

115TH CONGRESS  
1ST SESSION

**S.** \_\_\_\_\_

To ensure the privacy and security of sensitive personal information, to prevent and mitigate identity theft, to provide notice of security breaches involving sensitive personal information, and to enhance law enforcement assistance and other protections against security breaches, fraudulent access, and misuse of personal information.

---

IN THE SENATE OF THE UNITED STATES

\_\_\_\_\_ introduced the following bill; which was read twice  
and referred to the Committee on \_\_\_\_\_

---

## **A BILL**

To ensure the privacy and security of sensitive personal information, to prevent and mitigate identity theft, to provide notice of security breaches involving sensitive personal information, and to enhance law enforcement assistance and other protections against security breaches, fraudulent access, and misuse of personal information.

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

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

4 (a) SHORT TITLE.—This Act may be cited as the  
5 “Consumer Privacy Protection Act of 2017”.

1 (b) TABLE OF CONTENTS.—The table of contents for  
 2 this Act is as follows:

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

TITLE I—PUNISHMENT FOR CONCEALMENT OF SECURITY  
 BREACHES AND TOOLS TO COMBAT CYBERCRIME

- Sec. 101. Concealment of security breaches involving sensitive personally identifiable information.
- Sec. 102. Reporting of certain cybercrimes.
- Sec. 103. Authority to shut down botnets.
- Sec. 104. Deterring the development and sale of computer and cell phone spying devices.

TITLE II—CONSUMER PRIVACY AND SECURITY OF SENSITIVE  
 PERSONALLY IDENTIFIABLE INFORMATION

Subtitle A—Consumer Privacy and Data Security Program

- Sec. 201. Purpose and applicability of consumer privacy and data security program.
- Sec. 202. Requirements for consumer privacy and data security program.
- Sec. 203. Federal enforcement.
- Sec. 204. Enforcement by State attorneys general.
- Sec. 205. Relation to other laws.

Subtitle B—Security Breach Notification and Protection

- Sec. 211. Notice to individuals; protection.
- Sec. 212. Exemptions.
- Sec. 213. Methods of notice.
- Sec. 214. Content of notification.
- Sec. 215. Coordination of notification with credit reporting agencies.
- Sec. 216. Notice to the Federal Trade Commission.
- Sec. 217. Notice to law enforcement.
- Sec. 218. Federal enforcement.
- Sec. 219. Enforcement by State attorneys general.
- Sec. 220. Effect on Federal and State law.
- Sec. 221. Reporting on exemptions.
- Sec. 222. Effective date.

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

- Sec. 301. Budget compliance.

3 **SEC. 2. FINDINGS.**

4 Congress finds that—

5 (1) databases of sensitive personally identifiable  
 6 information are increasingly prime targets of hack-

1       ers, nation-state actors, identity thieves, rogue em-  
2       ployees, and other criminals, including organized  
3       and sophisticated criminal operations;

4           (2) security breaches caused by such criminal  
5       acts are a serious threat to consumer privacy, con-  
6       sumer confidence, homeland security, national secu-  
7       rity, e-commerce, and economic stability;

8           (3) misuse of sensitive personally identifiable  
9       information has the potential to cause serious or ir-  
10      reparable harm to an individual's livelihood, privacy,  
11      and liberty and undermine efficient and effective  
12      business and government operations;

13          (4) identity theft is a serious threat to the Na-  
14      tion's economic stability, national security, homeland  
15      security, cybersecurity, the development of e-com-  
16      merce, and the privacy rights of Americans;

17          (5) it is important for business entities that  
18      own, use, store, or license sensitive personally identi-  
19      fiable information to adopt reasonable policies and  
20      procedures to help ensure the security and privacy of  
21      sensitive personally identifiable information; and

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

1 **SEC. 3. DEFINITIONS.**

2 In this Act, the following definitions shall apply:

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

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

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

14 (4) **CONSUMER PRIVACY AND DATA SECURITY**  
15 **PROGRAM.**—The term “consumer privacy and data  
16 security program” means the program described in  
17 section 202(a).

18 (5) **CONSUMER REPORTING AGENCY.**—The term  
19 “consumer reporting agency” means a consumer re-  
20 porting agency described in section 603(p) of the  
21 Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

22 (6) **COVERED ENTITY.**—The term “covered en-  
23 tity” means any business entity, other than a service  
24 provider, that collects, uses, accesses, transmits,  
25 stores, or disposes of sensitive personally identifiable  
26 information, including a consumer reporting agency.

1           (7) DESIGNATED ENTITY.—The term “des-  
2           ignated entity” means the Federal Government enti-  
3           ty designated by the Secretary of Homeland Security  
4           under section 217(a).

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

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

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

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

20          (10) SECURITY BREACH.—

21          (A) IN GENERAL.—The term “security  
22          breach” means compromise of the privacy, in-  
23          tegrity, or security of computerized data that  
24          results in, or that there is a reasonable basis to  
25          conclude has resulted in, unauthorized access to

1 or acquisition of sensitive personally identifiable  
2 information.

3 (B) EXCLUSION.—The term “security  
4 breach” does not include—

5 (i) a good faith access or acquisition  
6 of sensitive personally identifiable informa-  
7 tion by a business entity, or an employee  
8 or agent of a business entity, if the sen-  
9 sitive personally identifiable information is  
10 not subject to further unauthorized disclo-  
11 sure;

12 (ii) the release of a public record not  
13 otherwise subject to confidentiality or non-  
14 disclosure requirements; or

15 (iii) any lawfully authorized investiga-  
16 tive, protective, or intelligence activity of a  
17 law enforcement or intelligence agency of  
18 the United States, a State, or a political  
19 subdivision of a State.

20 (11) SENSITIVE PERSONALLY IDENTIFIABLE IN-  
21 FORMATION.—The term “sensitive personally identi-  
22 fiable information” means any information or com-  
23 pilation of information, in electronic or digital form  
24 that identifies or could be used to identify a par-  
25 ticular person, including the following:

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

5           (B) A financial account number or credit  
6 or debit card number in combination with any  
7 security code, access code, or password if re-  
8 quired for an individual to obtain credit, with-  
9 draw funds, or engage in financial transactions.

10          (C) A unique electronic account identifier,  
11 including an online user name or email address,  
12 in combination with any security code, access  
13 code, password, or security question and an-  
14 swer, if required for an individual to obtain  
15 money, goods, services, access to digital photo-  
16 graphs, digital videos or electronic communica-  
17 tions, or any other thing of value.

18          (D) Unique biometric data, such as  
19 faceprint, fingerprint, voice print, a retina or  
20 iris image, or any other unique physical rep-  
21 resentation.

22          (E) An individual's first and last name or  
23 first initial and last name in combination with  
24 any information that relates to the individual's  
25 past, present, or future physical or mental

1 health or condition, or to the provision of health  
2 care to or diagnosis of the individual, including  
3 health insurance information such as a health  
4 insurance policy number or subscriber identi-  
5 fication number, or any information in an indi-  
6 vidual's health insurance application and claims  
7 history.

8 (F) Information about an individual's geo-  
9 graphic location generated by or derived from  
10 the operation or use of an electronic commu-  
11 nications device that is sufficient to identify the  
12 street and name of the city or town in which  
13 the device is located, excluding telephone num-  
14 bers or network or Internet protocol addresses.

15 (G) Password-protected digital photo-  
16 graphs and digital videos not otherwise avail-  
17 able to the public.

18 (12) SERVICE PROVIDER.—The term “service  
19 provider” means a business entity that provides elec-  
20 tronic data transmission, routing, intermediate and  
21 transient storage, or connections to its system or  
22 network, where the business entity providing such  
23 services does not select or modify the content of the  
24 electronic data, is not the sender or the intended re-  
25 cipient of the data, and the business entity trans-



1 mits, routes, or provides connections for sensitive  
2 personally identifiable information in a manner that  
3 sensitive personally identifiable information is undif-  
4 ferentiated from other types of data that such busi-  
5 ness entity transmits, routes, or provides connec-  
6 tions. Any such business entity shall be treated as  
7 a service provider under this Act only to the extent  
8 that it is engaged in the provision of such trans-  
9 mission, routing, intermediate and transient storage  
10 or connections.

11 **TITLE I—PUNISHMENT FOR CON-**  
12 **CEALMENT OF SECURITY**  
13 **BREACHES AND TOOLS TO**  
14 **COMBAT CYBERCRIME**

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

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

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

24 “(a) IN GENERAL.—Whoever, having knowledge of a  
25 security breach and of the fact that notice of such security

1 breach is required under title II of the Consumer Privacy  
2 Protection Act of 2017, intentionally and willfully conceals  
3 the fact of such security breach, shall, in the event that  
4 such security breach results in economic harm to any indi-  
5 vidual in the amount of \$1,000 or more, be fined under  
6 this title or imprisoned for not more than 5 years, or both.

7 “(b) PERSON DEFINED.—For purposes of subsection  
8 (a), the term ‘person’ has the meaning given the term in  
9 section 1030(e)(12).”.

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

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

14 (c) ENFORCEMENT AUTHORITY.—

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

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

1 **SEC. 102. REPORTING OF CERTAIN CYBERCRIMES.**

2 Section 1030 of title 18, United States Code, is  
3 amended by striking subsection (h) and inserting the fol-  
4 lowing:

5 “(h) **REPORTING CERTAIN CRIMINAL CASES.**—Not  
6 later than 1 year after the date of the enactment of this  
7 subsection, and annually thereafter, the Attorney General  
8 shall report to the Committee on the Judiciary of the Sen-  
9 ate and the Committee on the Judiciary of the House of  
10 Representatives the number of criminal cases brought  
11 under subsection (a) that involve conduct in which—

12 “(1) the defendant—

13 “(A) exceeded authorized access to a non-  
14 governmental computer; or

15 “(B) accessed a non-governmental com-  
16 puter without authorization; and

17 “(2) the sole basis for the Government deter-  
18 mining that access to the non-governmental com-  
19 puter was unauthorized, or in excess of authoriza-  
20 tion, was that the defendant violated a contractual  
21 obligation or agreement with a service provider or  
22 employer, such as an acceptable use policy or terms  
23 of service agreement.”.

24 **SEC. 103. AUTHORITY TO SHUT DOWN BOTNETS.**

25 (a) **AMENDMENT.**—Section 1345 of title 18, United  
26 States Code, is amended—

1 (1) in the heading, by inserting “**and abuse**”  
2 after “**fraud**”;

3 (2) in subsection (a)—

4 (A) in paragraph (1)—

5 (i) in subparagraph (B), by striking  
6 “or” at the end;

7 (ii) in subparagraph (C), by inserting  
8 “or” after the semicolon; and

9 (iii) by inserting after subparagraph  
10 (C) the following:

11 “(D) violating section 1030(a)(5) where such  
12 conduct would damage (as defined in section 1030),  
13 100 or more protected computers (as defined in sec-  
14 tion 1030) during any 1-year period, including by  
15 denying access to or operation of the computers, in-  
16 stalling unwanted software on the computers, using  
17 the computers without authorization, or obtaining  
18 information from the computers without authoriza-  
19 tion;” and

20 (B) in paragraph (2), by inserting “, a vio-  
21 lation of section 1030(a)(5) as described in sub-  
22 section (a)(1)(D),” before “or a Federal”;

23 (3) in subsection (b), by adding “, except in the  
24 case of a person violating section 1030(a)(5) in the

1 manner described in subsection (a)(1)(D),” before  
2 “take such other action”; and

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

4 “(c) A restraining order or prohibition described in  
5 subsection (b), if issued in circumstances described in sub-  
6 section (a)(1)(D)—

7 “(1) may only authorize action that solely af-  
8 fects persons violating section 1030 in the manner  
9 described in subsection (a)(1)(D); and

10 “(2) may, upon application of the Attorney  
11 General—

12 “(A) specify that no cause of action shall  
13 lie in any court against a person for complying  
14 with the restraining order, prohibition, or other  
15 action; and

16 “(B) provide that the United States shall  
17 pay to such person a fee for reimbursement for  
18 such costs as are reasonably necessary and  
19 which have been directly incurred in complying  
20 with the restraining order, prohibition, or other  
21 action.

22 “(d) There are authorized to be appropriated to the  
23 Department of Justice, the Department of Homeland Se-  
24 curity, and the Department of the Treasury such sums  
25 as are necessary to implement this section, including pay-

1 ments made by the United States of a fee for reimburse-  
2 ment.”.

3 (b) TECHNICAL AND CONFORMING AMENDMENT.—

4 The table of section for chapter 63 is amended by striking  
5 the item relating to section 1345 and inserting the fol-  
6 lowing:

“1345. Injunctions against fraud and abuse.”.

7 **SEC. 104. DETERRING THE DEVELOPMENT AND SALE OF**

8 **COMPUTER AND CELL PHONE SPYING DE-**

9 **VICES.**

10 Section 1956(c)(7)(D) of title 18, United States  
11 Code, is amended by inserting “section 2512 (relating to  
12 the manufacture, distribution, possession, and advertising  
13 of wire, oral, or electronic communication intercepting de-  
14 vices),” before “section 46502”.

15 **TITLE II—CONSUMER PRIVACY**  
16 **AND SECURITY OF SENSITIVE**  
17 **PERSONALLY IDENTIFIABLE**  
18 **INFORMATION**

19 **Subtitle A—Consumer Privacy and**  
20 **Data Security Program**

21 **SEC. 201. PURPOSE AND APPLICABILITY OF CONSUMER**

22 **PRIVACY AND DATA SECURITY PROGRAM.**

23 (a) PURPOSE.—The purpose of this subtitle is to en-  
24 sure standards for developing and implementing adminis-

1 trative, technical, and physical safeguards to protect the  
2 security of sensitive personally identifiable information.

3 (b) APPLICABILITY.—A covered entity engaging in  
4 interstate commerce that collects, uses, accesses, trans-  
5 mits, stores, or disposes of sensitive personally identifiable  
6 information in electronic or digital form of not less than  
7 10,000 United States persons during any 12-month period  
8 is subject to the requirements for a consumer privacy and  
9 data security program for protecting sensitive personally  
10 identifiable information.

11 (c) LIMITATIONS.—Notwithstanding any other obli-  
12 gation under this subtitle, this subtitle does not apply to  
13 the following:

14 (1) FINANCIAL INSTITUTIONS.—Financial insti-  
15 tutions—

16 (A) subject to and in compliance with the  
17 data security requirements and standards under  
18 section 501(b) of the Gramm-Leach-Bliley Act  
19 (15 U.S.C. 6801(b)); and

20 (B) subject to the jurisdiction of an agency  
21 or authority described in section 505(a) of the  
22 Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)).

23 (2) HIPAA AND HITECH REGULATED ENTI-  
24 TIES.—An entity that is subject to and in compli-  
25 ance with the data security requirements of the fol-

1       lowing, with respect to data that is subject to such  
2       requirements:

3               (A) Section 13401 of the Health Informa-  
4               tion Technology for Economic and Clinical  
5               Health Act (42 U.S.C. 17931).

6               (B) Part 160 or 164 of title 45, Code of  
7               Federal Regulations (or any successor regula-  
8               tions).

9               (C) The regulations promulgated under  
10              section 264(c) of the Health Insurance Port-  
11              ability and Accountability Act of 1996 (42  
12              U.S.C. 1320d–2 note).

13              (D) In the case of a business associate, as  
14              defined in section 13400 of the Health Informa-  
15              tion Technology for Economic and Clinical  
16              Health Act (42 U.S.C. 17921), the applicable  
17              privacy and data security requirements of part  
18              1 of subtitle D of title XIII of division A of the  
19              American Reinvestment and Recovery Act of  
20              2009 (42 U.S.C. 17931 et seq.).

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 engaged  
24              solely in the transmission, routing, or temporary, in-



1       intermediate, or transient storage of that communica-  
2       tion.

3       **SEC. 202. REQUIREMENTS FOR CONSUMER PRIVACY AND**  
4                                   **DATA SECURITY PROGRAM.**

5       (a) CONSUMER PRIVACY AND DATA SECURITY PRO-  
6       GRAM.—A covered entity subject to this subtitle shall com-  
7       ply with the following safeguards and any other adminis-  
8       trative, technical, or physical safeguards identified by the  
9       Federal Trade Commission for the protection of sensitive  
10      personally identifiable information:

11           (1) SCOPE.—A covered entity shall implement a  
12      comprehensive consumer privacy and data security  
13      program that includes administrative, technical, and  
14      physical safeguards appropriate to the size and com-  
15      plexity, and the nature and scope, of the activities  
16      of the covered entity.

17           (2) DESIGN.—The consumer privacy and data  
18      security program shall be designed to—

19           (A) ensure the privacy and security of sen-  
20      sitive personally identifying information;

21           (B) protect against any anticipated  
22      vulnerabilities to the privacy and security of  
23      sensitive personally identifying information; and

1           (C) protect against unauthorized access,  
2           destruction, acquisition, disclosure, or use of  
3           sensitive personally identifying information.

4           (3) RISK ASSESSMENT.—A covered entity  
5           shall—

6           (A) identify reasonably foreseeable internal  
7           and external vulnerabilities and internal and ex-  
8           ternal threats that could result in unauthorized  
9           access, destruction, acquisition, disclosure, or  
10          use of sensitive personally identifiable informa-  
11          tion or of systems containing sensitive person-  
12          ally identifiable information;

13          (B) assess the likelihood of and potential  
14          damage from unauthorized access, destruction,  
15          acquisition, disclosure, or use of sensitive per-  
16          sonally identifiable information;

17          (C) assess the sufficiency of its technical,  
18          physical, and administrative controls in place to  
19          control and minimize risks from unauthorized  
20          access, destruction, acquisition, disclosure, or  
21          use of sensitive personally identifiable informa-  
22          tion; and

23          (D) assess the vulnerability of sensitive  
24          personally identifiable information during de-  
25          struction and disposal of such information, in-

1 including through the disposal or retirement of  
2 hardware.

3 (4) RISK MANAGEMENT AND CONTROL.—Each  
4 covered entity shall—

5 (A) design its consumer privacy and data  
6 security program to control the risks identified  
7 under paragraph (3);

8 (B) adopt measures commensurate with  
9 the sensitivity of the data as well as the size,  
10 complexity, nature, and scope of the activities  
11 of the covered entity that—

12 (i) controls access to sensitive person-  
13 ally identifiable information, including con-  
14 trols to authenticate and permit access  
15 only to authorized individuals;

16 (ii) detect, record, and preserve infor-  
17 mation relevant to actual and attempted  
18 fraudulent, unlawful, or unauthorized ac-  
19 cess, acquisition, disclosure, or use of sen-  
20 sitive personally identifiable information,  
21 including by employees and other individ-  
22 uals otherwise authorized to have access;

23 (iii) protect sensitive personally identi-  
24 fiable information during use, trans-  
25 mission, storage, and disposal by

1 encryption, redaction, disclosure limitation  
2 methodologies, or access controls, that are  
3 widely accepted as an effective industry  
4 practice or industry standard, or other rea-  
5 sonable means;

6 (iv) ensure that sensitive personally  
7 identifiable information is properly de-  
8 stroyed and disposed of, including during  
9 the destruction of computers and other  
10 electronic media that contain sensitive per-  
11 sonally identifiable information; and

12 (v) ensure that no third party is au-  
13 thorized to access or acquire sensitive per-  
14 sonally identifiable information in its pos-  
15 session without the covered entity first per-  
16 forming sufficient due diligence to ascer-  
17 tain, with reasonable certainty, that such  
18 information is being sought for a valid  
19 legal purpose; and

20 (C) establish a plan and procedures for  
21 minimizing the amount of sensitive personally  
22 identifiable information maintained by the cov-  
23 ered entity and the length of time such infor-  
24 mation is retained, which shall provide for the  
25 retention of sensitive personally identifiable in-

1           formation only as reasonably needed for the  
2           business purposes of such business entity or as  
3           necessary to comply with any legal obligation  
4           and only as long as so needed.

5           (5) LIMITATION.—Nothing in this subsection  
6           shall be construed to permit, and nothing does per-  
7           mit, the Federal Trade Commission to issue regula-  
8           tions requiring, or according greater legal status to,  
9           the implementation of or application of a specific  
10          technology or technological specifications for meeting  
11          the requirements of this title.

12          (b) TRAINING.—Covered entities subject to this sub-  
13          title shall take steps to ensure employee training and su-  
14          pervision for implementation of the consumer privacy and  
15          data security program of the covered entity.

16          (c) VULNERABILITY TESTING.—

17               (1) IN GENERAL.—Covered entities subject to  
18               this subtitle shall take steps to ensure regular test-  
19               ing of key technical, physical, and administrative  
20               controls for information and information systems of  
21               the consumer privacy and data security program to  
22               detect, prevent, and respond to attacks or intrusions,  
23               or other system failures.

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

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

3           (d) RELATIONSHIP TO CERTAIN PROVIDERS OF  
4 SERVICES.—In the event a covered entity subject to this  
5 subtitle engages a person or entity not subject to this sub-  
6 title (other than a service provider) to receive sensitive  
7 personally identifiable information in performing services  
8 or functions (other than the services or functions provided  
9 by a service provider) on behalf of and under the instruc-  
10 tion of such covered entity, the covered entity shall—

11           (1) exercise appropriate due diligence in select-  
12           ing the person or entity for responsibilities related to  
13           sensitive personally identifiable information, and  
14           take reasonable steps to select and retain a person  
15           or entity that is capable of maintaining appropriate  
16           controls for the privacy and security of the sensitive  
17           personally identifiable information at issue; and

18           (2) require the person or entity by contract to  
19           implement and maintain appropriate measures de-  
20           signed to meet the objectives and requirements gov-  
21           erning subtitle A.

22           (e) PERIODIC ASSESSMENT AND CONSUMER PRIVACY  
23 AND DATA SECURITY MODERNIZATION.—Each covered  
24 entity subject to this subtitle shall on a regular basis mon-  
25 itor, evaluate, and adjust, as appropriate its consumer pri-

1 vacy and data security program in light of any relevant  
2 changes in—

3 (1) technology;

4 (2) internal or external threats and  
5 vulnerabilities to sensitive personally identifiable in-  
6 formation; and

7 (3) the changing business arrangements of the  
8 covered entity, such as—

9 (A) mergers and acquisitions;

10 (B) alliances and joint ventures;

11 (C) outsourcing arrangements;

12 (D) bankruptcy; and

13 (E) changes to sensitive personally identifi-  
14 able information systems.

15 (f) CONSUMER NOTICE.—Not less frequently than  
16 once every calendar year, a covered entity shall provide,  
17 upon request of a United States resident and at no cost  
18 to that individual, notice to that individual of what sen-  
19 sitive personally identifiable information of that individual  
20 is maintained or shared by the covered entity.

21 (g) CONSUMER OPT-OUT.—

22 (1) DEFINITIONS.—In this subsection, the  
23 terms “consumer” and “file” have the meanings  
24 given the terms in section 603 of the Fair Credit  
25 Reporting Act (15 U.S.C. 1681a).

1           (2) CREDIT FREEZE.—Upon the request of a  
2           consumer, a covered entity that is a consumer re-  
3           porting agency that compiles or maintains a file on  
4           the consumer and has received appropriate proof of  
5           the identity of the requester shall place or lift a  
6           credit freeze in the file of the consumer without  
7           charge to the consumer.

8           (h) RULEMAKING.—Not later than 1 year after the  
9           date of enactment of this Act, the Federal Trade Commis-  
10          sion shall issue regulations in accordance with section 553  
11          of title 5, United States Code, to implement subsections  
12          (a) through (g).

13          (i) IMPLEMENTATION TIMELINE.—Not later than 1  
14          year after the date on which the Federal Trade Commis-  
15          sion issues the final regulations required under subsection  
16          (h), a covered entity subject to the provisions of this sub-  
17          title shall implement a consumer privacy and data security  
18          program pursuant to this subtitle.

19          **SEC. 203. FEDERAL ENFORCEMENT.**

20          (a) IN GENERAL.—The Attorney General and the  
21          Federal Trade Commission may enforce civil violations of  
22          section 201 or 202.

23          (b) CIVIL ACTIONS BY THE ATTORNEY GENERAL OF  
24          THE UNITED STATES.—



1           (1) IN GENERAL.—The Attorney General may  
2 bring a civil action in the appropriate United States  
3 district court against any covered entity that en-  
4 gages in conduct constituting a violation of this sub-  
5 title and, upon proof of such conduct by a prepon-  
6 derance of the evidence, such covered entity shall be  
7 subject to a civil penalty in an amount that is not  
8 greater than the product of the number of individ-  
9 uals whose sensitive personally identifiable informa-  
10 tion was placed at risk as a result of the violation  
11 and \$16,500.

12           (2) DETERMINATIONS.—The determination of  
13 whether a violation of a provision of this subtitle has  
14 occurred, and if so, the amount of the penalty to be  
15 imposed, if any, shall be made by the court sitting  
16 as the finder of fact. The determination of whether  
17 a violation of a provision of this subtitle was willful  
18 or intentional, and if so, the amount of the addi-  
19 tional penalty to be imposed, if any, shall be made  
20 by the court sitting as the finder of fact.

21           (3) ADDITIONAL PENALTY LIMIT.—If a court  
22 determines under paragraph (2) that a violation of  
23 a provision of this subtitle was willful or intentional  
24 and imposes an additional penalty, the court may

1 not impose an additional penalty in an amount that  
2 exceeds \$10,000,000.

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

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

10 (A) enjoining such act or practice; or

11 (B) enforcing compliance with this subtitle.

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

16 (d) CIVIL ACTIONS BY THE FEDERAL TRADE COM-  
17 MISSION.—

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

1       pliance by any person with the requirements imposed  
2       under this title.

3               (2) CIVIL PENALTIES.—

4               (A) IN GENERAL.—Any covered entity that  
5       violates the provisions of this subtitle shall be  
6       subject to a civil penalty in the amount that is  
7       not greater than the product of the number of  
8       individuals whose sensitive personally identifi-  
9       able information was placed at risk as a result  
10      of the violation and \$16,500.

11              (B) DETERMINATIONS.—The determina-  
12      tion of whether a violation of a provision of this  
13      subtitle has occurred, and if so, the amount of  
14      the penalty to be imposed, if any, shall be made  
15      by the court sitting as the finder of fact. The  
16      determination of whether a violation of a provi-  
17      sion of this subtitle was willful or intentional,  
18      and if so, the amount of the additional penalty  
19      to be imposed, if any, shall be made by the  
20      court sitting as the finder of fact.

21              (C) ADDITIONAL PENALTY LIMIT.—If a  
22      court determines under subparagraph (B) that  
23      a violation of a provision of this subtitle was  
24      willful or intentional and imposes an additional  
25      penalty, the court may not impose an additional

1           penalty in an amount that exceeds  
2           \$10,000,000.

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

19          (e) COORDINATION OF ENFORCEMENT.—

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

23               (2) LIMITATION.—The Federal Trade Commis-  
24               sion may initiate investigations under this subsection  
25               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 date of  
8 enactment of this Act, the Attorney General  
9 and the Federal Trade Commission shall enter  
10 into an agreement for coordination regarding  
11 the enforcement of this 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 (f) OTHER RIGHTS AND REMEDIES.—The rights and  
21 remedies available under this section are cumulative and  
22 shall not affect any other rights and remedies available  
23 under law.

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

25 (a) STATE ENFORCEMENT.—

1           (1) CIVIL ACTIONS.—In any case in which the  
2 attorney general of a State or any State or local law  
3 enforcement agency authorized by the State attorney  
4 general or by State statute to prosecute violations of  
5 consumer protection law, has reason to believe that  
6 a covered entity has violated section 201 or 202, the  
7 State, as *parens patriae*, may bring a civil action on  
8 behalf of the residents of that State to—

9                   (A) enjoin that act or practice;

10                   (B) enforce compliance with section 201 or  
11 202; or

12                   (C) impose a civil penalty in an amount  
13 that is not greater than the product of the  
14 number of individuals whose sensitive personally  
15 identifiable information was placed at risk as a  
16 result of the violation and \$16,500.

17           (2) PENALTY DETERMINATION.—

18                   (A) DETERMINATIONS.—The determina-  
19 tion of whether a violation of a provision of this  
20 subtitle has occurred, and if so, the amount of  
21 the penalty to be imposed, if any, shall be made  
22 by the court sitting as the finder of fact. The  
23 determination of whether a violation of a provi-  
24 sion of this subtitle was willful or intentional,  
25 and if so, the amount of the additional penalty

1 to be imposed, if any, shall be made by the  
2 court sitting as the finder of fact.

3 (B) ADDITIONAL PENALTY LIMIT.—If a  
4 court determines under subparagraph (A) that  
5 a violation of a provision of this subtitle was  
6 willful or intentional and imposes an additional  
7 penalty, the court may not impose an additional  
8 penalty in an amount that exceeds  
9 \$10,000,000.

10 (3) NOTICE.—

11 (A) IN GENERAL.—Before filing an action  
12 under this subsection, the attorney general of  
13 the State involved shall provide to the Attorney  
14 General of the United States and the Federal  
15 Trade Commission—

16 (i) a written notice of that action; and  
17 (ii) a copy of the complaint for that  
18 action.

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

1 (C) NOTIFICATION WHEN PRACTICABLE.—

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

8 (4) FEDERAL PROCEEDINGS.—Upon receiving  
9 notice under paragraph (2), the Attorney General of  
10 the United States and the Federal Trade Commis-  
11 sion shall have the right to—

12 (A) move to stay the action, pending the  
13 final disposition of a pending Federal pro-  
14 ceeding or action as described in section 203;

15 (B) initiate an action in the appropriate  
16 United States district court under section 203  
17 and move to consolidate all pending actions, in-  
18 cluding State actions, in such court;

19 (C) intervene in an action brought under  
20 paragraph (1); and

21 (D) file petitions for appeal.

22 (5) PENDING PROCEEDINGS.—If the Attorney  
23 General of the United States or the Federal Trade  
24 Commission initiates a Federal civil action for a vio-  
25 lation of this subtitle, or any regulations thereunder,



1 no attorney general of a State may bring an action  
2 for a violation of this subtitle that resulted from the  
3 same or related acts or omissions against a defend-  
4 ant named in the Federal civil action initiated by the  
5 Attorney General of the United States or the Fed-  
6 eral Trade Commission.

7 (6) RULE OF CONSTRUCTION.—For purposes of  
8 bringing any civil action under paragraph (1) noth-  
9 ing in this subtitle shall be construed to prevent an  
10 attorney general of a State from exercising the pow-  
11 ers conferred on the attorney general by the laws of  
12 that State to—

13 (A) conduct investigations;

14 (B) administer oaths and affirmations; or

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

18 (7) VENUE; SERVICE OF PROCESS.—

19 (A) VENUE.—Any action brought under  
20 subsection (a) may be brought in—

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

1 (ii) another court of competent juris-  
2 diction.

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

6 (i) is an inhabitant; or

7 (ii) may be found.

8 (b) NO PRIVATE CAUSE OF ACTION.—Nothing in  
9 this subtitle establishes a private cause of action against  
10 a business entity for violation of any provision of this sub-  
11 title.

12 **SEC. 205. RELATION TO OTHER LAWS.**

13 (a) PREEMPTION.—For any covered entity that is  
14 subject to this subtitle, the provisions of this subtitle shall  
15 supersede any other provision of Federal law, or any provi-  
16 sions of the law of any State or political subdivision of  
17 a State, requiring data security practices that are less  
18 stringent than the requirements of this subtitle.

19 (b) CONSUMER PROTECTION LAWS.—Except as pro-  
20 vided in subsection (a), this section shall not be construed  
21 to limit the enforcement of any State consumer protection  
22 law by an attorney general of a State.

23 (c) PROTECTION OF CERTAIN STATE LAWS.—Noth-  
24 ing in this Act shall be construed to preempt the applica-  
25 bility of—

1 (1) State trespass, contract, or tort law; or

2 (2) any other State law to the extent that the  
3 law relates to acts of fraud.

4 (d) PRESERVATION OF FTC AUTHORITY.—Nothing  
5 in this Act may be construed in any way to limit the au-  
6 thority of the Federal Trade Commission under any other  
7 provision of law.

8 (e) PRESERVATION OF FCC AUTHORITY.—Nothing  
9 in this Act may be construed in any way to limit the au-  
10 thority of the Federal Communications Commission under  
11 any other provision of law.

12 **Subtitle B—Security Breach**  
13 **Notification and Protection**

14 **SEC. 211. NOTICE TO INDIVIDUALS; PROTECTION.**

15 (a) IN GENERAL.—Except as provided in section 212,  
16 a covered entity shall, following the discovery of a security  
17 breach of sensitive personally identifiable information held  
18 by that covered entity or any third party entity contracted  
19 to maintain or process data in electronic form containing  
20 sensitive personally identifiable information for that cov-  
21 ered entity—

22 (1) notify any resident of the United States  
23 whose sensitive personally identifiable information  
24 has been, or is reasonably believed to have been,  
25 accessed or acquired; and

1           (2) provide 5 years of appropriate identity theft  
2 prevention and mitigation services, if any, to any in-  
3 dividual notified under paragraph (1), upon request  
4 of the individual and at no cost to the individual,  
5 under which the individual shall not be—

6           (A) automatically enrolled, without the  
7 consent of the individual, into a fee-based iden-  
8 tity theft prevention and mitigation service at  
9 the end of the 5-year period; or

10          (B) required to seek arbitration of any  
11 claim arising from the identity theft prevention  
12 and mitigation service described in subpara-  
13 graph (A).

14 (b) OBLIGATION OF THIRD PARTY ENTITIES.—

15          (1) IN GENERAL.—In the event of a breach of  
16 security of a system maintained by a third party en-  
17 tity that has been contracted to maintain or process  
18 data in electronic form containing sensitive person-  
19 ally identifiable information on behalf of a covered  
20 entity who owns or possesses such data, the third  
21 party entity shall notify the covered entity of the  
22 breach of security. Upon receiving notification from  
23 the third party entity, such covered entity shall pro-  
24 vide the notification and identify theft prevention  
25 and mitigation service required under subsection (a).

1           (2) NOTICE BY THIRD PARTY ENTITIES.—Noth-  
2           ing in this subtitle shall prevent or abrogate an  
3           agreement between a covered entity required to give  
4           notice under this section and a third party entity  
5           that has been contracted to maintain or process data  
6           in electronic form containing sensitive personally  
7           identifiable information for a covered entity, to pro-  
8           vide the notifications required under subsection  
9           (a)(1) or the identity theft prevention and mitigation  
10          service required under subsection (a)(2).

11          (3) SERVICE PROVIDERS.—If a service provider  
12          becomes aware of a security breach containing sen-  
13          sitive personally identifiable information that is  
14          owned or possessed by a covered entity that connects  
15          to or uses a system or network provided by the serv-  
16          ice provider for the purpose of transmitting, routing,  
17          or providing intermediate or transient storage of  
18          such data, the service provider shall be required to  
19          promptly notify the covered entity who initiated such  
20          connection, transmission, routing, or storage of the  
21          security breach if the covered entity can be reason-  
22          ably identified. Upon receiving such notification  
23          from a service provider, the covered entity shall be  
24          required to provide the notification and identity

1 theft prevention and mitigation service required  
2 under subsection (a).

3 (c) TIMELINESS OF NOTIFICATION.—

4 (1) IN GENERAL.—All notifications and identity  
5 theft prevention and mitigation services required  
6 under this section shall be made as expediently as  
7 possible and without unreasonable delay following  
8 the discovery by the covered entity of a security  
9 breach.

10 (2) REASONABLE DELAY.—Reasonable delay  
11 under this subsection may include any reasonable  
12 time necessary to determine the scope of the security  
13 breach, prevent further disclosures, and provide no-  
14 tice to law enforcement when required. Except as  
15 provided in subsection (d), delay of notification or  
16 provision of identity theft prevention and mitigation  
17 service shall not exceed 7 days following the dis-  
18 covery of a security breach.

19 (3) BURDEN OF PRODUCTION.—The covered  
20 entity required to provide notice and identity theft  
21 prevention and mitigation service under this subtitle  
22 shall, upon the request of the Attorney General of  
23 the United States or the Federal Trade Commission  
24 provide records or other evidence of the notifications  
25 and identity theft prevention and mitigation service

1 required under this subtitle, including to the extent  
2 applicable, the reasons for any delay of notification  
3 or provision of identity theft prevention and mitiga-  
4 tion service.

5 (d) DELAY AUTHORIZED FOR LAW ENFORCEMENT  
6 OR NATIONAL SECURITY PURPOSES.—

7 (1) IN GENERAL.—If a Federal law enforce-  
8 ment agency or intelligence agency determines that  
9 the notification or provision of identity theft preven-  
10 tion and mitigation service required under this sec-  
11 tion would impede a criminal investigation, or na-  
12 tional security activity, such notification or provision  
13 of identity theft prevention and mitigation service,  
14 as the case may be, shall be delayed upon written  
15 notice from a Federal law enforcement agency or in-  
16 telligence agency to the covered entity that experi-  
17 enced the security breach. The notification from a  
18 Federal law enforcement agency or intelligence agen-  
19 cy shall specify in writing the period of delay re-  
20 quested for law enforcement or national security  
21 purposes.

22 (2) EXTENDED DELAY.—If the notification or  
23 provision of identity theft prevention and mitigation  
24 service required under subsection (a) is delayed pur-  
25 suant to paragraph (1), a covered entity shall give

1 notice or identity theft prevention and mitigation  
2 service, as the case may be, 15 days after the day  
3 such law enforcement or national security delay was  
4 invoked unless a Federal law enforcement or intel-  
5 ligence agency provides written notification that fur-  
6 ther delay is necessary.

7 (3) LAW ENFORCEMENT IMMUNITY.—No non-  
8 constitutional cause of action shall lie in any court  
9 against any agency for acts relating to the delay of  
10 notification for law enforcement or national security  
11 purposes under this subtitle.

12 (e) LIMITATIONS.—Notwithstanding any other obli-  
13 gation under this subtitle, this subtitle does not apply to  
14 the following:

15 (1) FINANCIAL INSTITUTIONS.—Financial insti-  
16 tutions—

17 (A) subject to and in compliance with the  
18 data security requirements and standards under  
19 section 501(b) of the Gramm-Leach-Bliley Act  
20 (15 U.S.C. 6801(b)); and

21 (B) subject to the jurisdiction of an agency  
22 or authority described in section 505(a) of the  
23 Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)).

24 (2) HIPAA AND HITECH REGULATED ENTI-  
25 TIES.—An entity that is subject to and in compli-



1       ance with the data breach notification of the fol-  
2       lowing, with respect to data that is subject to such  
3       requirements:

4               (A) Section 13401 of the Health Informa-  
5               tion Technology for Economic and Clinical  
6               Health Act (42 U.S.C. 17931).

7               (B) Part 160 or 164 of title 45, Code of  
8               Federal Regulations (or any successor regula-  
9               tions).

10              (C) The regulations promulgated under  
11              section 264(c) of the Health Insurance Port-  
12              ability and Accountability Act of 1996 (42  
13              U.S.C. 1320d-2 note).

14              (D) In the case of a business entity, the  
15              applicable data breach notification requirements  
16              of part 1 of subtitle D of title XIII of division  
17              A of the American Reinvestment and Recovery  
18              Act of 2009 (42 U.S.C. 17931 et seq.), if such  
19              business entity is acting as a covered entity, a  
20              business associate, or a vendor of personal  
21              health records, as those terms are defined in  
22              section 13400 of the Health Information Tech-  
23              nology for Economic and Clinical Health Act  
24              (42 U.S.C. 17921).

1           (E) In the case of and third party service  
2           provider, section 13407 of the Health Informa-  
3           tion Technology for Economic and Clinical  
4           Health Act (42 U.S.C. 17937).

5 **SEC. 212. EXEMPTIONS.**

6           (a) NATIONAL SECURITY AND LAW ENFORCEMENT  
7 EXEMPTION.—

8           (1) IN GENERAL.—Section 211 shall not apply  
9           to a covered entity if a Federal law enforcement  
10          agency or intelligence agency—

11           (A) determines that notification of the se-  
12          curity breach—

13           (i) could be expected to reveal sen-  
14          sitive sources and methods or similarly im-  
15          pede the ability of the Government to con-  
16          duct law enforcement investigations; or

17           (ii) could be expected to cause damage  
18          to the national security;

19           (B) communicates the determination made  
20          under subparagraph (A) to the covered entity;  
21          and

22           (C) orders that notification required under  
23          section 211 not be made.

24           (2) IMMUNITY.—No non-constitutional cause of  
25          action shall lie in any court against any Federal

1 agency for acts relating to the exemption from noti-  
2 fication for law enforcement or national security  
3 purposes under this title.

4 (b) **SAFE HARBOR EXEMPTION.**—A covered entity  
5 shall be exempt from the notice and identity theft preven-  
6 tion and mitigation service requirements under section  
7 211 if the covered entity reasonably determines that sen-  
8 sitive personally identifiable information is rendered unus-  
9 able, unreadable, or indecipherable through data security  
10 technology or methodology, including encryption or redac-  
11 tion, that is generally accepted by experts in the field of  
12 information security, such that there is no reasonable like-  
13 lihood that a security breach has resulted in, or will result  
14 in, the misuse of data.

15 **SEC. 213. METHODS OF NOTICE.**

16 A covered entity shall be in compliance with section  
17 211 if the covered entity provides the following:

18 (1) **INDIVIDUAL NOTICE.**—Notice to individuals  
19 by 1 of the following means if the method of notifi-  
20 cation selected can most likely be expected to reach  
21 the intended individual:

22 (A) Written notification to the last known  
23 home mailing address of the individual in the  
24 records of the covered entity.

1 (B) Telephone notice to the individual per-  
2 sonally, provided that the telephone notice is  
3 made directly to each affected consumer, and is  
4 not made through a prerecorded message.

5 (C) E-mail notice, if—

6 (i)(I) the covered entity's primary  
7 method of communication with the indi-  
8 vidual is by e-mail; or

9 (II) the individual has consented to  
10 receive such notice and the notice is con-  
11 sistent with the provisions permitting elec-  
12 tronic transmission of notices under sec-  
13 tion 101 of the Electronic Signatures in  
14 Global and National Commerce Act (15  
15 U.S.C. 7001); and

16 (ii) the e-mail notice does not request,  
17 or contain a hypertext link to a request,  
18 that the consumer provide personal infor-  
19 mation in response to the notice.

20 (2) MEDIA, WEBSITE, AND SOCIAL MEDIA NO-  
21 TICE.—In the event notice is required to more than  
22 5,000 individuals in 1 State and individual notice is  
23 not feasible due to lack of sufficient contact informa-  
24 tion for the individuals required to be notified, a cov-  
25 ered entity shall—

1 (A) provide notice to the major media out-  
2 lets serving the State or jurisdiction of the indi-  
3 viduals believed to be affected;

4 (B) place notice in a clear and conspicuous  
5 place on the website of the covered entity if the  
6 covered entity operates a website; and

7 (C) place notice on each social media plat-  
8 form on which the covered entity maintains a  
9 social media presence, if any.

10 **SEC. 214. CONTENT OF NOTIFICATION.**

11 (a) IN GENERAL.—Regardless of the method by  
12 which notice is provided to individuals under section 213,  
13 such notice shall include, to the extent possible—

14 (1) a general description of the incident and the  
15 date or estimated date of the security breach and  
16 the date range during which the sensitive personally  
17 identifiable information was compromised;

18 (2) a description of the categories of sensitive  
19 personally identifiable information that was, or is  
20 reasonably believed to have been, accessed or ac-  
21 quired by an unauthorized person;

22 (3) the acts the covered entity, or the agent of  
23 the covered entity, has taken to protect sensitive  
24 personally identifiable information from further se-  
25 curity breach;

1           (4) at the discretion of the covered entity, rea-  
2           sonable advice on steps the individual may take to  
3           protect himself or herself;

4           (5) if applicable, an offer to provide appropriate  
5           identity theft prevention and mitigation services, as  
6           described in section 211(a)(2);

7           (6) a toll-free number—

8                 (A) that the individual may use to contact  
9                 the covered entity, or the agent of the covered  
10                entity; and

11               (B) from which the individual may learn  
12                what types of sensitive personally identifiable  
13                information the covered entity maintained about  
14                that individual; and

15           (7) the toll-free contact telephone numbers and  
16           addresses for the major credit reporting agencies if  
17           the sensitive personally identifiable information that  
18           was breached could be used to commit financial  
19           fraud or identity theft.

20           (b) **DIRECT BUSINESS RELATIONSHIP.**—Regardless  
21           of whether a covered entity or a designated third party  
22           provides the notice required pursuant to section 211(b),  
23           such notice shall include the name of the covered entity  
24           that has the most direct relationship with the individual  
25           being notified.

1 **SEC. 215. COORDINATION OF NOTIFICATION WITH CREDIT**  
2 **REPORTING AGENCIES.**

3 If a covered entity is required to provide notification  
4 to more than 5,000 individuals under section 211(a) and  
5 the sensitive personally identifiable information that was  
6 breached could be used to commit financial fraud or iden-  
7 tity theft, the covered entity shall also notify all consumer  
8 reporting agencies that compile and maintain files on con-  
9 sumers on a nationwide basis (as defined in section 603(p)  
10 of the Fair Credit Reporting Act (15 U.S.C. 1681a(p))  
11 of the timing and distribution of the notices. Such notice  
12 shall be given to the consumer credit reporting agencies  
13 without unreasonable delay and, if it will not delay notice  
14 to the affected individuals, prior to the distribution of no-  
15 tices to the affected individuals.

16 **SEC. 216. NOTICE TO THE FEDERAL TRADE COMMISSION.**

17 (a) IN GENERAL.—A covered entity required to pro-  
18 vide notification under section 211(a) shall provide a copy  
19 of the notification to the Federal Trade Commission not  
20 later than the date on which notice is provided to individ-  
21 uals required to be notified. The Federal Trade Commis-  
22 sion shall establish procedures to ensure the attorneys  
23 general of each State with affected residents receives a  
24 copy of the notice provided to it under this section.

25 (b) PUBLIC DATABASE AND REPORT TO CON-  
26 GRESS.—The Federal Trade Commission shall—

1           (1) maintain a public database on the website  
2 of the Federal Trade Commission of notifications re-  
3 ceived under subsection (a); and

4           (2) on an annual basis, submit a report to Con-  
5 gress on the notifications received under subsection  
6 (a).

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

8           (a) DESIGNATION OF GOVERNMENT ENTITY TO RE-  
9 CEIVE NOTICE.—

10           (1) IN GENERAL.—Not later than 60 days after  
11 the date of enactment of this Act, the Secretary of  
12 Homeland Security, in consultation with the Attor-  
13 ney General, shall designate a Federal Government  
14 entity to receive the notices required under section  
15 211 and this section.

16           (2) RESPONSIBILITIES OF THE DESIGNATED  
17 ENTITY.—The designated entity shall—

18           (A) promptly provide the information that  
19 it receives to the United States Secret Service  
20 or the Federal Bureau of Investigation for law  
21 enforcement purposes; and

22           (B) provide the information described in  
23 subparagraph (A) as appropriate to other Fed-  
24 eral agencies for law enforcement, national se-  
25 curity, or data security purposes.



1 (b) NOTICE.—A covered entity shall notify the des-  
2 ignated entity of the fact that a security breach has oc-  
3 curred if—

4 (1) the number of individuals whose sensitive  
5 personally identifying information was, or is reason-  
6 ably believed to have been, accessed or acquired by  
7 an unauthorized person exceeds 5,000;

8 (2) the security breach involves a database,  
9 networked or integrated databases, or other data  
10 system containing the sensitive personally identifi-  
11 able information of more than 500,000 individuals  
12 nationwide;

13 (3) the security breach involves databases  
14 owned by the Federal Government; or

15 (4) the security breach involves primarily sen-  
16 sitive personally identifiable information of individ-  
17 uals known to the covered entity to be employees  
18 and contractors of the Federal Government involved  
19 in national security or law enforcement.

20 (c) DEPARTMENT OF JUSTICE REVIEW OF THRESH-  
21 OLDS FOR NOTICE.—The Attorney General, in consulta-  
22 tion with the Secretary of Homeland Security, after notice  
23 and the opportunity for public comment, and in a manner  
24 consistent with this section, shall promulgate regulations,  
25 as necessary, under section 553 of title 5, United States

1 Code, to adjust the thresholds for notice to law enforce-  
2 ment and national security authorities under subsection  
3 (a) and to facilitate the purposes of this section.

4 (d) **TIMING.**—The notice required under subsection  
5 (b) shall be provided as promptly as possible, but such  
6 notice must be provided not less than 48 hours before no-  
7 tice is provided to an individual pursuant to section 211,  
8 or not later than 7 days after the discovery of the events  
9 requiring notice, whichever occurs first. For each breach  
10 requiring notice under this subsection, a copy of the notice  
11 to individuals required under section 211 shall also be pro-  
12 vided to the designated entity not later than the date on  
13 which the notice is provided to affected individuals.

14 **SEC. 218. FEDERAL ENFORCEMENT.**

15 (a) **IN GENERAL.**—The Attorney General and the  
16 Federal Trade Commission may enforce civil violations of  
17 this subtitle.

18 (b) **CIVIL ACTIONS BY THE ATTORNEY GENERAL OF**  
19 **THE UNITED STATES.**—

20 (1) **IN GENERAL.**—The Attorney General may  
21 bring a civil action in the appropriate United States  
22 district court against any covered entity that en-  
23 engages in conduct constituting a violation of this sub-  
24 title and, upon proof of such conduct by a prepon-  
25 derance of the evidence, the covered entity shall be

1 subject to a civil penalty in an amount not greater  
2 than the product of the number of violations of this  
3 subtitle and \$16,500. Each failure to provide notifi-  
4 cation to an individual as required under this sub-  
5 title shall be treated as a separate violation.

6 (2) DETERMINATIONS.—The determination of  
7 whether a violation of a provision of this subtitle has  
8 occurred, and if so, the amount of the penalty to be  
9 imposed, if any, shall be made by the court sitting  
10 as the finder of fact. The determination of whether  
11 a violation of a provision of this subtitle was willful  
12 or intentional, and if so, the amount of the addi-  
13 tional penalty to be imposed, if any, shall be made  
14 by the court sitting as the finder of fact.

15 (3) ADDITIONAL PENALTY LIMIT.—If a court  
16 determines under paragraph (2) that a violation of  
17 a provision of this subtitle was willful or intentional  
18 and imposes an additional penalty, the court may  
19 not impose an additional penalty in an amount that  
20 exceeds \$10,000,000.

21 (c) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-  
22 ERAL.—

23 (1) IN GENERAL.—If it appears that a covered  
24 entity has engaged, or is engaged, in any act or  
25 practice constituting a violation of this subtitle, the

1 Attorney General may petition an appropriate dis-  
2 trict court of the United States for an order—

3 (A) enjoining such act or practice; or

4 (B) enforcing compliance with this subtitle.

5 (2) ISSUANCE OF ORDER.—A court may issue  
6 an order under paragraph (1), if the court finds that  
7 the conduct in question constitutes a violation of this  
8 subtitle.

9 (d) CIVIL ACTIONS BY THE FEDERAL TRADE COM-  
10 MISSION.—

11 (1) IN GENERAL.—Compliance with the require-  
12 ments imposed under this subtitle may be enforced  
13 under the Federal Trade Commission Act (15  
14 U.S.C. 41 et seq.) by the Federal Trade Commission  
15 with respect to business entities subject to this Act.  
16 All of the functions and powers of the Federal Trade  
17 Commission under the Federal Trade Commission  
18 Act are available to the Commission to enforce com-  
19 pliance by any person with the requirements imposed  
20 under this title.

21 (2) CIVIL PENALTIES.—

22 (A) IN GENERAL.—Any covered entity that  
23 violates this subtitle shall be subject to a civil  
24 penalty in the amount that is not greater than  
25 the product of the number of violations of this

1 subtitle and \$16,500. Each failure to provide  
2 notification to an individual as required under  
3 this subtitle shall be treated as a separate viola-  
4 tion.

5 (B) DETERMINATIONS.—The determina-  
6 tion of whether a violation of a provision of this  
7 subtitle has occurred, and if so, the amount of  
8 the penalty to be imposed, if any, shall be made  
9 by the court sitting as the finder of fact. The  
10 determination of whether a violation of a provi-  
11 sion of this subtitle was willful or intentional,  
12 and if so, the amount of the additional penalty  
13 to be imposed, if any, shall be made by the  
14 court sitting as the finder of fact.

15 (C) ADDITIONAL PENALTY LIMIT.—If a  
16 court determines under subparagraph (B) that  
17 a violation of a provision of this subtitle was  
18 willful or intentional and imposes an additional  
19 penalty, the court may not impose an additional  
20 penalty in an amount that exceeds  
21 \$10,000,000.

22 (3) UNFAIR OR DECEPTIVE ACTS OR PRAC-  
23 TICES.—For the purpose of the exercise by the Fed-  
24 eral Trade Commission of its functions and powers  
25 under the Federal Trade Commission Act, a viola-

1       tion of any requirement or prohibition imposed  
2       under this title shall constitute an unfair or decep-  
3       tive act or practice in commerce in violation of a  
4       regulation under section 18(a)(1)(B) of the Federal  
5       Trade Commission Act (15 U.S.C. 57a(a)(I)(B)) re-  
6       garding unfair or deceptive acts or practices and  
7       shall be subject to enforcement by the Federal Trade  
8       Commission under that Act with respect to any busi-  
9       ness entity, irrespective of whether that business en-  
10      tity is engaged in commerce or meets any other ju-  
11      risdictional tests in the Federal Trade Commission  
12      Act.

13      (e) COORDINATION OF ENFORCEMENT.—

14           (1) IN GENERAL.—When opening an investiga-  
15      tion, the Federal Trade Commission shall consult  
16      with the Attorney General.

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

22           (3) COORDINATION AGREEMENT.—

23           (A) IN GENERAL.—In order to avoid con-  
24      flicts and promote consistency regarding the en-  
25      forcement and litigation of matters under this

1 Act, not later than 180 days after the enact-  
2 ment of this Act, the Attorney General and the  
3 Federal Trade Commission shall enter into an  
4 agreement for coordination regarding the en-  
5 forcement of this Act.

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

14 (f) RULEMAKING.—The Federal Trade Commission  
15 may, in consultation with the Attorney General, issue such  
16 other regulations as it determines to be necessary to carry  
17 out this subtitle. All regulations promulgated under this  
18 Act shall be issued in accordance with section 553 of title  
19 5, United States Code.

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

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

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

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

6 (a) IN GENERAL.—

7 (1) CIVIL ACTIONS.—

8 (A) IN GENERAL.—In any case in which  
9 the attorney general of a State or any State or  
10 local law enforcement agency authorized by the  
11 State attorney general or by State statute to  
12 prosecute violations of consumer protection law,  
13 has reason to believe that a covered entity has  
14 violated this subtitle, the State, as *parens*  
15 *patriae*, may bring a civil action on behalf of  
16 the residents of the State to—

17 (i) enjoin that practice;

18 (ii) enforce compliance with this sub-  
19 title; or

20 (iii) impose a civil penalty in an  
21 amount not greater than the product of  
22 the number of violations of this subtitle  
23 and \$16,500.

24 (B) FAILURE TO PROVIDE NOTIFICA-  
25 TION.—For purposes of subparagraph (A)(iii),



1 each failure to provide notification to an indi-  
2 vidual as required under this subtitle shall be  
3 treated as a separate violation.

4 (2) PENALTY DETERMINATIONS.—

5 (A) DETERMINATIONS.—The determina-  
6 tion of whether a violation of a provision of this  
7 subtitle has occurred, and if so, the amount of  
8 the penalty to be imposed, if any, shall be made  
9 by the court sitting as the finder of fact. The  
10 determination of whether a violation of a provi-  
11 sion of this subtitle was willful or intentional,  
12 and if so, the amount of the additional penalty  
13 to be imposed, if any, shall be made by the  
14 court sitting as the finder of fact.

15 (B) ADDITIONAL PENALTY LIMIT.—If a  
16 court determines under subparagraph (A) that  
17 a violation of a provision of this subtitle was  
18 willful or intentional and imposes an additional  
19 penalty, the court may not impose an additional  
20 penalty in an amount that exceeds  
21 \$10,000,000.

22 (3) NOTICE.—

23 (A) IN GENERAL.—Before filing an action  
24 under paragraph (1), the attorney general of  
25 the State involved shall provide to the Attorney

1           General of the United States and the Federal  
2           Trade Commission—

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          of the United States and the Federal  
19          Trade Commission at the time the State  
20          attorney general files the action.

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

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

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

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

10          (4) file petitions for appeal.

11          (c) PENDING PROCEEDINGS.—If the Attorney Gen-  
12          eral or the Federal Trade Commission initiates a criminal  
13          proceeding or civil action for a violation of a provision of  
14          this subtitle, or any regulations thereunder, no attorney  
15          general of a State may bring an action for a violation of  
16          a provision of this subtitle against a defendant named in  
17          the Federal criminal proceeding or civil action.

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

24                 (1) conduct investigations;

25                 (2) administer oaths or affirmations; or

1           (3) compel the attendance of witnesses or the  
2 production of documentary and other evidence.

3           (e) VENUE; SERVICE OF PROCESS.—

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

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

10           (B) another court of competent jurisdic-  
11 tion.

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

15           (A) is an inhabitant; or

16           (B) may be found.

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

21 **SEC. 220. EFFECT ON FEDERAL AND STATE LAW.**

22           (a) PREEMPTION.—For a covered entity that is sub-  
23 ject to this subtitle, the provisions of this subtitle shall  
24 supersede any other provision of Federal law, or any provi-  
25 sions of the law of any State or political subdivision of

1 a State requiring notification of a security breach of sen-  
2 sitive personally identifiable information, which is less  
3 stringent than the requirements of this subtitle.

4 (b) CONSUMER PROTECTION LAWS.—Except as pro-  
5 vided in subsection (a), this section shall not be construed  
6 to limit the enforcement of any State consumer protection  
7 law by an attorney general of a State.

8 (c) PROTECTION OF CERTAIN STATE LAWS.—Noth-  
9 ing in this Act shall be construed to preempt the applica-  
10 bility of—

11 (1) State trespass, contract, or tort law; or

12 (2) any other State law to the extent that the  
13 law relates to acts of fraud.

14 (d) PRESERVATION OF FTC AUTHORITY.—Nothing  
15 in this Act may be construed in any way to limit the au-  
16 thority of the Federal Trade Commission under any other  
17 provision of law.

18 (e) PRESERVATION OF FCC AUTHORITY.—Nothing  
19 in this Act may be construed in any way to limit the au-  
20 thority of the Federal Communications Commission under  
21 any other provision of law.

22 **SEC. 221. REPORTING ON EXEMPTIONS.**

23 Not later than 18 months after the date of enactment  
24 of this Act, and upon the request by Congress thereafter,  
25 the Attorney General, in consultation with the Secretary

1 of Homeland Security, shall submit a report to Congress  
2 on the number and nature of security breaches subject to  
3 the national security and law enforcement exemptions  
4 under section 212(a).

5 **SEC. 222. EFFECTIVE DATE.**

6 This subtitle shall take effect on the expiration of the  
7 date that is 90 days after the date of enactment of this  
8 Act.

9 **TITLE III—COMPLIANCE WITH**  
10 **STATUTORY PAY-AS-YOU-GO ACT**

11 **SEC. 301. BUDGET COMPLIANCE.**

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