is found to be willful or inten-  
3 tional.

4 (2) INTENTIONAL OR WILLFUL VIOLATION.—A  
5 business entity that intentionally or willfully violates  
6 the provisions of this subtitle shall be subject to ad-  
7 ditional penalties in the amount of \$5,000 per viola-  
8 tion per day while such a violation exists.

9 (3) CONSIDERATIONS.—In determining the  
10 amount of a civil penalty under this subsection, the  
11 court shall take into account—

12 (A) the degree of culpability of the busi-  
13 ness entity;

14 (B) any prior violations of this subtitle by  
15 the business entity;

16 (C) the ability of the business entity to pay  
17 a civil penalty;

18 (D) the effect on the ability of the business  
19 entity to continue to do business;

20 (E) the number of individuals whose sen-  
21 sitive personally identifiable information was  
22 compromised by the breach;

23 (F) the relative cost of compliance with  
24 this subtitle; and

1 (G) such other matters as justice may re-  
2 quire.

3 (b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-  
4 ERAL.—

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

10 (A) enjoining such act or practice; or

11 (B) enforcing compliance with this subtitle.

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

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

20 **SEC. 204. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

21 (a) CIVIL ACTIONS.—

22 (1) IN GENERAL.—In any case in which the at-  
23 torney general of a State or any State or local law  
24 enforcement agency authorized by the State attorney  
25 general or by State statute to prosecute violations of

1 consumer protection law, has reason to believe that  
2 an interest of the residents of that State has been  
3 or is threatened or adversely affected by the acts or  
4 practices of a business entity that violate this sub-  
5 title, the State may bring a civil action on behalf of  
6 the residents of that State in a district court of the  
7 United States of appropriate jurisdiction, or any  
8 other court of competent jurisdiction, to—

9 (A) enjoin that act or practice;

10 (B) enforce compliance with this subtitle;

11 or

12 (C) obtain civil penalties of not more than  
13 \$5,000 per violation per day while such viola-  
14 tions persist, up to a maximum of \$20,000,000  
15 per violation.

16 (2) CONSIDERATIONS.—In determining the  
17 amount of a civil penalty under this subsection, the  
18 court shall take into account—

19 (A) the degree of culpability of the busi-  
20 ness entity;

21 (B) any prior violations of this subtitle by  
22 the business entity;

23 (C) the ability of the business entity to pay  
24 a civil penalty;

1 (D) the effect on the ability of the business  
2 entity to continue to do business;

3 (E) the number of individuals whose sen-  
4 sitive personally identifiable information was  
5 compromised by the breach;

6 (F) the relative cost of compliance with  
7 this subtitle; and

8 (G) such other matters as justice may re-  
9 quire.

10 (3) 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 in subparagraph (B), the  
3 attorney general of a State shall provide the  
4 written notice and a copy of the complaint to  
5 the Attorney General as soon after the filing of  
6 the complaint as practicable.

7 (b) FEDERAL PROCEEDINGS.—Upon receiving notice  
8 under subsection (a)(3), 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 described in subsection (c);

13 (2) initiate an action in the appropriate United  
14 States district court under section 218 and move to  
15 consolidate all pending actions, including State ac-  
16 tions, in such court;

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

19 (4) file petitions for appeal.

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

1 or civil action for any violation that is alleged in that pro-  
2 ceeding or action.

3 (d) CONSTRUCTION.—For purposes of bringing any  
4 civil action under subsection (a), nothing in this section  
5 shall be construed to prevent an attorney general of a  
6 State from exercising the powers conferred on such attor-  
7 ney general by the laws of that State to—

8 (1) conduct investigations;

9 (2) administer oaths or affirmations; or

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

12 (e) VENUE; SERVICE OF PROCESS.—

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

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

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

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

24 (A) is an inhabitant; or

25 (B) may be found.

1 **SEC. 205. SUPPLEMENTAL ENFORCEMENT BY INDIVIDUALS.**

2 (a) IN GENERAL.—Any person aggrieved by a viola-  
3 tion of the provisions of this subtitle by a business entity  
4 may bring a civil action in a court of appropriate jurisdic-  
5 tion to recover for personal injuries sustained as a result  
6 of the violation.

7 (b) AUTHORITY TO BRING CIVIL ACTION; JURISDIC-  
8 TION.—As provided in subsection (c), any person may  
9 commence a civil action on his own behalf against any  
10 business entity who is alleged to have violated the provi-  
11 sions of this subtitle.

12 (c) REMEDIES IN A CITIZEN SUIT.—

13 (1) DAMAGES.—Any individual harmed by a  
14 failure of a business entity to comply with the provi-  
15 sions of this subtitle, shall be able to collect damages  
16 of not more than \$10,000 per violation per day while  
17 such violations persist, up to a maximum of  
18 \$20,000,000 per violation.

19 (2) PUNITIVE DAMAGES.—A business entity  
20 may be liable for punitive damages if the business  
21 entity intentionally or willfully violates the provisions  
22 of this subtitle.

23 (3) EQUITABLE RELIEF.—A business entity  
24 that violates the provisions of this subtitle may be  
25 enjoined to comply with the provisions of those sec-  
26 tions.

1 (d) OTHER RIGHTS AND REMEDIES.—The rights and  
2 remedies available under this subsection are cumulative  
3 and shall not affect any other rights and remedies avail-  
4 able under law.

5 (e) NONENFORCEABILITY OF CERTAIN PROVISIONS  
6 WAIVING RIGHTS AND REMEDIES OR REQUIRING ARBI-  
7 TRATION OF DISPUTES.—

8 (1) WAIVER OF RIGHTS AND REMEDIES.—The  
9 rights and remedies provided for in this section may  
10 not be waived by any agreement, policy form, or con-  
11 dition of employment including by a predispute arbi-  
12 tration agreement.

13 (2) PREDISPUTE ARBITRATION AGREEMENTS.—  
14 No predispute arbitration agreement shall be valid  
15 or enforceable, if the agreement requires arbitration  
16 of a dispute arising under this section.

17 (f) CONSIDERATIONS.—In determining the amount of  
18 a civil penalty under this subsection, the court shall take  
19 into account—

20 (1) the degree of culpability of the business en-  
21 tity;

22 (2) any prior violations of this subtitle by the  
23 business entity;

24 (3) the ability of the business entity to pay a  
25 civil penalty;

1           (4) the effect on the ability of the business enti-  
2           ty to continue to do business;

3           (5) the number of individuals whose sensitive  
4           personally identifiable information was compromised  
5           by the breach;

6           (6) the relative cost of compliance with this  
7           subtitle; and

8           (7) such other matters as justice may require.

9           **Subtitle B—Security Breach**  
10           **Notification**

11       **SEC. 211. NOTICE TO INDIVIDUALS.**

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

21       (b) OBLIGATION OF OWNER OR LICENSEE.—

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

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

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

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

21 (4) SERVICE PROVIDERS.—If a service provider  
22 becomes aware of a security breach containing sen-  
23 sitive personally identifiable information that is  
24 owned or possessed by another business entity that  
25 connects to or uses a system or network provided by

1 the service provider for the purpose of transmitting,  
2 routing, or providing intermediate or transient stor-  
3 age of such data, the service provider shall be re-  
4 quired to notify the business entity who initiated  
5 such connection, transmission, routing, or storage of  
6 the security breach if the business entity can be rea-  
7 sonably identified. Upon receiving such notification  
8 from a service provider, the business entity shall be  
9 required to provide the notification required under  
10 subsection (a).

11 (c) TIMELINESS OF NOTIFICATION.—

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

16 (2) REASONABLE DELAY.—Reasonable delay  
17 under this subsection may include any time nec-  
18 essary to determine the scope of the security breach,  
19 conduct the risk assessment described in section  
20 212(b)(1), and provide notice to law enforcement  
21 when required.

22 (3) BURDEN OF PRODUCTION.—The agency,  
23 business entity, owner, or licensee required to pro-  
24 vide notice under this subtitle shall, upon the re-  
25 quest of the Attorney General, the Federal Trade

1 Commission, or the attorney general of a State or  
2 any State or local law enforcement agency author-  
3 ized by the attorney general of the State or by State  
4 statute to prosecute violations of consumer protec-  
5 tion law, provide records or other evidence of the no-  
6 tifications required under this subtitle, including to  
7 the extent applicable, the reasons for any delay of  
8 notification.

9 (d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW  
10 ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—

11 (1) IN GENERAL.—If a Federal law enforce-  
12 ment agency or member of the intelligence commu-  
13 nity determines that the notification required under  
14 this section would impede any lawfully authorized  
15 criminal investigation or authorized investigative,  
16 protective, or intelligence activities that are carried  
17 out by or on behalf of any element of the intelligence  
18 community and conducted in accordance with the  
19 United States laws, authorities, and regulations gov-  
20 erning such intelligence activities, such notification  
21 shall be delayed upon written notice from such Fed-  
22 eral law enforcement agency or member of the intel-  
23 ligence community to the agency or business entity  
24 that experienced the breach. The notification shall  
25 specify in writing the period of delay required.

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

9           (3) LAW ENFORCEMENT IMMUNITY.—No non-  
10          constitutional cause of action shall lie in any court  
11          against an agency for acts relating to the delay of  
12          notification for law enforcement or intelligence pur-  
13          poses under this subtitle.

14 **SEC. 212. EXEMPTIONS FROM NOTICE TO INDIVIDUALS.**

15          (a) EXEMPTION FOR NATIONAL SECURITY AND LAW  
16          ENFORCEMENT.—

17               (1) IN GENERAL.—Section 211 shall not apply  
18               to an agency or business entity if—

19                       (A) the United States Secret Service or the  
20                       Federal Bureau of Investigation determines  
21                       that notification of the security breach could be  
22                       expected to reveal sensitive sources and meth-  
23                       ods or similarly impede the ability of the Gov-  
24                       ernment to conduct law enforcement investiga-  
25                       tions; or

1 (B) the Federal Bureau of Investigation  
2 determines that notification of the security  
3 breach could be expected to cause damage to  
4 national security.

5 (2) IMMUNITY.—No non-constitutional cause of  
6 action shall lie in any court against any Federal  
7 agency for acts relating to the exemption from noti-  
8 fication under this subtitle.

9 (b) SAFE HARBOR.—

10 (1) IN GENERAL.—An agency or business entity  
11 shall be exempt from the notice requirements under  
12 section 211, if—

13 (A) a risk assessment conducted by the  
14 agency or business entity, in consultation with  
15 the Federal Trade Commission, concludes that  
16 there is no significant risk that a security  
17 breach has resulted in, or will result in harm to  
18 the individuals whose sensitive personally iden-  
19 tifiable information was subject to the security  
20 breach; and

21 (B) the Federal Trade Commission or des-  
22 ignated entity does not indicate within 7 busi-  
23 ness days from the receipt of written notifica-  
24 tion from an agency or business entity pursuant  
25 to subsection 212 (b)(2), that the agency or

1 business entity should not be exempt from the  
2 notice requirements of section 211.

3 (2) RISK ASSESSMENT REQUIREMENTS.—

4 (A) CONDUCTING A RISK ASSESSMENT.—

5 Upon discovery of a security breach of an agen-  
6 cy or business entity, the agency or business en-  
7 tity shall conduct a risk assessment to deter-  
8 mine if there is a significant risk that the secu-  
9 rity breach resulted in, or will result in, harm  
10 to the individuals whose sensitive personally  
11 identifiable information was subject to the secu-  
12 rity breach.

13 (i) PRESUMPTION OF NO SIGNIFICANT  
14 RISK.—It is presumed that there is no sig-  
15 nificant risk that the security breach has  
16 resulted in, or will result in, harm to the  
17 individuals whose sensitive personally iden-  
18 tifiable data was subject to the security  
19 breach, if the sensitive personally identifi-  
20 able information has been rendered unus-  
21 able, unreadable, or indecipherable through  
22 a security technology or methodology (if  
23 the technology or methodology is generally  
24 accepted by experts in the information se-  
25 curity field). Any such presumption may be

1           rebutted by facts demonstrating that the  
2           security technologies or methodologies in a  
3           specific case, have been or are reasonably  
4           likely to be compromised.

5           (ii) PRESUMPTION OF SIGNIFICANT  
6           RISK.—It is presumed that there is a sig-  
7           nificant risk that the security breach has  
8           resulted in, or will result in, harm to indi-  
9           viduals whose sensitive personally identifi-  
10          able information was subject to the secu-  
11          rity breach if the agency or business entity  
12          failed to render such sensitive personally  
13          identifiable information indecipherable  
14          through a security technology or method-  
15          ology (if the technology or methodology is  
16          generally accepted by experts in the infor-  
17          mation security field).

18          (iii) METHODOLOGIES OR TECH-  
19          NOLOGIES.—

20               (I) REQUIRED RULEMAKING.—

21               Not later than 1 year after the date  
22               of the enactment of this Act, and bi-  
23               annually thereafter, the Federal  
24               Trade Commission, after consultation  
25               with the National Institute of Stand-

1 ards and Technology, shall issue rules  
2 (pursuant to section 553 of title 5,  
3 United States Code) or guidance to  
4 identify security methodologies or  
5 technologies, such as encryption,  
6 which render sensitive personally iden-  
7 tifiable information unusable,  
8 unreadable, or indecipherable, that  
9 shall, if applied to such sensitive per-  
10 sonally identifiable information, estab-  
11 lish a presumption that no significant  
12 risk of harm exists to individuals  
13 whose sensitive personally identifiable  
14 information was subject to a security  
15 breach. Any such presumption may be  
16 rebutted by facts demonstrating that  
17 any such methodology or technology  
18 in a specific case has been or is rea-  
19 sonably likely to be compromised.

20 (II) REQUIRED CONSULTA-  
21 TION.—In issuing rules or guidance  
22 under subclause (II), the Commission  
23 shall also consult with relevant indus-  
24 tries, consumer organizations, and  
25 data security and identity theft pre-



1 standards generally accepted by experts in  
2 the field of information security; or

3 (ii) submit results of a risk assess-  
4 ment that—

5 (I) conceal violations of law, inef-  
6 ficiency, or administrative error;

7 (II) prevent embarrassment to a  
8 business entity, organization, or agen-  
9 cy;

10 (III) restrain competition;

11 (IV) contain fraudulent or delib-  
12 erately misleading information; or

13 (V) delay notification under sec-  
14 tion 211 for any other reason, except  
15 where the agency or business entity  
16 reasonably believes that the risk as-  
17 sessment exception may apply.

18 (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

19 (1) IN GENERAL.—A business entity shall be  
20 exempt from the notice requirements of this subtitle  
21 if the business entity utilizes or participates in a se-  
22 curity program that—

23 (A) effectively blocks the use of the sen-  
24 sitive personally identifiable information to ini-  
25 tiate unauthorized financial transactions before

1           they are charged to the account of the indi-  
2           vidual; and

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

6           (2) LIMITATION.—Paragraph (1) shall not  
7           apply to a business entity if the information subject  
8           to the security breach includes an individual’s first  
9           and last name, or any other type of sensitive person-  
10          ally identifiable information, other than a credit card  
11          or credit card security code identified in section 3,  
12          unless that information is only a credit card number  
13          or a credit card security code.

14          (d) LIMITATIONS.—Notwithstanding any other obli-  
15          gation under this subtitle, this subtitle does not apply to  
16          the following—

17                  (1) FINANCIAL INSTITUTIONS.—A financial in-  
18          stitution subject to the data security requirements  
19          and standards under 501(b) of the Gramm-Leach-  
20          Bliley Act (15 U.S.C. 6801 et seq.), and subject to  
21          the jurisdiction of an agency or authority described  
22          in section 505(a) of the Gramm-Leach-Bliley Act  
23          (15 U.S.C. 6805(a)), if the Federal functional regu-  
24          lator (as defined by section 509 of the Gramm-  
25          Leach-Bliley Act (15 U.S.C. 6809)) with jurisdiction

1 over that financial institution has issued a regulation  
2 under title V of the Gramm-Leach-Bliley Act (15  
3 U.S.C. 6801 et seq.) that requires financial institu-  
4 tions within its jurisdiction to provide notification to  
5 individuals following a breach of security.

6 (2) HIPAA REGULATED ENTITIES EXEMP-  
7 TION.—

8 (A) IN GENERAL.—A business entity shall  
9 be exempt from the notice requirement under  
10 section 211 if the business entity is one of the  
11 following:

12 (i) COVERED ENTITIES.—A business  
13 entity subject to the Health Insurance  
14 Portability and Accountability Act of 1996  
15 (42 U.S.C. 1301 et seq.), including the  
16 data breach notification requirements and  
17 implementing regulations of that Act.

18 (ii) BUSINESS ENTITIES.—A business  
19 entity that—

20 (I) is acting as a business asso-  
21 ciate, as that term is defined under  
22 the Health Insurance Portability and  
23 Accountability Act of 1996 (42 U.S.C.  
24 1301 et seq.) and is in compliance  
25 with the requirements imposed under

1 that Act and implementing regula-  
2 tions promulgated under that Act;  
3 and

4 (II) is subject to, and currently  
5 in compliance with, the data breach  
6 notification requirements under sec-  
7 tion 13402 or 13407 of the American  
8 Reinvestment and Recovery Act of  
9 2009 (42 U.S.C. 17932 and 17937)  
10 and implementing regulations promul-  
11 gated under such sections.

12 (B) LIMITATION.—Paragraph (1) shall not  
13 apply to a business entity if the information  
14 subject to the security breach includes an indi-  
15 vidual's first and last name, or any other type  
16 of sensitive personally identifiable information  
17 other than a health insurance policy or sub-  
18 scriber identification number or information re-  
19 garding an individual's medical history, mental  
20 or physical medical condition, or medical treat-  
21 ment or diagnosis by a health care professional  
22 as identified in section 3 unless that informa-  
23 tion is only a health insurance policy or sub-  
24 scriber identification number or information re-  
25 garding an individual's medical history, mental

1 or physical medical condition, or medical treat-  
2 ment or diagnosis by a health care professional.

3 **SEC. 213. METHODS OF NOTICE TO INDIVIDUALS.**

4 To comply with section 211, an agency or business  
5 entity shall provide the following forms of notice:

6 (1) **INDIVIDUAL WRITTEN NOTICE.**—Written  
7 notice to individuals by 1 of the following means:

8 (A) Individual written notification to the  
9 last known home mailing address of the indi-  
10 vidual in the records of the agency or business  
11 entity.

12 (B) E-mail notice, unless the individual  
13 has expressly opted not to receive such notices  
14 of security breaches or the notice is inconsistent  
15 with the provisions permitting electronic trans-  
16 mission of notices under section 101 of the  
17 Electronic Signatures in Global and National  
18 Commerce Act (15 U.S.C. 7001).

19 (2) **TELEPHONE NOTICE.**—Telephone notice to  
20 the individual personally.

21 (3) **PUBLIC NOTICE.**—

22 (A) **ELECTRONIC NOTICE.**—Prominent no-  
23 tice via all reasonable means of electronic con-  
24 tact between the individual and the agency or  
25 business entity, including any website,

1 networked devices, or other interface through  
2 which the agency or business entity regularly  
3 interacts with the consumer, if the number of  
4 individuals whose sensitive personally identifi-  
5 able information was or is reasonably believed  
6 to have been accessed or acquired by an unau-  
7 thorized person exceeds 5,000.

8 (B) MEDIA NOTICE.—Notice to major  
9 media outlets serving a State or jurisdiction, if  
10 the number of residents of such State whose  
11 sensitive personally identifiable information  
12 was, or is reasonably believed to have been,  
13 accessed or acquired by an unauthorized person  
14 exceeds 5,000.

15 **SEC. 214. CONTENT OF NOTICE TO INDIVIDUALS.**

16 (a) IN GENERAL.—Regardless of the method by  
17 which individual notice is provided to individuals under  
18 section 213(1), such notice shall include—

19 (1) a description of the categories of sensitive  
20 personally identifiable information that was, or is  
21 reasonably believed to have been, accessed or ac-  
22 quired by an unauthorized person, and how the  
23 agency or business entity came into possession of the  
24 sensitive personally identifiable information at issue;

25 (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 what types of sensitive personally identifiable  
6 information the agency or business entity main-  
7 tained about that individual;

8 (3) the toll-free contact telephone numbers,  
9 websites, and addresses for the major credit report-  
10 ing agencies;

11 (4) the telephone numbers and websites for the  
12 relevant Federal agencies that provide information  
13 regarding identity theft prevention and protection;

14 (5) notice that the individual is entitled to re-  
15 ceive, at no cost to such individual, consumer credit  
16 reports on a quarterly basis for a period of 2 years,  
17 credit monitoring or any other service that enables  
18 consumers to detect the misuse of sensitive person-  
19 ally identifiable information for a period of 2 years,  
20 and instructions to the individual on requesting such  
21 reports or service from the agency or business enti-  
22 ty;

23 (6) notice that the individual is entitled to re-  
24 ceive a security freeze and that the agency or busi-  
25 ness entity will be liable for any costs associated

1 with the security freeze for 2 years and the nec-  
2 essary instructions for requesting a security freeze;  
3 and

4 (7) notice that any costs or damages incurred  
5 by an individual as a result of a security breach will  
6 be paid by the business entity or agency that experi-  
7 enced the security breach.

8 (b) TELEPHONE NOTICE.—Telephone notice de-  
9 scribed in section 213(2) shall include, to the extent pos-  
10 sible—

11 (1) notification that a security breach has oc-  
12 curred and that the individual's sensitive personally  
13 identifiable information may have been com-  
14 promised;

15 (2) a description of the categories of sensitive  
16 personally identifiable information that were, or are  
17 reasonably believed to have been, accessed or ac-  
18 quired by an unauthorized person;

19 (3) a toll-free number and website—

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

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

1           tained about that individual and remedies avail-  
2           able to that individual; and

3           (4) an alert to the individual that the agency or  
4           business entity is sending or has sent written notifi-  
5           cation containing additional information as required  
6           under section 213(1)(A).

7           (c) PUBLIC NOTICE.—Public notice described in sec-  
8           tion 213(3) shall include—

9           (1) electronic notice, which includes—

10           (A) notification that a security breach has  
11           occurred and that the individual’s sensitive per-  
12           sonally identifiable information may have been  
13           compromised;

14           (B) a description of the categories of sen-  
15           sitive personally identifiable information that  
16           were, or are reasonably believed to have been,  
17           accessed or acquired by an unauthorized per-  
18           son; and

19           (C) a toll-free number and website—

20           (i) that the individual may use to con-  
21           tact the agency or business entity, or the  
22           authorized agent of the agency or business  
23           entity; and

24           (ii) from which the individual may  
25           learn what types of sensitive personally

1 identifiable information the agency or busi-  
2 ness entity maintained about that indi-  
3 vidual and remedies available to that indi-  
4 vidual;

5 (2) media notice, which includes—

6 (A) a description of the categories of sen-  
7 sitive personally identifiable information that  
8 was, or is reasonably believed to have been,  
9 accessed or acquired by an unauthorized per-  
10 son;

11 (B) a toll-free number—

12 (i) that the individual may use to con-  
13 tact the agency or business entity, or the  
14 authorized agent of the agency or business  
15 entity; and

16 (ii) from which the individual may  
17 learn what types of sensitive personally  
18 identifiable information the agency or busi-  
19 ness entity maintained about that indi-  
20 vidual and remedies available to that indi-  
21 vidual;

22 (C) the toll-free contact telephone num-  
23 bers, websites, and addresses for the major  
24 credit reporting agencies;

1 (D) the telephone numbers and websites  
2 for the relevant Federal agencies that provide  
3 information regarding identity theft prevention  
4 and protection;

5 (E) notice that the affected individuals are  
6 entitled to receive, at no cost to such individ-  
7 uals, consumer credit reports on a quarterly  
8 basis for a period of 2 years, credit monitoring,  
9 or any other service that enables consumers to  
10 detect the misuse of sensitive personally identi-  
11 fiable information for a period of 2 years;

12 (F) notice that the individual is entitled to  
13 receive a security freeze and that the agency or  
14 business entity will be liable for any costs asso-  
15 ciated with the security freeze for 2 years; and

16 (G) notice that the individual is entitled to  
17 receive compensation from the business entity  
18 or agency for any costs or damages incurred by  
19 the individual resulting from the security  
20 breach.

21 (d) ADDITIONAL CONTENT.—Notwithstanding sec-  
22 tion 221, a State may require that a notice under sub-  
23 section (a) shall also include information regarding victim  
24 protection assistance provided for by that State.

1 (e) DIRECT BUSINESS RELATIONSHIP.—Regardless  
2 of whether a business entity, agency, or a designated third  
3 party provides the notice required pursuant to section  
4 211(b), such notice shall include the name of the business  
5 entity or agency that has a direct relationship with the  
6 individual being notified.

7 **SEC. 215. REMEDIES FOR SECURITY BREACH.**

8 (a) CREDIT REPORTS AND CREDIT MONITORING.—  
9 An agency or business entity required to provide notifica-  
10 tion under this subtitle shall, upon request of an individual  
11 whose sensitive personally identifiable information was in-  
12 cluded in the security breach, provide or arrange for the  
13 provision of, to each such individual and at no cost to such  
14 individual—

15 (1) consumer credit reports from not fewer  
16 than 1 of the major credit reporting agencies begin-  
17 ning not later than 60 days following the request of  
18 the individual and continuing on a quarterly basis  
19 for a period of 2 years thereafter; and

20 (2) a credit monitoring or other service that en-  
21 ables consumers to detect the misuse of their per-  
22 sonal information, beginning not later than 60 days  
23 following the request of the individual and con-  
24 tinuing for a period of 2 years.

25 (b) SECURITY FREEZE.—

1           (1) REQUEST.—Any consumer may submit a  
2 written request, by certified mail or such other se-  
3 cure method as authorized by a credit rating agency,  
4 to a credit rating agency to place a security freeze  
5 on the credit report of the consumer.

6           (2) IMPLEMENTATION OF SECURITY FREEZE.—  
7 Upon receipt of a written request under paragraph  
8 (1), a credit rating agency shall—

9                   (A) not later than 5 business days after re-  
10 ceipt of the request, place a security freeze on  
11 the credit report of the consumer; and

12                   (B) not later than 10 business days after  
13 placing a security freeze, send a written con-  
14 firmation of such security freeze to the con-  
15 sumer, which shall provide the consumer with a  
16 unique personal identification number or pass-  
17 word to be used by the consumer when pro-  
18 viding authorization for the release of the credit  
19 report of the consumer to a third party or for  
20 a specified period of time.

21           (3) DURATION OF SECURITY FREEZE.—Except  
22 as provided in paragraph (4), any security freeze au-  
23 thorized pursuant to the provisions of this section  
24 shall remain in effect until the consumer requests  
25 security freeze to be removed.

1           (4) DISCLOSURE OF CREDIT REPORT TO THIRD  
2 PARTY.—

3           (A) IN GENERAL.—If a consumer that has  
4 requested a security freeze under this sub-  
5 section wishes to authorize the disclosure of the  
6 credit report of the consumer to a third party,  
7 or for a specified period of time, while such se-  
8 curity freeze is in effect, the consumer shall  
9 contact the credit rating agency and provide—

10                   (i) proper identification;

11                   (ii) the unique personal identification  
12 number or password described in para-  
13 graph (2)(B); and

14                   (iii) proper information regarding the  
15 third party who is to receive the credit re-  
16 port or the time period for which the credit  
17 report shall be available.

18           (B) REQUIREMENT.—Not later than 3  
19 business days after receipt of a request under  
20 subparagraph (A), a credit rating agency shall  
21 lift the security freeze.

22           (5) PROCEDURES.—

23           (A) IN GENERAL.—A credit rating agency  
24 shall develop procedures to receive and process

1 requests from consumers under paragraph (2)  
2 of this section.

3 (B) REQUIREMENT.—Procedures developed  
4 under subparagraph (A), at a minimum, shall  
5 include the ability of a consumer to send such  
6 temporary lift or removal request by electronic  
7 mail, letter, telephone, or facsimile.

8 (6) REQUESTS BY THIRD PARTY.—If a third  
9 party requests access to a credit report of a con-  
10 sumer that has been frozen under this subsection  
11 and the consumer has not authorized the disclosure  
12 of the credit report of the consumer to the third  
13 party, the third party may deem such credit applica-  
14 tion as incomplete.

15 (7) DETERMINATION BY CREDIT RATING AGEN-  
16 CY.—

17 (A) IN GENERAL.—A credit rating agency  
18 may refuse to implement or may remove a secu-  
19 rity freeze under this subsection if the agency  
20 determines, in good faith, that—

21 (i) the request for a security freeze  
22 was made as part of a fraud that the con-  
23 sumer participated in, had knowledge of,  
24 or that can be demonstrated by cir-  
25 cumstantial evidence; or

1                   (ii) the consumer credit report was  
2                   frozen due to a material misrepresentation  
3                   of fact by the consumer.

4                   (B) NOTICE.—If a credit rating agency  
5                   makes a determination under subparagraph (A)  
6                   to not implement, or to remove, a security  
7                   freeze under this subsection, the credit rating  
8                   agency shall notify the consumer in writing of  
9                   such determination—

10                   (i) in the case of a determination not  
11                   to implement a security freeze, not later  
12                   than 5 business days after the determina-  
13                   tion is made; and

14                   (ii) in the case of a removal of a secu-  
15                   rity freeze, prior to removing the freeze on  
16                   the credit report of the consumer.

17                   (8) RULE OF CONSTRUCTION.—Nothing in this  
18                   section shall be construed to prohibit disclosure of a  
19                   credit report of a consumer to—

20                   (A) a person, or the person's subsidiary,  
21                   affiliate, agent or assignee with which the con-  
22                   sumer has or, prior to assignment, had an ac-  
23                   count, contract or debtor-creditor relationship  
24                   for the purpose of reviewing the account or col-

1 lecting the financial obligation owing for the ac-  
2 count, contract or debt;

3 (B) a subsidiary, affiliate, agent, assignee  
4 or prospective assignee of a person to whom ac-  
5 cess has been granted under paragraph (4) for  
6 the purpose of facilitating the extension of cred-  
7 it or other permissible use;

8 (C) any person acting pursuant to a court  
9 order, warrant or subpoena;

10 (D) any person for the purpose of using  
11 such credit information to prescreen as provided  
12 by the Fair Credit Reporting Act (15 U.S.C.  
13 1681 et seq.);

14 (E) any person for the sole purpose of pro-  
15 viding a credit file monitoring subscription serv-  
16 ice to which the consumer has subscribed;

17 (F) a credit rating agency for the sole pur-  
18 pose of providing a consumer with a copy of the  
19 credit report of the consumer upon the request  
20 of the consumer; or

21 (G) a Federal, State or local governmental  
22 entity, including a law enforcement agency, or  
23 court, or their agents or assignees pursuant to  
24 their statutory or regulatory duties. For pur-  
25 poses of this subsection, “reviewing the ac-

1           count” includes activities related to account  
2           maintenance, monitoring, credit line increases  
3           and account upgrades and enhancements; and

4           (H) any person for the sole purpose of pro-  
5           viding a remedy requested by an individual  
6           under this section.

7           (9) EXCEPTIONS.—The following persons shall  
8           not be required to place a security freeze under this  
9           subsection, but shall be subject to any security  
10          freeze placed on a credit report by another credit  
11          rating agency:

12           (A) A check services or fraud prevention  
13           services company that reports on incidents of  
14           fraud or issues authorizations for the purpose  
15           of approving or processing negotiable instru-  
16           ments, electronic fund transfers or similar  
17           methods of payment.

18           (B) A deposit account information service  
19           company that issues reports regarding account  
20           closures due to fraud, substantial overdrafts,  
21           automated teller machine abuse, or similar in-  
22           formation regarding a consumer to inquiring  
23           banks or other financial institutions for use  
24           only in reviewing a consumer request for a de-

1           posit account at the inquiring bank or financial  
2           institution.

3           (C) A credit rating agency that—

4                 (i) acts only to resell credit informa-  
5                 tion by assembling and merging informa-  
6                 tion contained in a database of 1 or more  
7                 credit reporting agencies; and

8                 (ii) does not maintain a permanent  
9                 database of credit information from which  
10                new credit reports are produced.

11          (10) FEES.—

12                 (A) IN GENERAL.—A credit rating agency  
13                 may charge reasonable fees for each security  
14                 freeze, removal of such freeze or temporary lift  
15                 of such freeze for a period of time, and a tem-  
16                 porary lift of such freeze for a specific party.

17                 (B) REQUIREMENT.—Any fees charged  
18                 under subparagraph (A) shall be borne by the  
19                 agency or business entity providing notice under  
20                 section 214 for 2 years following the establish-  
21                 ment of the security freeze under this sub-  
22                 section.

23          (c) COSTS RESULTING FROM A SECURITY  
24          BREACH.—

1           (1) IN GENERAL.—A business entity or agency  
2           that experiences a security breach and is required to  
3           provide notice under this subtitle shall pay, upon re-  
4           quest, to any individual whose sensitive personally  
5           identifiable information has been, or is reasonably  
6           believed to have been, accessed or acquired as a re-  
7           sult of such security breach, any costs or damages  
8           incurred by the individual as a result of such secu-  
9           rity breach, including costs associated with identity  
10          theft suffered as a result of such security breach.

11          (2) COMPLIANCE.—A business entity or agency  
12          shall be deemed in compliance with this subsection  
13          if the business entity or agency—

14                (A) provides insurance to any individual  
15                whose sensitive personally identifiable informa-  
16                tion has been, or is reasonably believed to have  
17                been, accessed or acquired as a result of a secu-  
18                rity breach and such insurance is sufficient to  
19                compensate the consumer for not less than  
20                \$25,000 of costs or damages; or

21                (B) pays, without unreasonable delay, any  
22                actual costs or damages incurred by an indi-  
23                vidual as a result of the security breach.

1 **SEC. 216. NOTICE TO CREDIT REPORTING AGENCIES.**

2 If an agency or business entity is required to provide  
3 notification to more than 5,000 individuals under section  
4 211(a), the agency or business entity shall also notify all  
5 consumer reporting agencies that compile and maintain  
6 files on consumers on a nationwide basis (as defined in  
7 section 603(p) of the Fair Credit Reporting Act (15  
8 U.S.C. 1681a(p)) of the timing and distribution of the no-  
9 tices. Such notice shall be given to the consumer credit  
10 reporting agencies without unreasonable delay and, if it  
11 will not delay notice to the affected individuals, prior to  
12 the distribution of notices to the affected individuals.

13 **SEC. 217. NOTICE TO LAW ENFORCEMENT.**

14 (a) DESIGNATION OF A GOVERNMENT ENTITY TO  
15 RECEIVE NOTICE.—

16 (1) IN GENERAL.—Not later than 60 days after  
17 the date of enactment of this Act, the Secretary of  
18 Homeland Security, in consultation with the Attor-  
19 ney General, shall designate a Federal Government  
20 entity to receive the information required to be sub-  
21 mitted under this subtitle, and any other reports and  
22 information about information security incidents,  
23 threats, and vulnerabilities.

24 (2) RESPONSIBILITIES OF THE DESIGNATED  
25 ENTITY.—The designated entity shall—

1           (A) be responsible for promptly providing  
2           the information it receives to the United States  
3           Secret Service and the Federal Bureau of In-  
4           vestigation, and to the Federal Trade Commis-  
5           sion for civil law enforcement purposes; and

6           (B) provide the information described in  
7           subparagraph (A) as appropriate to other Fed-  
8           eral agencies for law enforcement, national se-  
9           curity, or data security purposes.

10       (b) NOTICE.—Any business entity or agency shall no-  
11       tify the designated entity of the fact that a security breach  
12       has occurred if—

13           (1) the number of individuals whose sensitive  
14           personally identifiable information was, or is reason-  
15           ably believed to have been, accessed or acquired by  
16           an unauthorized person exceeds 5,000;

17           (2) the security breach involves a database,  
18           networked or integrated databases, or other data  
19           system containing the sensitive personally identifi-  
20           able information of more than 500,000 individuals  
21           nationwide;

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

24           (4) the security breach involves primarily sen-  
25           sitive personally identifiable information of individ-

1 uals known to the agency or business entity to be  
2 employees and contractors of the Federal Govern-  
3 ment involved in national security or law enforce-  
4 ment.

5 (c) FTC REVIEW OF THRESHOLDS.—

6 (1) REVIEW.—Not later than 1 year after the  
7 date of enactment of this Act, the Federal Trade  
8 Commission, in consultation with the Attorney Gen-  
9 eral and the Secretary of Homeland Security, shall  
10 promulgate regulations regarding the reports re-  
11 quired under subsection (a).

12 (2) RULEMAKING.—The Federal Trade Com-  
13 mission, in consultation with the Attorney General  
14 and the Secretary of Homeland Security, after no-  
15 tice and the opportunity for public comment, and in  
16 a manner consistent with this section, shall promul-  
17 gate regulations, as necessary, under section 553 of  
18 title 5, United States Code, to adjust the thresholds  
19 for notice to law enforcement and national security  
20 authorities under subsection (a) and to facilitate the  
21 purposes of this section.

22 (d) TIMING OF NOTICES.—The notices required  
23 under this section shall be delivered as follows:

1           (1) Notice under subsection (a) shall be deliv-  
2           ered as promptly as possible, but not later than 10  
3           days after discovery of the security breach.

4           (2) Notice under section 211 shall be delivered  
5           to individuals not later than 48 hours after the Fed-  
6           eral Bureau of Investigation or the Secret Service  
7           receives notice of a security breach from an agency  
8           or business entity.

9   **SEC. 218. FEDERAL ENFORCEMENT.**

10   (a) CIVIL ACTIONS BY THE ATTORNEY GENERAL.—

11           (1) IN GENERAL.—The Attorney General may  
12           bring a civil action in the appropriate United States  
13           district court against any business entity that en-  
14           gages in conduct constituting a violation of this sub-  
15           title and, upon proof of such conduct by a prepon-  
16           derance of the evidence, such business entity shall be  
17           subject to a civil penalty of not more than \$500 per  
18           day per individual whose sensitive personally identi-  
19           fiable information was, or is reasonably believed to  
20           have been, accessed or acquired by an unauthorized  
21           person, up to a maximum of \$20,000,000 per viola-  
22           tion, unless such conduct is found to be willful or in-  
23           tentional.

1           (2) PRESUMPTION.—A violation of section  
2           212(b)(2)(C) shall be presumed to be willful or in-  
3           tentional conduct.

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

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

11                   (A) enjoining such act or practice; or

12                   (B) enforcing compliance with this subtitle.

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

17          (c) CIVIL ACTIONS BY THE FEDERAL TRADE COM-  
18          MISSION.—

19          (1) IN GENERAL.—Compliance with the require-  
20          ments imposed under this subtitle may be enforced  
21          under the Federal Trade Commission Act (15  
22          U.S.C. 41 et seq.) by the Federal Trade Commission  
23          with respect to business entities subject to this Act.  
24          All of the functions and powers of the Federal Trade  
25          Commission under the Federal Trade Commission

1 Act are available to the Commission to enforce com-  
2 pliance by any person with the requirements imposed  
3 under this title.

4 (2) UNFAIR OR DECEPTIVE ACTS OR PRAC-  
5 TICES.—For the purpose of the exercise by the Fed-  
6 eral Trade Commission of its functions and powers  
7 under the Federal Trade Commission Act, a viola-  
8 tion of any requirement or prohibition imposed  
9 under this title shall constitute an unfair or decep-  
10 tive act or practice in commerce in violation of a  
11 regulation under section 18(a)(1)(B) of the Federal  
12 Trade Commission Act (15 U.S.C. 57a(a)(I)(B)) re-  
13 garding unfair or deceptive acts or practices and  
14 shall be subject to enforcement by the Federal Trade  
15 Commission under that Act with respect to any busi-  
16 ness entity, irrespective of whether that business en-  
17 tity is engaged in commerce or meets any other ju-  
18 risdictional tests in the Federal Trade Commission.

19 (d) CONSIDERATIONS.—In determining the amount  
20 of a civil penalty under this subsection, the court shall  
21 take into account—

22 (1) the degree of culpability of the business en-  
23 tity;

24 (2) any prior violations of this subtitle by the  
25 business entity;

1           (3) the ability of the business entity to pay a  
2           civil penalty;

3           (4) the effect on the ability of the business enti-  
4           ty to continue to do business;

5           (5) the number of individuals whose sensitive  
6           personally identifiable information was compromised  
7           by the breach;

8           (6) the relative cost of compliance with this  
9           subtitle; and

10          (7) such other matters as justice may require.

11          (e) COORDINATION OF ENFORCEMENT.—

12           (1) IN GENERAL.—Before opening an investiga-  
13           tion, the Federal Trade Commission shall consult  
14           with the Attorney General.

15           (2) LIMITATION.—The Federal Trade Commis-  
16           sion may initiate investigations under this subsection  
17           unless the Attorney General determines that such an  
18           investigation would impede an ongoing criminal in-  
19           vestigation or national security activity.

20           (3) COORDINATION AGREEMENT.—

21           (A) IN GENERAL.—In order to avoid con-  
22           flicts and promote consistency regarding the en-  
23           forcement and litigation of matters under this  
24           Act, not later than 180 days after the enact-  
25           ment of this Act, the Attorney General and the

1 Commission shall enter into an agreement for  
2 coordination regarding the enforcement of this  
3 Act.

4 (B) REQUIREMENT.—The coordination  
5 agreement entered into under subparagraph (A)  
6 shall include provisions to ensure that parallel  
7 investigations and proceedings under this sec-  
8 tion are conducted in a manner that avoids con-  
9 flicts and does not impede the ability of the At-  
10 torney General to prosecute violations of Fed-  
11 eral criminal laws.

12 (4) COORDINATION WITH THE FCC.—If an en-  
13 forcement action under this Act relates to customer  
14 proprietary network information, the Federal Trade  
15 Commission shall coordinate the enforcement action  
16 with the Federal Communications Commission.

17 (f) RULEMAKING.—The Federal Trade Commission  
18 may, in consultation with the Attorney General, issue such  
19 other regulations as it determines to be necessary to carry  
20 out this subtitle. All regulations promulgated under this  
21 Act shall be issued in accordance with section 553 of title  
22 5, United States Code. Where regulations relate to cus-  
23 tomer proprietary network information, the promulgation  
24 of such regulations will be coordinated with the Federal  
25 Communications Commission.

1 (g) OTHER RIGHTS AND REMEDIES.—The rights and  
2 remedies available under this subtitle are cumulative and  
3 shall not affect any other rights and remedies available  
4 under law.

5 (h) FRAUD ALERT.—Section 605A(b)(1) of the Fair  
6 Credit Reporting Act (15 U.S.C. 1681c–1(b)(1)) is  
7 amended by inserting “, or evidence that the consumer  
8 has received notice that the consumer’s financial informa-  
9 tion has or may have been compromised,” after “identity  
10 theft report”.

11 **SEC. 219. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

12 (a) IN GENERAL.—

13 (1) CIVIL ACTIONS.—

14 (A) IN GENERAL.—In any case in which  
15 the attorney general of a State or any State or  
16 local law enforcement agency authorized by the  
17 State attorney general or by State statute to  
18 prosecute violations of consumer protection law,  
19 has reason to believe that an interest of the  
20 residents of that State has been or is threat-  
21 ened or adversely affected by the engagement of  
22 a business entity in a practice that is prohibited  
23 under this subtitle, the State or the State or  
24 local law enforcement agency on behalf of the  
25 residents of the agency’s jurisdiction, may bring

1 a civil action on behalf of the residents of the  
2 State or jurisdiction in a district court of the  
3 United States of appropriate jurisdiction or any  
4 other court of competent jurisdiction, including  
5 a State court, to—

6 (i) enjoin that practice;

7 (ii) enforce compliance with this sub-  
8 title; or

9 (iii) obtain civil penalties of not more  
10 than \$500 per day per individual whose  
11 sensitive personally identifiable information  
12 was, or is reasonably believed to have been,  
13 accessed or acquired by an unauthorized  
14 person, up to a maximum of \$20,000,000  
15 per violation, unless such conduct is found  
16 to be willful or intentional.

17 (B) PRESUMPTION.—A violation of section  
18 212(b)(2)(C) shall be presumed to be willful or  
19 intentional.

20 (2) CONSIDERATIONS.—In determining the  
21 amount of a civil penalty under this subsection, the  
22 court shall take into account—

23 (A) the degree of culpability of the busi-  
24 ness entity;

1 (B) any prior violations of this subtitle by  
2 the business entity;

3 (C) the ability of the business entity to pay  
4 a civil penalty;

5 (D) the effect on the ability of the business  
6 entity to continue to do business;

7 (E) the number of individuals whose sen-  
8 sitive personally identifiable information was  
9 compromised by the breach;

10 (F) the relative cost of compliance with  
11 this subtitle; and

12 (G) such other matters as justice may re-  
13 quire.

14 (3) NOTICE.—

15 (A) IN GENERAL.—Before filing an action  
16 under paragraph (1), the attorney general of  
17 the State involved shall provide to the Attorney  
18 General of the United States—

19 (i) written notice of the action; and

20 (ii) a copy of the complaint for the ac-  
21 tion.

22 (B) EXEMPTION.—

23 (i) IN GENERAL.—Subparagraph (A)  
24 shall not apply with respect to the filing of  
25 an action by an attorney general of a State

1 under this subtitle, if the State attorney  
2 general determines that it is not feasible to  
3 provide the notice described in such sub-  
4 paragraph before the filing of the action.

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

11 (b) FEDERAL PROCEEDINGS.—Upon receiving notice  
12 under subsection (a)(2), the Attorney General shall have  
13 the right to—

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

17 (2) initiate an action in the appropriate United  
18 States district court under section 218 and move to  
19 consolidate all pending actions, including State ac-  
20 tions, in such court;

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

23 (4) file petitions for appeal.

24 (c) PENDING PROCEEDINGS.—If the Attorney Gen-  
25 eral has instituted a proceeding or action for a violation

1 of this subtitle or any regulations thereunder, no attorney  
2 general of a State may, during the pendency of such pro-  
3 ceeding or action, bring an action under this subtitle  
4 against any defendant named in such criminal proceeding  
5 or civil action for any violation that is alleged in that pro-  
6 ceeding or action.

7 (d) CONSTRUCTION.—For purposes of bringing any  
8 civil action under subsection (a), nothing in this subtitle  
9 regarding notification shall be construed to prevent an at-  
10 torney general of a State from exercising the powers con-  
11 ferred on such attorney general by the laws of that State  
12 to—

- 13 (1) conduct investigations;
- 14 (2) administer oaths or affirmations; or
- 15 (3) compel the attendance of witnesses or the  
16 production of documentary and other evidence.

17 (e) VENUE; SERVICE OF PROCESS.—

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

20 (A) the district court of the United States  
21 that meets applicable requirements relating to  
22 venue under section 1391 of title 28, United  
23 States Code; or

24 (B) another court of competent jurisdic-  
25 tion.

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

4                   (A) is an inhabitant; or

5                   (B) may be found.

6 **SEC. 220. SUPPLEMENTAL ENFORCEMENT BY INDIVIDUALS.**

7           (a) IN GENERAL.—Any person aggrieved by a viola-  
8 tion of the provisions of section 211, 213, 214, 215, or  
9 216 by a business entity may bring a civil action in a court  
10 of appropriate jurisdiction to recover for personal injuries  
11 sustained as a result of the violation.

12           (b) AUTHORITY TO BRING CIVIL ACTION; JURISDIC-  
13 TION.—As provided in subsection (c), an individual may  
14 commence a civil action on his own behalf against any  
15 business entity who is alleged to have violated the provi-  
16 sions of this subtitle.

17           (c) REMEDIES IN A CITIZEN SUIT.—

18                   (1) DAMAGES.—Any individual harmed by a  
19 failure of a business entity to comply with the provi-  
20 sions of section 211, 213, 214, 215, or 216, shall be  
21 able to collect damages of not more than \$500 per  
22 day per individual whose sensitive personally identi-  
23 fiable information was, or is reasonably believed to  
24 have been, accessed or acquired by an unauthorized

1 person, up to a maximum of \$20,000,000 per viola-  
2 tion

3 (2) PUNITIVE DAMAGES.—A business entity  
4 may be liable for punitive damages if it—

5 (A) intentionally or willfully violates the  
6 provisions of section 211, 213, 214, 215, or  
7 216; or

8 (B) failed to comply with the requirements  
9 of subsections (a) through (d) of section 202.

10 (3) EQUITABLE RELIEF.—A business entity  
11 that violates the provisions of section 211, 213, 214,  
12 215, or 216 may be enjoined to provide required  
13 remedies under section 215 by a court of competent  
14 jurisdiction.

15 (d) OTHER RIGHTS AND REMEDIES.—The rights and  
16 remedies available under this subsection are cumulative  
17 and shall not affect any other rights and remedies avail-  
18 able under law.

19 (e) NONENFORCEABILITY OF CERTAIN PROVISIONS  
20 WAIVING RIGHTS AND REMEDIES OR REQUIRING ARBI-  
21 TRATION OF DISPUTES.—

22 (1) WAIVER OF RIGHTS AND REMEDIES.—The  
23 rights and remedies provided for in this section may  
24 not be waived by any agreement, policy form, or con-

1        dition of employment including by a predispute arbi-  
2        tration agreement.

3            (2) PREDISPUTE ARBITRATION AGREEMENTS.—

4        No predispute arbitration agreement shall be valid  
5        or enforceable, if the agreement requires arbitration  
6        of a dispute arising under this section.

7            (f) CONSIDERATIONS.—In determining the amount of  
8        a civil penalty under this subsection, the court shall take  
9        into account—

10           (1) the degree of culpability of the business en-  
11           tity;

12           (2) any prior violations of this subtitle by the  
13           business entity;

14           (3) the ability of the business entity to pay a  
15           civil penalty;

16           (4) the effect on the ability of the business enti-  
17           ty to continue to do business;

18           (5) the number of individuals whose sensitive  
19           personally identifiable information was compromised  
20           by the breach;

21           (6) the relative cost of compliance with this  
22           subtitle; and

23           (7) such other matters as justice may require.

1 **SEC. 221. RELATION TO OTHER LAWS.**

2 (a) IN GENERAL.—The provisions of this subtitle  
3 shall supersede any other provision of Federal law or any  
4 provision of law of any State relating to notification by  
5 a business entity engaged in interstate commerce or an  
6 agency of a security breach, except as provided in this sub-  
7 section.

8 (b) LIMITATIONS.—

9 (1) STATE COMMON LAW.—Nothing in this sub-  
10 title shall be construed to exempt any entity from li-  
11 ability under common law, including through the op-  
12 eration of ordinary preemption principles, and in-  
13 cluding liability through state trespass, contract, or  
14 tort law, for damages caused by the failure to notify  
15 an individual following a security breach.

16 (2) GRAMM-LEACH-BLILEY ACT.—Nothing in  
17 this Act shall supersede the data security require-  
18 ments of the Gramm-Leach-Bliley Act (15 U.S.C.  
19 6801 et seq.), or implementing regulations based on  
20 that Act.

21 (3) HEALTH PRIVACY.—

22 (A) To the extent that a business entity  
23 acts as a covered entity or a business associate  
24 under the Health Information Technology for  
25 Economic and Clinical Health Act (42 U.S.C.  
26 17932), and has the obligation to provide

1 breach notification under that Act or its imple-  
2 menting regulations, the requirements of this  
3 Act shall not apply.

4 (B) To the extent that a business entity  
5 acts as a vendor of personal health records, a  
6 third party service provider, or other entity sub-  
7 ject to the Health Information Technology for  
8 Economical and Clinical Health Act (42 U.S.C.  
9 17937), and has the obligation to provide  
10 breach notification under that Act or its imple-  
11 menting regulations, the requirements of this  
12 Act shall not apply.

13 **SEC. 222. AUTHORIZATION OF APPROPRIATIONS.**

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

19 **SEC. 223. REPORTING ON RISK ASSESSMENT EXEMPTIONS.**

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

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

1       ness entities invoking the risk assessment exemption  
2       under section 212(b) and the response of the United  
3       States Secret Service and the Federal Bureau of In-  
4       vestigation to such notices; and

5               (2) the number and nature of security breaches  
6       subject to the national security and law enforcement  
7       exemptions under section 212(a), provided that such  
8       report may not disclose the contents of any risk as-  
9       sessment provided to the United States Secret Serv-  
10      ice and the Federal Bureau of Investigation pursu-  
11      ant to this subtitle.

12      **Subtitle C—Post-Breach Technical**  
13      **Information Clearinghouse**

14      **SEC. 230. CLEARINGHOUSE INFORMATION COLLECTION,**  
15      **MAINTENANCE, AND ACCESS.**

16      (a) IN GENERAL.—The designated entity shall main-  
17      tain a clearinghouse of technical information concerning  
18      system vulnerabilities identified in the wake of security  
19      breaches, which shall—

20               (1) contain information disclosed by agencies or  
21      business entities under subsection (b); and

22               (2) be accessible to certified entities under sub-  
23      section (c).

24      (b) POST-BREACH TECHNICAL NOTIFICATION.—In  
25      any instance where an agency or business entity is re-

1 quired to notify the designated entity under section 217,  
2 the agency or business entity shall also provide the des-  
3 ignated entity with technical information concerning the  
4 nature of the security breach, including—

5 (1) technical information regarding any system  
6 vulnerabilities of the agency or business entity re-  
7 vealed by or identified as a consequence of the secu-  
8 rity breach;

9 (2) technical information regarding any system  
10 vulnerabilities of the agency or business entity actu-  
11 ally exploited during the security breach; and

12 (3) any other technical information concerning  
13 the nature of the security breach deemed appro-  
14 priate for collection by the designated entity in fur-  
15 therance of this subtitle.

16 (c) ACCESS TO CLEARINGHOUSE.—Any entity cer-  
17 tified under subsection (d) may review information main-  
18 tained by the technical information clearinghouse for the  
19 purpose of preventing security breaches that threaten the  
20 security of sensitive personally identifiable information.

21 (d) CERTIFICATION FOR ACCESS.—The designated  
22 entity shall issue and revoke certifications to agencies and  
23 business entities wishing to review information maintained  
24 by the technical information clearinghouse and shall estab-  
25 lish conditions for obtaining and maintaining such certifi-

1 cations, including agreement that any information ob-  
2 tained directly or derived indirectly from the review of in-  
3 formation maintained by the technical information clear-  
4 inghouse—

5 (1) shall only be used to improve the security  
6 and reduce the vulnerability of networks that collect,  
7 access, transmit, use, store, or dispose of sensitive  
8 personally identifiable information;

9 (2) may not be used for any competitive com-  
10 mercial purpose; and

11 (3) may not be shared with any third party, in-  
12 cluding other parties certified for access to the infor-  
13 mation clearinghouse, without the express written  
14 consent of the designated entity.

15 (e) RULEMAKING.—In consultation with the private  
16 sector, appropriate representatives of State and local gov-  
17 ernments, and other appropriate Federal agencies, the  
18 designated entity may issue such regulations as it deter-  
19 mines to be necessary to carry out this subtitle. All regula-  
20 tions promulgated under this Act shall be issued in accord-  
21 ance with section 553 of title 5, United States Code.

22 **SEC. 231. PROTECTIONS FOR CLEARINGHOUSE PARTICI-**  
23 **PANTS.**

24 (a) PROTECTION OF PROPRIETARY INFORMATION.—  
25 To the extent feasible, the designated entity shall ensure

1 that any technical information disclosed to the designated  
2 entity under this subtitle shall be stored in a format de-  
3 signed to protect proprietary business information from  
4 inadvertent disclosure.

5 (b) ANONYMOUS DATA RELEASE.—To the extent fea-  
6 sible, the designated entity shall ensure that all informa-  
7 tion stored in the technical information clearinghouse and  
8 accessed by certified parties is presented in a form that  
9 minimizes the potential for such information to be traced  
10 to a particular network, company, or security breach inci-  
11 dent.

12 (c) PROTECTION FROM PUBLIC DISCLOSURE.—Ex-  
13 cept as otherwise provided in this subtitle—

14 (1) security and vulnerability information col-  
15 lected under this section and provided to the Federal  
16 Government, including aggregated analysis and data,  
17 shall be exempt from disclosure under section  
18 552(b)(3) of title 5, United States Code; and

19 (2) under section 230(e), security and vulner-  
20 ability-related information provided to the Federal  
21 Government under this section, including aggregated  
22 analysis and data, shall be protected from public dis-  
23 closure, except that this paragraph—

24 (A) does not prohibit the sharing of such  
25 information, as the designated entity deter-

1 mines to be appropriate, in order to mitigate  
2 cybersecurity threats or further the official  
3 functions of a government agency; and

4 (B) does not authorized such information  
5 to be withheld from a committee of Congress  
6 authorized to request the information.

7 (d) PROTECTION OF CLASSIFIED INFORMATION.—  
8 Nothing in this subtitle permits the unauthorized dislo-  
9 sure of classified information.

10 **SEC. 232. 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 III—ACCESS TO AND USE**  
15 **OF COMMERCIAL DATA**

16 **SEC. 301. GENERAL SERVICES ADMINISTRATION REVIEW**  
17 **OF CONTRACTS.**

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

23 (1) the data privacy and security program of a  
24 data broker to ensure the privacy and security of  
25 data containing sensitive personally identifiable in-

1 formation, including whether such program ade-  
2 quately addresses privacy and security threats cre-  
3 ated by malicious software or code, or the use of  
4 peer-to-peer file sharing software;

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

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

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

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

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

1 ating sensitive personally identifiable information, the Ad-  
2 ministrator 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 II; or

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

10 (2) require a data broker that engages service  
11 providers not subject to subtitle A of title II 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 sensitive personally identifiable  
17 information;

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 sensitive personally  
22 identifiable 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 II.

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. 302. 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 sen-  
21 sitive personally identifiable information (as that  
22 term is defined in section 3 of the Personal Data  
23 Protection and Breach Accountability Act of 2011)  
24 and ensuring remedial action to address any signifi-  
25 cant deficiencies.”.

1 **SEC. 303. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT**  
2 **USE OF COMMERCIAL INFORMATION SERV-**  
3 **ICES CONTAINING SENSITIVE PERSONALLY**  
4 **IDENTIFIABLE 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 (2) in subparagraph (A)(ii), by striking the pe-  
9 riod and inserting “; or”; and

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

11 “(iii) purchasing or subscribing for a  
12 fee to sensitive personally identifiable in-  
13 formation from a data broker (as such  
14 terms are defined in section 3 of the Per-  
15 sonal Data Protection and Breach Ac-  
16 countability 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 sensitive personally identifiable in-  
22 formation concerning United States persons (other than  
23 news reporting or telephone directories) unless the head  
24 of such department 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 sensitive personally identifiable information  
15 accessed, analyzed, or used is the minimum nec-  
16 essary to accomplish the intended legitimate  
17 purpose of the Federal agency;

18 (D) standards limiting the retention and  
19 redisclosure of sensitive personally identifiable  
20 information 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 II  
20 of this Act; or

21 (ii) if the entity knows or has reason  
22 to know that the sensitive personally iden-  
23 tifiable information being provided to the  
24 Federal department or agency is inac-

1 curate, and provides such inaccurate infor-  
2 mation; and

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

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

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

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

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

25 (d) STUDY OF GOVERNMENT USE.—

1           (1) SCOPE OF STUDY.—Not later than 180  
2           days after the date of enactment of this Act, the  
3           Comptroller General of the United States shall con-  
4           duct a study and audit and prepare a report on Fed-  
5           eral agency actions to address the recommendations  
6           in the Government Accountability Office’s April  
7           2006 report on agency adherence to key privacy  
8           principles in using data brokers or commercial data-  
9           bases containing sensitive personally identifiable in-  
10          formation.

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

13 **SEC. 304. FBI REPORT ON REPORTED BREACHES AND COM-**  
14 **PLIANCE.**

15          (a) IN GENERAL.—Not later than 1 year after the  
16          date of enactment of this Act, and each year thereafter,  
17          the Federal Bureau of Investigation, in coordination with  
18          the Secret Service, shall submit to the Committee on the  
19          Judiciary of the Senate and the Committee on the Judici-  
20          ary of the House of Representatives a report regarding  
21          any reported breaches at agencies or business entities dur-  
22          ing the preceding year.

23          (b) REPORT CONTENT.—Such reporting shall in-  
24          clude—

1           (1) the total instances of breaches of security in  
2           the previous year;

3           (2) the percentage of breaches described in sub-  
4           section (a) that occurred at an agency or business  
5           entity that did not comply with the personal data  
6           privacy and security program under section 202; and

7           (3) recommendations, if any, for modifying or  
8           amending this Act to increase its effectiveness.

9   **SEC. 305. DEPARTMENT OF JUSTICE REPORT ON ENFORCE-**  
10                                   **MENT ACTIONS.**

11           Section 529 of title 28, United States Code, is  
12           amended by adding at the end the following:

13           “(c) Not later than 1 year after the date of enactment  
14           of the Personal Data Protection and Breach Account-  
15           ability Act of 2011, and every fiscal year thereafter, the  
16           Attorney General shall submit to Congress a report on  
17           Federal enforcement actions, State attorneys general en-  
18           forcement actions, and private enforcement actions, un-  
19           dertaken pursuant to the Personal Data Protection and  
20           Breach Accountability Act of 2011 that shall include a de-  
21           scription of the best practices for enforcement of such Act  
22           as well as recommendations, if any, for modifying or  
23           amending this Act to increase the effectiveness of such en-  
24           forcement actions.”.

1 **SEC. 306. REPORT ON NOTIFICATION EFFECTIVENESS.**

2 (a) IN GENERAL.—Not later than 1 year after the  
3 date of enactment of this Act, and each year thereafter,  
4 the designated entity, in coordination with the Attorney  
5 General and the Federal Trade Commission, shall submit  
6 to the Committee on the Judiciary of the Senate and the  
7 Committee on the Judiciary of the House of Representa-  
8 tives a report regarding the effectiveness of post-breach  
9 notification practices by agencies and business entities.

10 (b) REPORT CONTENT.—The report required under  
11 subsection (a) shall include—

12 (1) in each instance of a breach of security, the  
13 amount of time between the instance of the breach  
14 and the discovery of the breach by the affected busi-  
15 ness entity;

16 (2) in each instance of a breach of security, the  
17 amount of time between the discovery of the breach  
18 by the affected business entity and the notification  
19 to the FBI and Secret Service; and

20 (3) in each instance of a breach of security, the  
21 amount of time between the discovery of the breach  
22 by the affected business entity and the notification  
23 to individuals whose sensitive personally identifiable  
24 information was compromised.

1     **TITLE IV—COMPLIANCE WITH**  
2     **STATUTORY PAY-AS-YOU-GO ACT**

3     **SEC. 401. BUDGET COMPLIANCE.**

4           The budgetary effects of this Act, for the purpose of  
5 complying with the Statutory Pay-As-You-Go Act of 2010,  
6 shall be determined by reference to the latest statement  
7 titled “Budgetary Effects of PAYGO Legislation” for this  
8 Act, submitted for printing in the Congressional Record  
9 by the Chairman of the Senate Budget Committee, pro-  
10 vided that such statement has been submitted prior to the  
11 vote on passage.