

113TH CONGRESS  
2D SESSION

# S. 1995

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.

---

IN THE SENATE OF THE UNITED STATES

FEBRUARY 4, 2014

Mr. BLUMENTHAL (for himself and Mr. MARKEY) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

## A BILL

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.

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

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

2 (a) SHORT TITLE.—This Act may be cited as the  
 3 “Personal Data Protection and Breach Accountability Act  
 4 of 2014”.

5 (b) TABLE OF CONTENTS.—The table of contents of  
 6 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 people in the United States;

12 (3) over 9,300,000 individuals were victims of  
 13 identity theft in the United States in 2010;

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

17 (5) it is important for business entities that  
 18 own, use, or license personally identifiable informa-  
 19 tion to adopt reasonable procedures to ensure the se-

1       curity, privacy, and confidentiality of that personally  
2       identifiable information;

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

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

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

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

21          (10) because government use of commercial  
22      data containing personal information potentially af-  
23      fects individual privacy, and law enforcement and  
24      national security operations, there is a need for Con-

1       gress to exercise oversight over government use of  
2       commercial data;

3               (11) over 22,960,000 cases of data breaches in-  
4       volving personally identifiable information were re-  
5       ported through July of 2011, and in 2009 through  
6       2010, over 230,900,000 cases of personal data  
7       breaches were reported;

8               (12) facilitating information sharing among  
9       business entities and across sectors in the event of  
10      a breach can assist in remediating the breach and  
11      preventing similar breaches in the future;

12              (13) because the Federal Government has lim-  
13      ited resources, consumers themselves play a vital  
14      and complementary role in facilitating prompt notifi-  
15      cation and protecting against future breaches of se-  
16      curity;

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

1           (15) victims of personal data breaches may suf-  
2           fer debilitating emotional and physical effects and  
3           become depressed or anxious, especially in cases of  
4           repeated or unresolved instances of data breaches.

5 **SEC. 3. DEFINITIONS.**

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

8           (1) AFFILIATE.—The term “affiliate” means  
9           persons related by common ownership or by cor-  
10          porate control.

11          (2) AGENCY.—The term “agency” has the  
12          meaning given the term in section 551 of title 5,  
13          United States Code.

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

19          (4) CREDIT RATING AGENCY.—The term “cred-  
20          it rating agency” has the meaning given the term in  
21          section 3(a)(61) of the Securities Exchange Act of  
22          1934 (15 U.S.C. 78c(a)(61)).

23          (5) CREDIT REPORT.—The term “credit report”  
24          means a consumer report, as that term is defined in

1 section 603(d) of the Fair Credit Reporting Act (15  
2 U.S.C. 1681a(d)).

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

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

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

16 (A) means the protection of data in elec-  
17 tronic form, in storage or in transit, using an  
18 encryption technology that has been generally  
19 accepted by experts in the field of information  
20 security that renders such data indecipherable  
21 in the absence of associated cryptographic keys  
22 necessary to enable decryption of such data;  
23 and

1 (B) includes appropriate management and  
2 safeguards of such cryptographic keys so as to  
3 protect the integrity of the encryption.

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

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

9 (A) The Office of the Director of National  
10 Intelligence.

11 (B) The Central Intelligence Agency.

12 (C) The National Security Agency.

13 (D) The Defense Intelligence Agency.

14 (E) The National Geospatial-Intelligence  
15 Agency.

16 (F) The National Reconnaissance Office.

17 (G) Other offices within the Department of  
18 Defense for the collection of specialized national  
19 intelligence through reconnaissance programs.

20 (H) The intelligence elements of the Army,  
21 the Navy, the Air Force, the Marine Corps, the  
22 Federal Bureau of Investigation, and the De-  
23 partment of Energy.

24 (I) The Bureau of Intelligence and Re-  
25 search of the Department of State.



1           (J) The Office of Intelligence and Analysis  
2 of the Department of the Treasury.

3           (K) The elements of the Department of  
4 Homeland Security concerned with the analysis  
5 of intelligence information, including the Office  
6 of Intelligence of the Coast Guard.

7           (L) Such other elements of any other de-  
8 partment or agency as may be designated by  
9 the President, or designated jointly by the Di-  
10 rector of National Intelligence and the head of  
11 the department or agency concerned, as an ele-  
12 ment of the intelligence community.

13           (11) PREDISPUTE ARBITRATION AGREEMENT.—  
14 The term “predispute arbitration agreement” means  
15 any agreement to arbitrate a dispute that had not  
16 yet arisen at the time of the making of the agree-  
17 ment.

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

1 personally identifiable information in records avail-  
2 able to the public.

3 (13) SECURITY BREACH.—

4 (A) IN GENERAL.—The term “security  
5 breach” means compromise of the security, con-  
6 fidentiality, or integrity of, or the loss of, com-  
7 puterized data through misrepresentation or ac-  
8 tions that result in, or that there is a reason-  
9 able basis to conclude has resulted in—

10 (i) the unauthorized acquisition of  
11 sensitive personally identifiable informa-  
12 tion; or

13 (ii) access to sensitive personally iden-  
14 tifiable information that is for an unau-  
15 thorized purpose, or in excess of authoriza-  
16 tion.

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

19 (i) a good faith acquisition of sensitive  
20 personally identifiable information by a  
21 business entity or agency, or an employee  
22 or agent of a business entity or agency, if  
23 the sensitive personally identifiable infor-  
24 mation is not subject to further unauthor-  
25 ized disclosure;

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

6 (iii) any lawfully authorized criminal  
7 investigation or authorized investigative,  
8 protective, or intelligence activities that are  
9 carried out by or on behalf of any element  
10 of the intelligence community and con-  
11 ducted in accordance with the United  
12 States laws, authorities, and regulations  
13 governing such intelligence activities.

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

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

1 (A) An individual's first and last name or  
2 first initial and last name in combination with  
3 any 2 of the following data elements:

4 (i) Home address.

5 (ii) Telephone number of the indi-  
6 vidual.

7 (iii) Mother's maiden name.

8 (iv) Month, day, and year of birth.

9 (B) A non-truncated social security num-  
10 ber, driver's license number, passport number,  
11 or alien registration number or other govern-  
12 ment-issued unique identification number.

13 (C) Information about an individual's geo-  
14 graphic location that is in whole or in part gen-  
15 erated by or derived from that individual's use  
16 of a wireless communication device or other  
17 electronic device, excluding telephone and in-  
18 strument numbers and network or Internet  
19 Protocol addresses.

20 (D) Unique biometric data such as a fin-  
21 gerprint, voice print, face print, a retina or iris  
22 image, or any other unique physical representa-  
23 tion.

24 (E) A unique account identifier, including  
25 a financial account number or credit or debit

1 card number, electronic identification number,  
2 user name, health insurance policy or subscriber  
3 identification number, or routing code.

4 (F) Not less than 2 of the following data  
5 elements:

6 (i) An individual's first and last name  
7 or first initial and last name.

8 (ii) A unique account identifier, in-  
9 cluding a financial account number or  
10 credit or debit card number, electronic  
11 identification number, user name, or rout-  
12 ing code.

13 (iii) Any security code, access code, or  
14 password, or source code that could be  
15 used to generate such codes and pass-  
16 words.

17 (iv) Information regarding an individ-  
18 ual's medical history, mental or physical  
19 medical condition, or medical treatment or  
20 diagnosis by a health care professional.

21 (G) Any other combination of data ele-  
22 ments that could allow unauthorized access to  
23 or acquisition of the information described in  
24 subparagraph (A), (B), (C), (D), (E), or (F),  
25 including—

- 1 (i) a unique account identifier;  
2 (ii) an electronic identification num-  
3 ber;  
4 (iii) a user name;  
5 (iv) a routing code; or  
6 (v) any associated security code, ac-  
7 cess code, or password or any associated  
8 security questions and answers that could  
9 allow unauthorized access to the account.

10 (16) SERVICE PROVIDER.—

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

13 (i) provides electronic data trans-  
14 mission, routing, intermediate and tran-  
15 sient storage, or connections to the system  
16 or network of the business entity;

17 (ii) is not the sender or the intended  
18 recipient of the data;

19 (iii) is not ordinarily expected to select  
20 or modify the content of the electronic  
21 data; and

22 (iv) transmits, routes, stores, or pro-  
23 vides connections for personal information  
24 in a manner that personal information is  
25 undifferentiated from other types of data

1           that such business entity transmits, routes,  
2           stores, or provides connections.

3           (B) SAVINGS CLAUSE.—Any such business  
4           entity shall be treated as a service provider  
5           under this Act only to the extent that the busi-  
6           ness entity is engaged in the provision of the  
7           transmission, routing, intermediate and tran-  
8           sient storage or connections described in sub-  
9           paragraph (A).

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

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

6 **SEC. 101. CONCEALMENT OF SECURITY BREACHES INVOLV-**  
7 **ING SENSITIVE PERSONALLY IDENTIFIABLE**  
8 **INFORMATION.**

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

12 **“§ 1041. Concealment of security breaches involving**  
13 **sensitive personally identifiable informa-**  
14 **tion**

15 “(a) Whoever, having knowledge of a security breach  
16 and of the fact that notice of such security breach is re-  
17 quired under title II of the Personal Data Protection and  
18 Breach Accountability Act of 2014, intentionally or will-  
19 fully conceals the fact of such security breach and which  
20 breach, shall, in the event that such security breach results  
21 in economic harm or substantial emotional distress to 1  
22 or more persons, shall be fined under this title or impris-  
23 oned not more than 5 years, or both.



1       “(b) For purposes of subsection (a), the term ‘person’  
2 has the meaning given the term in section 1030(e)(12)  
3 of title 18, United States Code.

4       “(c) Any person seeking an exemption under section  
5 212(b) of the Personal Data Protection and Breach Ac-  
6 countability Act of 2014 shall be immune from prosecution  
7 under this section if the United States Secret Service does  
8 not indicate, in writing, that such notice be given under  
9 section 212(b)(1)(B) of the Personal Data Protection and  
10 Breach Accountability Act of 2014.”.

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

“1041. Concealment of security breaches involving sensitive personally identifiable information.”.

15       (c) ENFORCEMENT AUTHORITY.—

16           (1) IN GENERAL.—The United States Secret  
17 Service and the Federal Bureau of Investigation  
18 shall have the authority to investigate offenses under  
19 section 1041 of title 18, United States Code, as  
20 added by subsection (a).

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

1 **SEC. 102. UNAUTHORIZED MANIPULATION OF INTERNET**  
2 **TRAFFIC ON A USER'S COMPUTER.**

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

6 (b) PROHIBITION.—

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

15 (A) bypass the display of search engine re-  
16 sults and redirect web searches or queries en-  
17 tered by an authorized user of a protected com-  
18 puter directly to a commercial website, counter-  
19 feit web page, or targeted advertisement and  
20 derive an economic benefit from such activity;  
21 or

22 (B) monitor, manipulate, aggregate, and  
23 market the data collected in the process of  
24 intercepting a web search or query entered by  
25 an authorized user of a protected computer and  
26 derive an economic benefit from such activity.

1           (2) CONSENT.—A service provider may not re-  
2       require consent to perform the collection of data de-  
3       scribed in paragraph (1) as a condition of providing  
4       service to an authorized user of the protected com-  
5       puter.

6           (c) LIMITATIONS ON LIABILITY.—The restrictions  
7       imposed under this section do not apply to any monitoring  
8       of, or interaction with, a subscriber’s Internet or other  
9       network connection or service, or a protected computer,  
10      by or at the direction of a telecommunications carrier,  
11      cable operator, computer hardware or software provider,  
12      financial institution or provider of information services or  
13      interactive computer service for—

- 14           (1) network or computer security purposes;
- 15           (2) diagnostics;
- 16           (3) technical support;
- 17           (4) repair;
- 18           (5) network management;
- 19           (6) authorized updates of software or system  
20      firmware;
- 21           (7) authorized remote system management;
- 22           (8) authorized provision of protection for users  
23      of the computer from objectionable content;

1           (9) authorized scanning for computer software  
2 used in violation of this section for removal by an  
3 authorized user; or

4           (10) detection or prevention of fraud.

5       (d) ENFORCEMENT BY THE ATTORNEY GENERAL.—

6           (1) LIABILITY AND PENALTY FOR VIOLA-  
7 TIONS.—Any person who engages in an activity in  
8 violation of this section shall be fined not more than  
9 \$500,000.

10          (2) ENHANCED LIABILITY AND PENALTIES FOR  
11 PATTERN OR PRACTICE OF VIOLATIONS.—

12           (A) IN GENERAL.—Any person who en-  
13 engages in a pattern or practice of activity that  
14 violates the provisions of this section shall be  
15 fined not more than \$1,000,000.

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

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

24           (A) the degree of culpability of the defend-  
25 ant;

1 (B) any history of prior such conduct;

2 (C) the ability of the defendant to pay any  
3 fine imposed;

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

6 (E) such other matters as justice may re-  
7 quire.

8 **TITLE II—PRIVACY AND SECU-**  
9 **RITY OF SENSITIVE PERSON-**  
10 **ALLY IDENTIFIABLE INFOR-**  
11 **MATION**

12 **Subtitle A—A Data Privacy and**  
13 **Security Program**

14 **SEC. 201. PURPOSE AND APPLICABILITY OF DATA PRIVACY**  
15 **AND SECURITY PROGRAM.**

16 (a) PURPOSE.—The purpose of this subtitle is to en-  
17 sure standards for developing and implementing adminis-  
18 trative, technical, and physical safeguards to protect the  
19 security of sensitive personally identifiable information.

20 (b) IN GENERAL.—A business entity engaging in  
21 interstate commerce that involves collecting, accessing,  
22 transmitting, using, storing, or disposing of sensitive per-  
23 sonally identifiable information in electronic or digital  
24 form on 10,000 or more United States persons is subject  
25 to the requirements for a data privacy and security pro-

1 gram under section 202 for protecting sensitive personally  
2 identifiable information.

3 (c) LIMITATIONS.—Notwithstanding any other obli-  
4 gation under this subtitle, this subtitle does not apply to  
5 the following:

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

20 (2) HIPAA REGULATED ENTITIES.—

21 (A) COVERED ENTITIES.—A business enti-  
22 ty subject to the Health Insurance Portability  
23 and Accountability Act of 1996 (42 U.S.C.  
24 1301 et seq.), including the data security re-

1            requirements and implementing regulations of  
2            that Act.

3            (B) COMPLIANCE.—A business entity  
4            that—

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

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

21            (3) SERVICE PROVIDERS.—A service provider  
22            for any electronic communication by a third party,  
23            to the extent that the service provider is exclusively  
24            engaged in the transmission, routing, or temporary,

1 intermediate, or transient storage of that commu-  
2 nication.

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

8 (d) RULE OF CONSTRUCTION.—Nothing in this sub-  
9 title shall be construed to modify, limit, or supersede the  
10 operation of the provisions of the Gramm-Leach-Bliley Act  
11 (15 U.S.C. 6801 et seq.), or its implementing regulations,  
12 including such regulations adopted or enforced by the  
13 States.

14 **SEC. 202. REQUIREMENTS FOR A PERSONAL DATA PRIVACY**  
15 **AND SECURITY PROGRAM.**

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

24 (1) SCOPE.—A business entity shall implement  
25 a comprehensive personal data privacy and security



1 program that includes administrative, technical, and  
2 physical safeguards appropriate to the size and com-  
3 plexity of the business entity and the nature and  
4 scope of its activities.

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

7 (A) ensure the privacy, security, and con-  
8 fidentiality of sensitive personally identifiable  
9 information;

10 (B) protect against any anticipated  
11 vulnerabilities to the privacy, security, or integ-  
12 rity of sensitive personally identifiable informa-  
13 tion; and

14 (C) protect against unauthorized access to  
15 or use of sensitive personally identifiable infor-  
16 mation that could create a significant risk of  
17 harm to any individual.

18 (3) RISK ASSESSMENT.—A business entity  
19 shall—

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

1 (B) assess the likelihood of and potential  
2 damage from unauthorized access, disclosure,  
3 use, or alteration of sensitive personally identifi-  
4 able information;

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

10 (D) assess the vulnerability of sensitive  
11 personally identifiable information during de-  
12 struction and disposal of such information, in-  
13 cluding through the disposal or retirement of  
14 hardware.

15 (4) RISK MANAGEMENT AND CONTROL.—Each  
16 business entity shall—

17 (A) design its personal data privacy and  
18 security program to control the risks identified  
19 under paragraph (3); and

20 (B) adopt measures commensurate with  
21 the sensitivity of the data as well as the size,  
22 complexity, and scope of the activities of the  
23 business entity that—

24 (i) control access to systems and fa-  
25 cilities containing sensitive personally iden-

1 tifiable information, including controls to  
2 authenticate and permit access only to au-  
3 thorized individuals;

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

11 (iii) protect sensitive personally identi-  
12 fiable information during use, trans-  
13 mission, storage, and disposal by  
14 encryption, redaction, or access controls  
15 that are widely accepted as an effective in-  
16 dustry practice or industry standard, or  
17 other reasonable means (including as di-  
18 rected for disposal of records under section  
19 628 of the Fair Credit Reporting Act (15  
20 U.S.C. 1681w) and the implementing regu-  
21 lations of such Act as set forth in section  
22 682 of title 16, Code of Federal Regula-  
23 tions);

24 (iv) ensure that sensitive personally  
25 identifiable information is properly de-

1           stroyed and disposed of, including during  
2           the destruction of computers, diskettes,  
3           and other electronic media that contain  
4           sensitive personally identifiable informa-  
5           tion;

6           (v) trace access to records containing  
7           sensitive personally identifiable information  
8           so that the business entity can determine  
9           who accessed or acquired such sensitive  
10          personally identifiable information per-  
11          taining to specific individuals;

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

20          (vii) minimize the amount of personal  
21          information maintained by the business en-  
22          tity, providing for the retention of such  
23          personal information only as reasonably  
24          needed for the business purposes of the

1 business entity or as necessary to comply  
2 with any other provision of law.

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

7 (c) VULNERABILITY TESTING.—

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

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

18 (d) CERTAIN RELATIONSHIP TO PROVIDERS OF  
19 SERVICES.—In the event a business entity subject to this  
20 subtitle engages a person or entity not subject to this sub-  
21 title (other than a service provider) to receive sensitive  
22 personally identifiable information in performing services  
23 or functions (other than the services or functions provided  
24 by a service provider) on behalf of and under the instruc-  
25 tion of such business entity, such business entity shall—

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

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

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

20                 (1) technology;

21                 (2) the sensitivity of sensitive personally identi-  
22                 fiable information;

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

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

3           (A) mergers and acquisitions;

4           (B) alliances and joint ventures;

5           (C) outsourcing arrangements;

6           (D) bankruptcy; and

7           (E) changes to sensitive personally identifi-  
8 able information systems.

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

14 **SEC. 203. FEDERAL ENFORCEMENT.**

15           (a) CIVIL PENALTIES.—

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

1 less such conduct is found to be willful or inten-  
2 tional.

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

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

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

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

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

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

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

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

24 (G) such other matters as justice may re-  
25 quire.



1 (b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-  
2 ERAL.—

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

8 (A) enjoining such act or practice; or

9 (B) enforcing compliance with this subtitle.

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

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

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

19 (a) CIVIL ACTIONS.—

20 (1) IN GENERAL.—In any case in which the at-  
21 torney general of a State or any State or local law  
22 enforcement agency authorized by the State attorney  
23 general or by State statute to prosecute violations of  
24 consumer protection law, has reason to believe that  
25 an interest of the residents of that State has been

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

7 (A) enjoin that act or practice;

8 (B) enforce compliance with this subtitle;

9 or

10 (C) obtain civil penalties of not more than  
11 \$5,000 per violation per day while such viola-  
12 tions persist, up to a maximum of \$20,000,000  
13 per violation.

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

17 (A) the degree of culpability of the busi-  
18 ness entity;

19 (B) any prior violations of this subtitle by  
20 the business entity;

21 (C) the ability of the business entity to pay  
22 a civil penalty;

23 (D) the effect on the ability of the business  
24 entity to continue to do business;

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

4 (F) the relative cost of compliance with  
5 this subtitle; and

6 (G) such other matters as justice may re-  
7 quire.

8 (3) NOTICE.—

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

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

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

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

23 (C) NOTIFICATION WHEN PRACTICABLE.—

24 In an action described in subparagraph (B), the  
25 attorney general of a State shall provide the

1           written notice and a copy of the complaint to  
2           the Attorney General as soon after the filing of  
3           the complaint as practicable.

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

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

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

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

16           (4) file petitions for appeal.

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

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

6 (1) conduct investigations;

7 (2) administer oaths or affirmations; or

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

10 (e) VENUE; SERVICE OF PROCESS.—

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

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

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

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

22 (A) is an inhabitant; or

23 (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.—Except as provided in section 212,  
13 any agency, or business entity engaged in interstate com-  
14 merce other than a service provider, that uses, accesses,  
15 transmits, stores, disposes of or collects sensitive person-  
16 ally identifiable information that experiences a security  
17 breach of such information, shall, following the discovery  
18 of such security breach of such information, notify any  
19 resident of the United States whose sensitive personally  
20 identifiable information has been, or is reasonably believed  
21 to have been, accessed, or acquired.

22           (b) OBLIGATION OF OWNER OR LICENSEE.—

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



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

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

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

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

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

12 (c) TIMELINESS OF NOTIFICATION.—

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

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

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

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

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

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

1 that experienced the breach. The notification shall  
2 specify in writing the period of delay required.

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

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

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

17 (a) EXEMPTION FOR NATIONAL SECURITY AND LAW  
18 ENFORCEMENT.—

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

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

1           ernment to conduct law enforcement investiga-  
2           tions; or

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

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

11         (b) SAFE HARBOR.—

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

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

23                           (B) the Federal Trade Commission or des-  
24                           ignated entity does not indicate within 7 busi-  
25                           ness days from the receipt of written notifica-

1           tion from an agency or business entity pursuant  
2           to subsection 212(b)(2), that the agency or  
3           business entity should not be exempt from the  
4           notice requirements of section 211.

5           (2) RISK ASSESSMENT REQUIREMENTS.—

6                 (A) CONDUCTING A RISK ASSESSMENT.—

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

15                 (i) PRESUMPTION OF NO SIGNIFICANT

16                 RISK.—It is presumed that there is no sig-  
17                 nificant risk that the security breach has  
18                 resulted in, or will result in, harm to the  
19                 individuals whose sensitive personally iden-  
20                 tifiable data was subject to the security  
21                 breach, if the sensitive personally identifi-  
22                 able information has been rendered unus-  
23                 able, unreadable, or indecipherable through  
24                 a security technology or methodology (if  
25                 the technology or methodology is generally

1 accepted by experts in the information se-  
2 curity field). Any such presumption may be  
3 rebutted by facts demonstrating that the  
4 security technologies or methodologies in a  
5 specific case, have been or are reasonably  
6 likely to be compromised.

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

20 (iii) METHODOLOGIES OR TECH-  
21 NOLOGIES.—

22 (I) REQUIRED RULEMAKING.—

23 Not later than 1 year after the date  
24 of the enactment of this Act, and bi-  
25 annually thereafter, the Federal

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

22 (II) REQUIRED CONSULTA-  
23 TION.—In issuing rules or guidance  
24 under subclause (II), the Commission  
25 shall also consult with relevant indus-



1                   tries, consumer organizations, and  
2                   data security and identity theft pre-  
3                   vention experts and established stand-  
4                   ards setting bodies.

5                   (iv) FTC GUIDANCE.—Not later than  
6                   1 year after the date of the enactment of  
7                   this Act, the Federal Trade Commission,  
8                   after consultation with the National Insti-  
9                   tute of Standards and Technology, shall  
10                  issue guidance regarding the application of  
11                  the exemption in clause (i).

12                  (B) WRITTEN NOTIFICATION.—Without  
13                  unreasonable delay, but not later than 7 days  
14                  after the discovery of a security breach, unless  
15                  extended by the United States Secret Service or  
16                  the Federal Bureau of Investigation, the agency  
17                  or business entity must notify the Federal  
18                  Trade Commission and designated entity, in  
19                  writing, of—

20                         (i) the results of the risk assessment;

21                                 and

22                         (ii) its decision to invoke the risk as-  
23                         sessment exemption.

24                  (C) VIOLATIONS.—It shall be a violation of  
25                  this section to—

1 (i) fail to conduct a risk assessment in  
2 a reasonable manner, or according to  
3 standards generally accepted by experts in  
4 the field of information security; or

5 (ii) submit results of a risk assess-  
6 ment that—

7 (I) conceal violations of law, inef-  
8 ficiency, or administrative error;

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

12 (III) restrain competition;

13 (IV) contain fraudulent or delib-  
14 erately misleading information; or

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

20 (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

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

1 (A) effectively blocks the use of the sen-  
2 sitive personally identifiable information to ini-  
3 tiate unauthorized financial transactions before  
4 they are charged to the account of the indi-  
5 vidual; and

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

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

17 (d) LIMITATIONS.—Notwithstanding any other obli-  
18 gation under this subtitle, this subtitle does not apply to  
19 the following—

20 (1) FINANCIAL INSTITUTIONS.—A financial in-  
21 stitution subject to the data security requirements  
22 and standards under 501(b) of the Gramm-Leach-  
23 Bliley Act (15 U.S.C. 6801 et seq.), and subject to  
24 the jurisdiction of an agency or authority described  
25 in section 505(a) of the Gramm-Leach-Bliley Act

1 (15 U.S.C. 6805(a)), if the Federal functional regu-  
2 lator (as defined by section 509 of the Gramm-  
3 Leach-Bliley Act (15 U.S.C. 6809)) with jurisdiction  
4 over that financial institution has issued a regulation  
5 under title V of the Gramm-Leach-Bliley Act (15  
6 U.S.C. 6801 et seq.) that requires financial institu-  
7 tions within its jurisdiction to provide notification to  
8 individuals following a breach of security.

9 (2) HIPAA REGULATED ENTITIES EXEMP-  
10 TION.—

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

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

21 (ii) BUSINESS ENTITIES.—A business  
22 entity that—

23 (I) is acting as a business asso-  
24 ciate, as that term is defined under  
25 the Health Insurance Portability and

1 Accountability Act of 1996 (42 U.S.C.  
2 1301 et seq.) and is in compliance  
3 with the requirements imposed under  
4 that Act and implementing regula-  
5 tions promulgated under that Act;  
6 and

7 (II) is subject to, and currently  
8 in compliance with, the data breach  
9 notification requirements under sec-  
10 tion 13402 or 13407 of the American  
11 Reinvestment and Recovery Act of  
12 2009 (42 U.S.C. 17932 and 17937)  
13 and implementing regulations promul-  
14 gated under such sections.

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

1           tion is only a health insurance policy or sub-  
2           scriber identification number or information re-  
3           garding an individual's medical history, mental  
4           or physical medical condition, or medical treat-  
5           ment or diagnosis by a health care professional.

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

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

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

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

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

22           (2) **TELEPHONE NOTICE.**—Telephone notice to  
23          the individual personally.

24           (3) **PUBLIC NOTICE.**—

1 (A) ELECTRONIC NOTICE.—Prominent no-  
2 tice via all reasonable means of electronic con-  
3 tact between the individual and the agency or  
4 business entity, including any website,  
5 networked devices, or other interface through  
6 which the agency or business entity regularly  
7 interacts with the consumer, if the number of  
8 individuals whose sensitive personally identifi-  
9 able information was or is reasonably believed  
10 to have been accessed or acquired by an unau-  
11 thorized person exceeds 5,000.

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

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

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

23 (1) a description of the categories of sensitive  
24 personally identifiable information that was, or is  
25 reasonably believed to have been, accessed or ac-

1       quired by an unauthorized person, and how the  
2       agency or business entity came into possession of the  
3       sensitive personally identifiable information at issue;

4               (2) a toll-free number—

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

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

12               (3) the toll-free contact telephone numbers,  
13       websites, and addresses for the major credit report-  
14       ing agencies;

15               (4) the telephone numbers and websites for the  
16       relevant Federal agencies that provide information  
17       regarding identity theft prevention and protection;

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



1 reports or service from the agency or business enti-  
2 ty;

3 (6) notice that the individual is entitled to re-  
4 ceive a security freeze and that the agency or busi-  
5 ness entity will be liable for any costs associated  
6 with the security freeze for 2 years and the nec-  
7 essary instructions for requesting a security freeze;  
8 and

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

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

16 (1) notification that a security breach has oc-  
17 curred and that the individual’s sensitive personally  
18 identifiable information may have been com-  
19 promised;

20 (2) a description of the categories of sensitive  
21 personally identifiable information that were, or are  
22 reasonably believed to have been, accessed or ac-  
23 quired by an unauthorized person;

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

1 (A) that the individual may use to contact  
2 the agency or business entity, or the authorized  
3 agent of 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 and remedies avail-  
8 able to that individual; and

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

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

15 (1) electronic notice, which includes—

16 (A) notification that a security breach has  
17 occurred and that the individual's sensitive per-  
18 sonally identifiable information may have been  
19 compromised;

20 (B) a description of the categories of sen-  
21 sitive personally identifiable information that  
22 were, or are reasonably believed to have been,  
23 accessed or acquired by an unauthorized per-  
24 son; and

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

1 (i) that the individual may use to con-  
2 tact the agency or business entity, or the  
3 authorized agent of the agency or business  
4 entity; and

5 (ii) from which the individual may  
6 learn what types of sensitive personally  
7 identifiable information the agency or busi-  
8 ness entity maintained about that indi-  
9 vidual and remedies available to that indi-  
10 vidual; and

11 (2) media notice, which includes—

12 (A) a description of the categories of sen-  
13 sitive personally identifiable information that  
14 was, or is reasonably believed to have been,  
15 accessed or acquired by an unauthorized per-  
16 son;

17 (B) a toll-free number—

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

22 (ii) from which the individual may  
23 learn what types of sensitive personally  
24 identifiable information the agency or busi-  
25 ness entity maintained about that indi-

1           vidual and remedies available to that indi-  
2           vidual;

3           (C) the toll-free contact telephone num-  
4           bers, websites, and addresses for the major  
5           credit reporting agencies;

6           (D) the telephone numbers and websites  
7           for the relevant Federal agencies that provide  
8           information regarding identity theft prevention  
9           and protection;

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

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

21          (G) notice that the individual is entitled to  
22          receive compensation from the business entity  
23          or agency for any costs or damages incurred by  
24          the individual resulting from the security  
25          breach.

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

5 (e) DIRECT BUSINESS RELATIONSHIP.—Regardless  
6 of whether a business entity, agency, or a designated third  
7 party provides the notice required pursuant to section  
8 211(b), such notice shall include the name of the business  
9 entity or agency that has a direct relationship with the  
10 individual being notified.

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

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

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

24 (2) a credit monitoring or other service that en-  
25 ables consumers to detect the misuse of their per-

1       sonal information, beginning not later than 60 days  
2       following the request of the individual and con-  
3       tinuing for a period of 2 years.

4       (b) SECURITY FREEZE.—

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

10          (2) IMPLEMENTATION OF SECURITY FREEZE.—  
11       Upon receipt of a written request under paragraph  
12       (1), a credit rating agency shall—

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

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

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

6           (4) DISCLOSURE OF CREDIT REPORT TO THIRD  
7 PARTY.—

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

15                   (i) proper identification;

16                   (ii) the unique personal identification  
17 number or password described in para-  
18 graph (2)(B); and

19                   (iii) proper information regarding the  
20 third party who is to receive the credit re-  
21 port or the time period for which the credit  
22 report shall be available.

23           (B) REQUIREMENT.—Not later than 3  
24 business days after receipt of a request under

1           subparagraph (A), a credit rating agency shall  
2           lift the security freeze.

3           (5) PROCEDURES.—

4                 (A) IN GENERAL.—A credit rating agency  
5           shall develop procedures to receive and process  
6           requests from consumers under paragraph (2)  
7           of this section.

8                 (B) REQUIREMENT.—Procedures developed  
9           under subparagraph (A), at a minimum, shall  
10          include the ability of a consumer to send such  
11          temporary lift or removal request by electronic  
12          mail, letter, telephone, or facsimile.

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

20           (7) DETERMINATION BY CREDIT RATING AGEN-  
21          CY.—

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



1 (i) the request for a security freeze  
2 was made as part of a fraud that the con-  
3 sumer participated in, had knowledge of,  
4 or that can be demonstrated by cir-  
5 cumstantial evidence; or

6 (ii) the consumer credit report was  
7 frozen due to a material misrepresentation  
8 of fact by the consumer.

9 (B) NOTICE.—If a credit rating agency  
10 makes a determination under subparagraph (A)  
11 to not implement, or to remove, a security  
12 freeze under this subsection, the credit rating  
13 agency shall notify the consumer in writing of  
14 such determination—

15 (i) in the case of a determination not  
16 to implement a security freeze, not later  
17 than 5 business days after the determina-  
18 tion is made; and

19 (ii) in the case of a removal of a secu-  
20 rity freeze, prior to removing the freeze on  
21 the credit report of the consumer.

22 (8) RULE OF CONSTRUCTION.—

23 (A) IN GENERAL.—Nothing in this section  
24 shall be construed to prohibit disclosure of a  
25 credit report of a consumer to—

1 (i) a person, or the person's sub-  
2 sidiary, affiliate, agent or assignee with  
3 which the consumer has or, prior to assign-  
4 ment, had an account, contract or debtor-  
5 creditor relationship for the purpose of re-  
6 viewing the account or collecting the finan-  
7 cial obligation owing for the account, con-  
8 tract or debt;

9 (ii) a subsidiary, affiliate, agent, as-  
10 signee or prospective assignee of a person  
11 to whom access has been granted under  
12 paragraph (4) for the purpose of facili-  
13 tating the extension of credit or other per-  
14 missible use;

15 (iii) any person acting pursuant to a  
16 court order, warrant, or subpoena;

17 (iv) any person for the purpose of  
18 using such credit information to prescreen  
19 as provided by the Fair Credit Reporting  
20 Act (15 U.S.C. 1681 et seq.);

21 (v) any person for the sole purpose of  
22 providing a credit file monitoring subscrip-  
23 tion service to which the consumer has  
24 subscribed;

1 (vi) a credit rating agency for the sole  
2 purpose of providing a consumer with a  
3 copy of the credit report of the consumer  
4 upon the request of the consumer; or

5 (vii) a Federal, State or local govern-  
6 mental entity, including a law enforcement  
7 agency, or court, or their agents or assign-  
8 ees pursuant to their statutory or regu-  
9 latory duties; and

10 (viii) any person for the sole purpose  
11 of providing a remedy requested by an in-  
12 dividual under this section.

13 (B) REVIEWING THE ACCOUNT.—For pur-  
14 poses of this subsection, “reviewing the ac-  
15 count” shall include activities relating to ac-  
16 count maintenance, monitoring, credit line in-  
17 creases, and account upgrades and enhance-  
18 ments.

19 (9) EXCEPTIONS.—The following persons shall  
20 not be required to place a security freeze under this  
21 subsection, but shall be subject to any security  
22 freeze placed on a credit report by another credit  
23 rating agency:

24 (A) A check services or fraud prevention  
25 services company that reports on incidents of

1 fraud or issues authorizations for the purpose  
2 of approving or processing negotiable instru-  
3 ments, electronic fund transfers or similar  
4 methods of payment.

5 (B) A deposit account information service  
6 company that issues reports regarding account  
7 closures due to fraud, substantial overdrafts,  
8 automated teller machine abuse, or similar in-  
9 formation regarding a consumer to inquiring  
10 banks or other financial institutions for use  
11 only in reviewing a consumer request for a de-  
12 posit account at the inquiring bank or financial  
13 institution.

14 (C) A credit rating agency that—

15 (i) acts only to resell credit informa-  
16 tion by assembling and merging informa-  
17 tion contained in a database of 1 or more  
18 credit reporting agencies; and

19 (ii) does not maintain a permanent  
20 database of credit information from which  
21 new credit reports are produced.

22 (10) FEES.—

23 (A) IN GENERAL.—A credit rating agency  
24 may charge reasonable fees for each security  
25 freeze, removal of such freeze or temporary lift

1 of such freeze for a period of time, and a tem-  
2 porary lift of such freeze for a specific party.

3 (B) REQUIREMENT.—Any fees charged  
4 under subparagraph (A) shall be borne by the  
5 agency or business entity providing notice under  
6 section 214 for 2 years following the establish-  
7 ment of the security freeze under this sub-  
8 section.

9 (c) COSTS RESULTING FROM A SECURITY  
10 BREACH.—

11 (1) IN GENERAL.—A business entity or agency  
12 that experiences a security breach and is required to  
13 provide notice under this subtitle shall pay, upon re-  
14 quest, to any individual whose sensitive personally  
15 identifiable information has been, or is reasonably  
16 believed to have been, accessed or acquired as a re-  
17 sult of such security breach, any costs or damages  
18 incurred by the individual as a result of such secu-  
19 rity breach, including costs associated with identity  
20 theft suffered as a result of such security breach.

21 (2) COMPLIANCE.—A business entity or agency  
22 shall be deemed in compliance with this subsection  
23 if the business entity or agency—

24 (A) provides insurance to any individual  
25 whose sensitive personally identifiable informa-

1           tion has been, or is reasonably believed to have  
2           been, accessed or acquired as a result of a secu-  
3           rity breach and such insurance is sufficient to  
4           compensate the consumer for not less than  
5           \$25,000 of costs or damages; or

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

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

10       If an agency or business entity is required to provide  
11       notification to more than 5,000 individuals under section  
12       211(a), the agency or business entity shall also notify all  
13       consumer reporting agencies that compile and maintain  
14       files on consumers on a nationwide basis (as defined in  
15       section 603(p) of the Fair Credit Reporting Act (15  
16       U.S.C. 1681a(p))) of the timing and distribution of the  
17       notices. Such notice shall be given to the consumer credit  
18       reporting agencies without unreasonable delay and, if it  
19       will not delay notice to the affected individuals, prior to  
20       the distribution of notices to the affected individuals.

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

22       (a) DESIGNATION OF A GOVERNMENT ENTITY TO  
23       RECEIVE NOTICE.—

24               (1) IN GENERAL.—Not later than 60 days after  
25       the date of enactment of this Act, the Secretary of

1 Homeland Security, in consultation with the Attor-  
2 ney General, shall designate a Federal Government  
3 entity to receive the information required to be sub-  
4 mitted under this subtitle, and any other reports and  
5 information about information security incidents,  
6 threats, and vulnerabilities.

7 (2) RESPONSIBILITIES OF THE DESIGNATED  
8 ENTITY.—The designated entity shall—

9 (A) be responsible for promptly providing  
10 the information it receives to the United States  
11 Secret Service and the Federal Bureau of In-  
12 vestigation, and to the Federal Trade Commis-  
13 sion for civil law enforcement purposes; and

14 (B) provide the information described in  
15 subparagraph (A) as appropriate to other Fed-  
16 eral agencies for law enforcement, national se-  
17 curity, or data security purposes.

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

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

1           (2) the security breach involves a database,  
2 networked or integrated databases, or other data  
3 system containing the sensitive personally identifi-  
4 able information of more than 500,000 individuals  
5 nationwide;

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

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

14 (c) FTC REVIEW OF THRESHOLDS.—

15           (1) REVIEW.—Not later than 1 year after the  
16 date of enactment of this Act, the Federal Trade  
17 Commission, in consultation with the Attorney Gen-  
18 eral and the Secretary of Homeland Security, shall  
19 promulgate regulations regarding the reports re-  
20 quired under subsection (a).

21           (2) RULEMAKING.—The Federal Trade Com-  
22 mission, in consultation with the Attorney General  
23 and the Secretary of Homeland Security, after no-  
24 tice and the opportunity for public comment, and in  
25 a manner consistent with this section, shall promul-



1 gate regulations, as necessary, under section 553 of  
2 title 5, United States Code, to adjust the thresholds  
3 for notice to law enforcement and national security  
4 authorities under subsection (a) and to facilitate the  
5 purposes of this section.

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

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

11 (2) Notice under section 211 shall be delivered  
12 to individuals not later than 48 hours after the Fed-  
13 eral Bureau of Investigation or the Secret Service  
14 receives notice of a security breach from an agency  
15 or business entity.

16 **SEC. 218. FEDERAL ENFORCEMENT.**

17 (a) **CIVIL ACTIONS BY THE ATTORNEY GENERAL.**—

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 engages 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 \$500 per  
25 day per individual whose sensitive personally identi-

1        fiable information was, or is reasonably believed to  
2        have been, accessed or acquired by an unauthorized  
3        person, up to a maximum of \$20,000,000 per viola-  
4        tion, unless such conduct is found to be willful or in-  
5        tentional.

6            (2) PRESUMPTION.—A violation of section  
7        212(b)(2)(C) shall be presumed to be willful or in-  
8        tentional conduct.

9        (b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-  
10       ERAL.—

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

16            (A) enjoining such act or practice; or

17            (B) enforcing compliance with this subtitle.

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

22        (c) CIVIL ACTIONS BY THE FEDERAL TRADE COM-  
23       MISSION.—

24            (1) IN GENERAL.—Compliance with the require-  
25        ments imposed under subtitle A and this subtitle

1 may be enforced under the Federal Trade Commis-  
2 sion Act (15 U.S.C. 41 et seq.) by the Federal  
3 Trade Commission with respect to business entities  
4 subject to this Act. All of the functions and powers  
5 of the Federal Trade Commission under the Federal  
6 Trade Commission Act are available to the Commis-  
7 sion to enforce compliance by any person with the  
8 requirements imposed under this title.

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

1 (d) CONSIDERATIONS.—In determining the amount  
2 of a civil penalty under this subsection, the court shall  
3 take into account—

4 (1) the degree of culpability of the business en-  
5 tity;

6 (2) any prior violations of this subtitle by the  
7 business entity;

8 (3) the ability of the business entity to pay a  
9 civil penalty;

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

12 (5) the number of individuals whose sensitive  
13 personally identifiable information was compromised  
14 by the breach;

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

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

18 (e) COORDINATION OF ENFORCEMENT.—

19 (1) IN GENERAL.—Before opening an investiga-  
20 tion, the Federal Trade Commission shall consult  
21 with the Attorney General.

22 (2) LIMITATION.—The Federal Trade Commis-  
23 sion may initiate investigations under this subsection  
24 unless the Attorney General determines that such an

1 investigation would impede an ongoing criminal in-  
2 vestigation or national security activity.

3 (3) COORDINATION AGREEMENT.—

4 (A) IN GENERAL.—In order to avoid con-  
5 flicts and promote consistency regarding the en-  
6 forcement and litigation of matters under this  
7 Act, not later than 180 days after the enact-  
8 ment of this Act, the Attorney General and the  
9 Commission shall enter into an agreement for  
10 coordination regarding the enforcement of this  
11 Act.

12 (B) REQUIREMENT.—The coordination  
13 agreement entered into under subparagraph (A)  
14 shall include provisions to ensure that parallel  
15 investigations and proceedings under this sec-  
16 tion are conducted in a manner that avoids con-  
17 flicts and does not impede the ability of the At-  
18 torney General to prosecute violations of Fed-  
19 eral criminal laws.

20 (4) COORDINATION WITH THE FCC.—If an en-  
21 forcement action under this Act relates to customer  
22 proprietary network information, the Federal Trade  
23 Commission shall coordinate the enforcement action  
24 with the Federal Communications Commission.

1 (f) RULEMAKING.—The Federal Trade Commission  
2 may, in consultation with the Attorney General, issue such  
3 other regulations as it determines to be necessary to carry  
4 out this subtitle. All regulations promulgated under this  
5 Act shall be issued in accordance with section 553 of title  
6 5, United States Code. Where regulations relate to cus-  
7 tomer proprietary network information, the promulgation  
8 of such regulations will be coordinated with the Federal  
9 Communications Commission.

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

14 (h) FRAUD ALERT.—Section 605A(b)(1) of the Fair  
15 Credit Reporting Act (15 U.S.C. 1681c–1(b)(1)) is  
16 amended in the matter preceding subparagraph (A) by in-  
17 serting “, or evidence that the consumer has received no-  
18 tice that the consumer’s financial information has or may  
19 have been compromised,” after “identity theft report”.

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

21 (a) IN GENERAL.—

22 (1) CIVIL ACTIONS.—

23 (A) IN GENERAL.—In any case in which  
24 the attorney general of a State or any State or  
25 local law enforcement agency authorized by the

1 State attorney general or by State statute to  
2 prosecute violations of consumer protection law,  
3 has reason to believe that an interest of the  
4 residents of that State has been or is threat-  
5 ened or adversely affected by the engagement of  
6 a business entity in a practice that is prohibited  
7 under this subtitle, the State or the State or  
8 local law enforcement agency on behalf of the  
9 residents of the agency's jurisdiction, may bring  
10 a civil action on behalf of the residents of the  
11 State or jurisdiction in a district court of the  
12 United States of appropriate jurisdiction or any  
13 other court of competent jurisdiction, including  
14 a State court, to—

15 (i) enjoin that practice;

16 (ii) enforce compliance with this sub-  
17 title; or

18 (iii) obtain civil penalties of not more  
19 than \$500 per day per individual whose  
20 sensitive personally identifiable information  
21 was, or is reasonably believed to have been,  
22 accessed or acquired by an unauthorized  
23 person, up to a maximum of \$20,000,000  
24 per violation, unless such conduct is found  
25 to be willful or intentional.

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

4           (2) CONSIDERATIONS.—In determining the  
5           amount of a civil penalty under this subsection, the  
6           court shall take into account—

7                   (A) the degree of culpability of the busi-  
8                   ness entity;

9                   (B) any prior violations of this subtitle by  
10                  the business entity;

11                  (C) the ability of the business entity to pay  
12                  a civil penalty;

13                  (D) the effect on the ability of the business  
14                  entity to continue to do business;

15                  (E) the number of individuals whose sen-  
16                  sitive personally identifiable information was  
17                  compromised by the breach;

18                  (F) the relative cost of compliance with  
19                  this subtitle; and

20                  (G) such other matters as justice may re-  
21                  quire.

22           (3) NOTICE.—

23                   (A) IN GENERAL.—Before filing an action  
24                   under paragraph (1), the attorney general of



1 the State involved shall provide to the Attorney  
2 General of the United States—

3 (i) written notice of the action; and

4 (ii) a copy of the complaint for the ac-  
5 tion.

6 (B) EXEMPTION.—

7 (i) IN GENERAL.—Subparagraph (A)  
8 shall not apply with respect to the filing of  
9 an action by an attorney general of a State  
10 under this subtitle, if the State attorney  
11 general determines that it is not feasible to  
12 provide the notice described in such sub-  
13 paragraph before the filing of the action.

14 (ii) NOTIFICATION.—In an action de-  
15 scribed in clause (i), the attorney general  
16 of a State shall provide notice and a copy  
17 of the complaint to the Attorney General  
18 at the time the State attorney general files  
19 the action.

20 (b) FEDERAL PROCEEDINGS.—Upon receiving notice  
21 under subsection (a)(2), the Attorney General shall have  
22 the right to—

23 (1) move to stay the action, pending the final  
24 disposition of a pending Federal proceeding or ac-  
25 tion;

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

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

7           (4) file petitions for appeal.

8           (c) PENDING PROCEEDINGS.—If the Attorney Gen-  
9 eral has instituted a proceeding or action for a violation  
10 of this subtitle or any regulations thereunder, no attorney  
11 general of a State may, during the pendency of such pro-  
12 ceeding or action, bring an action under this subtitle  
13 against any defendant named in such criminal proceeding  
14 or civil action for any violation that is alleged in that pro-  
15 ceeding or action.

16           (d) CONSTRUCTION.—For purposes of bringing any  
17 civil action under subsection (a), nothing in this subtitle  
18 regarding notification shall be construed to prevent an at-  
19 torney general of a State from exercising the powers con-  
20 ferred on such attorney general by the laws of that State  
21 to—

22           (1) conduct investigations;

23           (2) administer oaths or affirmations; or

24           (3) compel the attendance of witnesses or the  
25 production of documentary and other evidence.

1 (e) VENUE; SERVICE OF PROCESS.—

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

4 (A) the district court of the United States  
5 that meets applicable requirements relating to  
6 venue under section 1391 of title 28, United  
7 States Code; or

8 (B) another court of competent jurisdic-  
9 tion.

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

13 (A) is an inhabitant; or

14 (B) may be found.

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

16 (a) IN GENERAL.—Any person aggrieved by a viola-  
17 tion of the provisions of section 211, 213, 214, 215, or  
18 216 by a business entity may bring a civil action in a court  
19 of appropriate jurisdiction to recover for personal injuries  
20 sustained as a result of the violation.

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

1 (c) REMEDIES IN A CITIZEN SUIT.—

2 (1) DAMAGES.—Any individual harmed by a  
3 failure of a business entity to comply with the provi-  
4 sions of section 211, 213, 214, 215, or 216 shall be  
5 able to collect damages of not more than \$500 per  
6 day per individual whose sensitive personally identi-  
7 fiable information was, or is reasonably believed to  
8 have been, accessed or acquired by an unauthorized  
9 person, up to a maximum of \$20,000,000 per viola-  
10 tion.

11 (2) PUNITIVE DAMAGES.—A business entity  
12 may be liable for punitive damages if the business  
13 entity—

14 (A) intentionally or willfully violates the  
15 provisions of section 211, 213, 214, 215, or  
16 216; or

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

19 (3) EQUITABLE RELIEF.—A business entity  
20 that violates the provisions of section 211, 213, 214,  
21 215, or 216 may be enjoined to provide required  
22 remedies under section 215 by a court of competent  
23 jurisdiction.

24 (d) OTHER RIGHTS AND REMEDIES.—The rights and  
25 remedies available under this subsection are cumulative

1 and shall not affect any other rights and remedies avail-  
2 able under law.

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

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

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

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

18 (1) the degree of culpability of the business en-  
19 tity;

20 (2) any prior violations of this subtitle by the  
21 business entity;

22 (3) the ability of the business entity to pay a  
23 civil penalty;

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

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

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

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

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

8           (a) IN GENERAL.—The provisions of this subtitle  
9 shall supersede any other provision of Federal law or any  
10 provision of law of any State relating to notification by  
11 a business entity engaged in interstate commerce or an  
12 agency of a security breach, except as provided in this sub-  
13 section.

14           (b) LIMITATIONS.—

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

22           (2) GRAMM-LEACH-BLILEY ACT.—Nothing in  
23 this Act shall supersede the data security require-  
24 ments of the Gramm-Leach-Bliley Act (15 U.S.C.

1 6801 et seq.), or implementing regulations based on  
2 that Act.

3 (3) HEALTH PRIVACY.—

4 (A) To the extent that a business entity  
5 acts as a covered entity or a business associate  
6 under the Health Information Technology for  
7 Economic and Clinical Health Act (42 U.S.C.  
8 17932), and has the obligation to provide  
9 breach notification under that Act or its imple-  
10 menting regulations, the requirements of this  
11 Act shall not apply.

12 (B) To the extent that a business entity  
13 acts as a vendor of personal health records, a  
14 third-party service provider, or other entity sub-  
15 ject to the Health Information Technology for  
16 Economical and Clinical Health Act (42 U.S.C.  
17 17937), and has the obligation to provide  
18 breach notification under that Act or its imple-  
19 menting regulations, the requirements of this  
20 Act shall not apply.

21 **SEC. 222. AUTHORIZATION OF APPROPRIATIONS.**

22 There are authorized to be appropriated such sums  
23 as may be necessary to cover the costs incurred by the  
24 United States Secret Service to carry out investigations

1 and risk assessments of security breaches as required  
2 under this subtitle.

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

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

8 (1) the number and nature of the security  
9 breaches described in the notices filed by those busi-  
10 ness entities invoking the risk assessment exemption  
11 under section 212(b) and the response of the United  
12 States Secret Service and the Federal Bureau of In-  
13 vestigation to such notices; and

14 (2) the number and nature of security breaches  
15 subject to the national security and law enforcement  
16 exemptions under section 212(a), provided that such  
17 report may not disclose the contents of any risk as-  
18 sessment provided to the United States Secret Serv-  
19 ice and the Federal Bureau of Investigation pursu-  
20 ant to this subtitle.



1 **Subtitle C—Post-Breach Technical**  
2 **Information Clearinghouse**

3 **SEC. 230. CLEARINGHOUSE INFORMATION COLLECTION,**  
4 **MAINTENANCE, AND ACCESS.**

5 (a) IN GENERAL.—The designated entity shall main-  
6 tain a clearinghouse of technical information concerning  
7 system vulnerabilities identified in the wake of security  
8 breaches, which shall—

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

11 (2) be accessible to certified entities under sub-  
12 section (c).

13 (b) POST-BREACH TECHNICAL NOTIFICATION.—In  
14 any instance in which an agency or business entity is re-  
15 quired to notify the designated entity under section 217,  
16 the agency or business entity shall also provide the des-  
17 ignated entity with technical information concerning the  
18 nature of the security breach, including—

19 (1) technical information regarding any system  
20 vulnerabilities of the agency or business entity re-  
21 vealed by or identified as a consequence of the secu-  
22 rity breach;

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

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

5           (c) ACCESS TO CLEARINGHOUSE.—Any entity cer-  
6           tified under subsection (d) may review information main-  
7           tained by the technical information clearinghouse for the  
8           purpose of preventing security breaches that threaten the  
9           security of sensitive personally identifiable information.

10          (d) CERTIFICATION FOR ACCESS.—The designated  
11          entity shall issue and revoke certifications to agencies and  
12          business entities wishing to review information maintained  
13          by the technical information clearinghouse and shall estab-  
14          lish conditions for obtaining and maintaining such certifi-  
15          cations, including agreement that any information ob-  
16          tained directly or derived indirectly from the review of in-  
17          formation maintained by the technical information clear-  
18          inghouse—

19                (1) shall only be used to improve the security  
20                and reduce the vulnerability of networks that collect,  
21                access, transmit, use, store, or dispose of sensitive  
22                personally identifiable information;

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

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

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

12       **SEC. 231. PROTECTIONS FOR CLEARINGHOUSE PARTICI-**  
13                               **PANTS.**

14          (a) PROTECTION OF PROPRIETARY INFORMATION.—  
15          To the extent feasible, the designated entity shall ensure  
16          that any technical information disclosed to the designated  
17          entity under this subtitle shall be stored in a format de-  
18          signed to protect proprietary business information from  
19          inadvertent disclosure.

20          (b) ANONYMOUS DATA RELEASE.—To the extent fea-  
21          sible, the designated entity shall ensure that all informa-  
22          tion stored in the technical information clearinghouse and  
23          accessed by certified parties is presented in a form that  
24          minimizes the potential for such information to be traced

1 to a particular network, company, or security breach inci-  
2 dent.

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

5 (1) security and vulnerability information col-  
6 lected under this section and provided to the Federal  
7 Government, including aggregated analysis and data,  
8 shall be exempt from disclosure under section  
9 552(b)(3) of title 5, United States Code; and

10 (2) under section 230(e), security and vulner-  
11 ability-related information provided to the Federal  
12 Government under this section, including aggregated  
13 analysis and data, shall be protected from public dis-  
14 closure, except that this paragraph—

15 (A) does not prohibit the sharing of such  
16 information, as the designated entity deter-  
17 mines to be appropriate, in order to mitigate  
18 cybersecurity threats or further the official  
19 functions of a government agency; and

20 (B) does not authorized such information  
21 to be withheld from a committee of Congress  
22 authorized to request the information.

23 (d) PROTECTION OF CLASSIFIED INFORMATION.—  
24 Nothing in this subtitle permits the unauthorized dislo-  
25 sure of classified information.

1 **SEC. 232. EFFECTIVE DATE.**

2 This subtitle shall take effect on the expiration of the  
3 date that is 90 days after the date of enactment of this  
4 Act.

5 **TITLE III—ACCESS TO AND USE**  
6 **OF COMMERCIAL DATA**

7 **SEC. 301. GENERAL SERVICES ADMINISTRATION REVIEW**  
8 **OF CONTRACTS.**

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

14 (1) the data privacy and security program of a  
15 data broker to ensure the privacy and security of  
16 data containing sensitive personally identifiable in-  
17 formation, including whether such program ade-  
18 quately addresses privacy and security threats cre-  
19 ated by malicious software or code, or the use of  
20 peer-to-peer file sharing software;

21 (2) the compliance of a data broker with such  
22 program;

23 (3) the extent to which the databases and sys-  
24 tems containing sensitive personally identifiable in-  
25 formation of a data broker have been compromised  
26 by security breaches; and

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

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

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

17                (1) include monetary or other penalties—

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

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

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

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

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

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

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

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

20 **SEC. 302. REQUIREMENT TO AUDIT INFORMATION SECU-**  
21 **RITY PRACTICES OF CONTRACTORS AND**  
22 **THIRD-PARTY BUSINESS ENTITIES.**

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

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

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

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

6 “(9) procedures for evaluating and auditing the  
7 information security practices of contractors or  
8 third-party business entities supporting the informa-  
9 tion systems or operations of the agency involving  
10 sensitive personally identifiable information (as that  
11 term is defined in section 3 of the Personal Data  
12 Protection and Breach Accountability Act of 2014)  
13 and ensuring remedial action to address any signifi-  
14 cant deficiencies.”.

15 **SEC. 303. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT**  
16 **USE OF COMMERCIAL INFORMATION SERV-**  
17 **ICES CONTAINING SENSITIVE PERSONALLY**  
18 **IDENTIFIABLE INFORMATION.**

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

22 (1) in clause (i), by striking “or”;

23 (2) in clause (ii)(II), by striking the period and  
24 inserting “; or”; and

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



1                   “(iii) purchasing or subscribing for a  
2                   fee to sensitive personally identifiable in-  
3                   formation from a data broker (as such  
4                   terms are defined in section 3 of the Per-  
5                   sonal Data Protection and Breach Ac-  
6                   countability Act of 2014).”.

7           (b) LIMITATION.—Notwithstanding any other provi-  
8           sion of law, beginning 1 year after the date of enactment  
9           of this Act, no Federal agency may enter into a contract  
10          with a data broker to access for a fee any database con-  
11          sisting primarily of sensitive personally identifiable infor-  
12          mation concerning United States persons (other than news  
13          reporting or telephone directories) unless the head of the  
14          agency—

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

20                       (A) such database;

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

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

24               (2) adopts regulations that specify—

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

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

5 (C) any standards used to ensure that the  
6 sensitive personally identifiable information  
7 accessed, analyzed, or used is the minimum nec-  
8 essary to accomplish the intended legitimate  
9 purpose of the Federal agency;

10 (D) standards limiting the retention and  
11 redisclosure of sensitive personally identifiable  
12 information obtained from such databases;

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

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

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

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

1 (I) an outline of enforcement mechanisms  
2 for accountability to protect individuals and the  
3 public against unlawful or illegitimate access or  
4 use of databases; and

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

8 (A) providing for penalties—

9 (i) for failure to comply with title II  
10 of this Act; or

11 (ii) if the entity knows or has reason  
12 to know that the sensitive personally iden-  
13 tifiable information being provided to the  
14 Federal department or agency is inac-  
15 curate, and provides such inaccurate infor-  
16 mation; and

17 (B) requiring a data broker that engages  
18 service providers not subject to subtitle A of  
19 title II of this Act for responsibilities related to  
20 sensitive personally identifiable information  
21 to—

22 (i) exercise appropriate due diligence  
23 in selecting those service providers for re-  
24 sponsibilities related to sensitive personally  
25 identifiable information;

1 (ii) take reasonable steps to select and  
2 retain service providers that are capable of  
3 maintaining appropriate safeguards for the  
4 security, privacy, and integrity of the sen-  
5 sitive personally identifiable information at  
6 issue; and

7 (iii) require such service providers, by  
8 contract, to implement and maintain ap-  
9 propriate measures designed to meet the  
10 objectives and requirements in title II of  
11 this Act.

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

16 (d) STUDY OF GOVERNMENT USE.—

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

1 bases containing sensitive personally identifiable in-  
2 formation.

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

5 **SEC. 304. FBI REPORT ON REPORTED BREACHES AND COM-**  
6 **PLIANCE.**

7 (a) IN GENERAL.—Not later than 1 year after the  
8 date of enactment of this Act, and each year thereafter,  
9 the Federal Bureau of Investigation, in coordination with  
10 the Secret Service, shall submit to the Committee on the  
11 Judiciary of the Senate and the Committee on the Judici-  
12 ary of the House of Representatives a report regarding  
13 any reported breaches at agencies or business entities dur-  
14 ing the preceding year.

15 (b) REPORT CONTENT.—Such reporting shall in-  
16 clude—

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

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

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

1 **SEC. 305. DEPARTMENT OF JUSTICE REPORT ON ENFORCE-**  
2 **MENT ACTIONS.**

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

5 “(c) Not later than 1 year after the date of enactment  
6 of the Personal Data Protection and Breach Account-  
7 ability Act of 2014, and every fiscal year thereafter, the  
8 Attorney General shall submit to Congress a report on  
9 Federal enforcement actions, State attorneys general en-  
10 forcement actions, and private enforcement actions, un-  
11 dertaken pursuant to the Personal Data Protection and  
12 Breach Accountability Act of 2014 that shall include a de-  
13 scription of the best practices for enforcement of such Act  
14 as well as recommendations, if any, for modifying or  
15 amending this Act to increase the effectiveness of such en-  
16 forcement actions.”.

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

18 (a) IN GENERAL.—Not later than 1 year after the  
19 date of enactment of this Act, and each year thereafter,  
20 the designated entity, in coordination with the Attorney  
21 General and the Federal Trade Commission, shall submit  
22 to the Committee on the Judiciary of the Senate and the  
23 Committee on the Judiciary of the House of Representa-  
24 tives a report regarding the effectiveness of post-breach  
25 notification practices by agencies and business entities.

1 (b) REPORT CONTENT.—The report required under  
2 subsection (a) shall include—

3 (1) in each instance of a breach of security, the  
4 amount of time between the instance of the breach  
5 and the discovery of the breach by the affected busi-  
6 ness entity;

7 (2) in each instance of a breach of security, the  
8 amount of time between the discovery of the breach  
9 by the affected business entity and the notification  
10 to the Federal Bureau of Investigation and the  
11 United States Secret Service; and

12 (3) in each instance of a breach of security, the  
13 amount of time between the discovery of the breach  
14 by the affected business entity and the notification  
15 to individuals whose sensitive personally identifiable  
16 information was compromised.

17 **TITLE IV—COMPLIANCE WITH**  
18 **STATUTORY PAY-AS-YOU-GO ACT**

19 **SEC. 401. BUDGET COMPLIANCE.**

20 The budgetary effects of this Act, for the purpose of  
21 complying with the Statutory Pay-As-You-Go Act of 2010,  
22 shall be determined by reference to the latest statement  
23 titled “Budgetary Effects of PAYGO Legislation” for this  
24 Act, submitted for printing in the Congressional Record  
25 by the Chairman of the Senate Budget Committee, pro-

- 1 vided that such statement has been submitted prior to the
- 2 vote on passage.

