

115TH CONGRESS  
1ST SESSION

# S. 2124

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

NOVEMBER 14, 2017

Mr. LEAHY (for himself, Mr. MARKEY, Mr. BLUMENTHAL, Mr. WYDEN, Mr. FRANKEN, Ms. BALDWIN, and Ms. HARRIS) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

## 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,*

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

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

4 (b) TABLE OF CONTENTS.—The table of contents for  
5 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.

1 **SEC. 2. FINDINGS.**

2 Congress finds that—

3 (1) databases of sensitive personally identifiable  
4 information are increasingly prime targets of hack-  
5 ers, nation-state actors, identity thieves, rogue em-  
6 ployees, and other criminals, including organized  
7 and sophisticated criminal operations;

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

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

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

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

1           (6) individuals whose personal information has  
2           been compromised or who have been victims of iden-  
3           tity theft should receive the necessary information  
4           and assistance to mitigate any potential damage.

5 **SEC. 3. DEFINITIONS.**

6           In this Act, the following definitions shall apply:

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

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

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

18          (4) **CONSUMER PRIVACY AND DATA SECURITY**  
19          **PROGRAM.**—The term “consumer privacy and data  
20          security program” means the program described in  
21          section 202(a).

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

1           (6) COVERED ENTITY.—The term “covered en-  
2           tity” means any business entity, other than a service  
3           provider, that collects, uses, accesses, transmits,  
4           stores, or disposes of sensitive personally identifiable  
5           information, including a consumer reporting agency.

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

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

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

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

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

25          (10) SECURITY BREACH.—

1 (A) IN GENERAL.—The term “security  
2 breach” means compromise of the privacy, in-  
3 tegrity, or security of computerized data that  
4 results in, or that there is a reasonable basis to  
5 conclude has resulted in, unauthorized access to  
6 or acquisition of sensitive personally identifiable  
7 information.

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

10 (i) a good faith access or acquisition  
11 of sensitive personally identifiable informa-  
12 tion by a business entity, or an employee  
13 or agent of a business entity, if the sen-  
14 sitive personally identifiable information is  
15 not subject to further unauthorized disclo-  
16 sure;

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

20 (iii) any lawfully authorized investiga-  
21 tive, protective, or intelligence activity of a  
22 law enforcement or intelligence agency of  
23 the United States, a State, or a political  
24 subdivision of a State.

1           (11) SENSITIVE PERSONALLY IDENTIFIABLE IN-  
2           FORMATION.—The term “sensitive personally identi-  
3           fiable information” means any information or com-  
4           pilation of information, in electronic or digital form  
5           that identifies or could be used to identify a par-  
6           ticular person, including the following:

7                   (A) A non-truncated Social Security num-  
8                   ber, a driver’s license number, passport num-  
9                   ber, or alien registration number or other gov-  
10                  ernment-issued unique identification number.

11                  (B) A financial account number or credit  
12                  or debit card number in combination with any  
13                  security code, access code, or password if re-  
14                  quired for an individual to obtain credit, with-  
15                  draw funds, or engage in financial transactions.

16                  (C) A unique electronic account identifier,  
17                  including an online user name or e-mail ad-  
18                  dress, in combination with any security code,  
19                  access code, password, or security question and  
20                  answer, if required for an individual to obtain  
21                  money, goods, services, access to digital photo-  
22                  graphs, digital videos or electronic communica-  
23                  tions, or any other thing of value.

24                  (D) Unique biometric data, such as  
25                  faceprint, fingerprint, voice print, a retina or

1 iris image, or any other unique physical rep-  
2 resentation.

3 (E) An individual's first and last name or  
4 first initial and last name in combination with  
5 any information that relates to the individual's  
6 past, present, or future physical or mental  
7 health or condition, or to the provision of health  
8 care to or diagnosis of the individual, including  
9 health insurance information such as a health  
10 insurance policy number or subscriber identi-  
11 fication number, or any information in an indi-  
12 vidual's health insurance application and claims  
13 history.

14 (F) Information about an individual's geo-  
15 graphic location generated by or derived from  
16 the operation or use of an electronic commu-  
17 nications device that is sufficient to identify the  
18 street and name of the city or town in which  
19 the device is located, excluding telephone num-  
20 bers or network or internet protocol addresses.

21 (G) Password-protected digital photo-  
22 graphs and digital videos not otherwise avail-  
23 able to the public.

24 (12) SERVICE PROVIDER.—The term “service  
25 provider” means a business entity that provides elec-



1       tronic data transmission, routing, intermediate and  
2       transient storage, or connections to its system or  
3       network, where the business entity providing such  
4       services does not select or modify the content of the  
5       electronic data, is not the sender or the intended re-  
6       cipient of the data, and the business entity trans-  
7       mits, routes, or provides connections for sensitive  
8       personally identifiable information in a manner that  
9       sensitive personally identifiable information is undif-  
10      ferentiated from other types of data that such busi-  
11      ness entity transmits, routes, or provides connec-  
12      tions. Any such business entity shall be treated as  
13      a service provider under this Act only to the extent  
14      that it is engaged in the provision of such trans-  
15      mission, routing, intermediate and transient storage  
16      or connections.

1 **TITLE I—PUNISHMENT FOR CON-**  
 2 **CEALMENT OF SECURITY**  
 3 **BREACHES AND TOOLS TO**  
 4 **COMBAT CYBERCRIME**

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

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

11 **“§ 1041. Concealment of security breaches involving**  
 12 **sensitive personally identifiable informa-**  
 13 **tion**

14 “(a) IN GENERAL.—Whoever, having knowledge of a  
 15 security breach and of the fact that notice of such security  
 16 breach is required under title II of the Consumer Privacy  
 17 Protection Act of 2017, intentionally and willfully conceals  
 18 the fact of such security breach, shall, in the event that  
 19 such security breach results in economic harm to any indi-  
 20 vidual in the amount of \$1,000 or more, be fined under  
 21 this title or imprisoned for not more than 5 years, or both.

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

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

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

5 (c) ENFORCEMENT AUTHORITY.—

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

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

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

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

18 “(h) REPORTING CERTAIN CRIMINAL CASES.—Not  
19 later than 1 year after the date of the enactment of this  
20 subsection, and annually thereafter, the Attorney General  
21 shall report to the Committee on the Judiciary of the Sen-  
22 ate and the Committee on the Judiciary of the House of  
23 Representatives the number of criminal cases brought  
24 under subsection (a) that involve conduct in which—

1 “(1) the defendant—

2 “(A) exceeded authorized access to a non-  
3 governmental computer; or

4 “(B) accessed a nongovernmental com-  
5 puter without authorization; and

6 “(2) the sole basis for the Government deter-  
7 mining that access to the nongovernmental computer  
8 was unauthorized, or in excess of authorization, was  
9 that the defendant violated a contractual obligation  
10 or agreement with a service provider or employer,  
11 such as an acceptable use policy or terms of service  
12 agreement.”.

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

14 (a) AMENDMENT.—Section 1345 of title 18, United  
15 States Code, is amended—

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

18 (2) in subsection (a)—

19 (A) in paragraph (1)—

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

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

24 (iii) by inserting after subparagraph  
25 (C) the following:

1           “(D) violating section 1030(a)(5) where such  
2           conduct would damage (as defined in section 1030),  
3           100 or more protected computers (as defined in sec-  
4           tion 1030) during any 1-year period, including by  
5           denying access to or operation of the computers, in-  
6           stalling unwanted software on the computers, using  
7           the computers without authorization, or obtaining  
8           information from the computers without authoriza-  
9           tion;” and

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

13           (3) in subsection (b), by adding “, except in the  
14           case of a person violating section 1030(a)(5) in the  
15           manner described in subsection (a)(1)(D),” before  
16           “take such other action”; and

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

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

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

24                   “(2) may, upon application of the Attorney  
25                   General—

1           “(A) specify that no cause of action shall  
2           lie in any court against a person for complying  
3           with the restraining order, prohibition, or other  
4           action; and

5           “(B) provide that the United States shall  
6           pay to such person a fee for reimbursement for  
7           such costs as are reasonably necessary and  
8           which have been directly incurred in complying  
9           with the restraining order, prohibition, or other  
10          action.

11          “(d) There are authorized to be appropriated to the  
12          Department of Justice, the Department of Homeland Se-  
13          curity, and the Department of the Treasury such sums  
14          as are necessary to implement this section, including pay-  
15          ments made by the United States of a fee for reimburse-  
16          ment.”.

17          (b) TECHNICAL AND CONFORMING AMENDMENT.—  
18          The table of sections for chapter 63 is amended by strik-  
19          ing the item relating to section 1345 and inserting the  
20          following:

          “1345. Injunctions against fraud and abuse.”.

21      **SEC. 104. DETERRING THE DEVELOPMENT AND SALE OF**  
22                              **COMPUTER AND CELL PHONE SPYING DE-**  
23                              **VICES.**

24          Section 1956(c)(7)(D) of title 18, United States  
25          Code, is amended by inserting “section 2512 (relating to

1 the manufacture, distribution, possession, and advertising  
2 of wire, oral, or electronic communication intercepting de-  
3 vices),” before “section 46502”.

4 **TITLE II—CONSUMER PRIVACY**  
5 **AND SECURITY OF SENSITIVE**  
6 **PERSONALLY IDENTIFIABLE**  
7 **INFORMATION**

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

10 **SEC. 201. PURPOSE AND APPLICABILITY OF CONSUMER**  
11 **PRIVACY AND DATA SECURITY PROGRAM.**

12 (a) **PURPOSE.**—The purpose of this subtitle is to en-  
13 sure standards for developing and implementing adminis-  
14 trative, technical, and physical safeguards to protect the  
15 security of sensitive personally identifiable information.

16 (b) **APPLICABILITY.**—A covered entity engaging in  
17 interstate commerce that collects, uses, accesses, trans-  
18 mits, stores, or disposes of sensitive personally identifiable  
19 information in electronic or digital form of not less than  
20 10,000 United States persons during any 12-month period  
21 is subject to the requirements for a consumer privacy and  
22 data security program for protecting sensitive personally  
23 identifiable information.

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

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

6 (A) subject to and in compliance with the  
7 data security requirements and standards under  
8 section 501(b) of the Gramm-Leach-Bliley Act  
9 (15 U.S.C. 6801(b)); and

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

13 (2) HIPAA AND HITECH REGULATED ENTI-  
14 TIES.—An entity that is subject to and in compli-  
15 ance with the data security requirements of the fol-  
16 lowing, with respect to data that is subject to such  
17 requirements:

18 (A) Section 13401 of the Health Informa-  
19 tion Technology for Economic and Clinical  
20 Health Act (42 U.S.C. 17931).

21 (B) Part 160 or 164 of title 45, Code of  
22 Federal Regulations (or any successor regula-  
23 tions).

24 (C) The regulations promulgated under  
25 section 264(c) of the Health Insurance Port-



1 ability and Accountability Act of 1996 (42  
2 U.S.C. 1320d–2 note).

3 (D) In the case of a business associate, as  
4 defined in section 13400 of the Health Informa-  
5 tion Technology for Economic and Clinical  
6 Health Act (42 U.S.C. 17921), the applicable  
7 privacy and data security requirements of part  
8 1 of subtitle D of title XIII of division A of the  
9 American Reinvestment and Recovery Act of  
10 2009 (42 U.S.C. 17931 et seq.).

11 (3) SERVICE PROVIDERS.—A service provider  
12 for any electronic communication by a third party,  
13 to the extent that the service provider is engaged  
14 solely in the transmission, routing, or temporary, in-  
15 termediate, or transient storage of that communica-  
16 tion.

17 **SEC. 202. REQUIREMENTS FOR CONSUMER PRIVACY AND**  
18 **DATA SECURITY PROGRAM.**

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

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

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

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

11                  (B) protect against any anticipated  
12                  vulnerabilities to the privacy and security of  
13                  sensitive personally identifying information; and

14                  (C) protect against unauthorized access,  
15                  destruction, acquisition, disclosure, or use of  
16                  sensitive personally identifying information.

17           (3) RISK ASSESSMENT.—A covered entity  
18           shall—

19                   (A) identify reasonably foreseeable internal  
20                  and external vulnerabilities and internal and ex-  
21                  ternal threats that could result in unauthorized  
22                  access, destruction, acquisition, disclosure, or  
23                  use of sensitive personally identifiable informa-  
24                  tion or of systems containing sensitive person-  
25                  ally identifiable information;

1           (B) assess the likelihood of and potential  
2 damage from unauthorized access, destruction,  
3 acquisition, disclosure, or use of sensitive per-  
4 sonally identifiable information;

5           (C) assess the sufficiency of its technical,  
6 physical, and administrative controls in place to  
7 control and minimize risks from unauthorized  
8 access, destruction, acquisition, disclosure, or  
9 use of sensitive personally identifiable informa-  
10 tion; and

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

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

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

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

1 (i) controls access to sensitive person-  
2 ally identifiable information, including con-  
3 trols to authenticate and permit access  
4 only to authorized individuals;

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

12 (iii) protect sensitive personally identi-  
13 fiable information during use, trans-  
14 mission, storage, and disposal by  
15 encryption, redaction, disclosure limitation  
16 methodologies, or access controls, that are  
17 widely accepted as an effective industry  
18 practice or industry standard, or other rea-  
19 sonable means;

20 (iv) ensure that sensitive personally  
21 identifiable information is properly de-  
22 stroyed and disposed of, including during  
23 the destruction of computers and other  
24 electronic media that contain sensitive per-  
25 sonally identifiable information; and

1 (v) ensure that no third party is au-  
2 thorized to access or acquire sensitive per-  
3 sonally identifiable information in its pos-  
4 session without the covered entity first per-  
5 forming sufficient due diligence to ascer-  
6 tain, with reasonable certainty, that such  
7 information is being sought for a valid  
8 legal purpose; and

9 (C) establish a plan and procedures for  
10 minimizing the amount of sensitive personally  
11 identifiable information maintained by the cov-  
12 ered entity and the length of time such infor-  
13 mation is retained, which shall provide for the  
14 retention of sensitive personally identifiable in-  
15 formation only as reasonably needed for the  
16 business purposes of such business entity or as  
17 necessary to comply with any legal obligation  
18 and only as long as so needed.

19 (5) LIMITATION.—Nothing in this subsection  
20 shall be construed to permit, and nothing does per-  
21 mit, the Federal Trade Commission to issue regula-  
22 tions requiring, or according greater legal status to,  
23 the implementation of or application of a specific  
24 technology or technological specifications for meeting  
25 the requirements of this title.

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

5 (c) VULNERABILITY TESTING.—

6 (1) IN GENERAL.—Covered entities subject to  
7 this subtitle shall take steps to ensure regular test-  
8 ing of key technical, physical, and administrative  
9 controls for information and information systems of  
10 the consumer privacy and data security program to  
11 detect, prevent, and respond to attacks or intrusions,  
12 or other system failures.

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

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

8           (2) require the person or entity by contract to  
9           implement and maintain appropriate measures de-  
10          signed to meet the objectives and requirements gov-  
11          erning subtitle A.

12          (e) PERIODIC ASSESSMENT AND CONSUMER PRIVACY  
13          AND DATA SECURITY MODERNIZATION.—Each covered  
14          entity subject to this subtitle shall on a regular basis mon-  
15          itor, evaluate, and adjust, as appropriate its consumer pri-  
16          vacy and data security program in light of any relevant  
17          changes in—

18               (1) technology;

19               (2) internal or external threats and  
20          vulnerabilities to sensitive personally identifiable in-  
21          formation; and

22               (3) the changing business arrangements of the  
23          covered entity, such as—

24                       (A) mergers and acquisitions;

25                       (B) alliances and joint ventures;

1 (C) outsourcing arrangements;

2 (D) bankruptcy; and

3 (E) changes to sensitive personally identifi-  
4 able information systems.

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

11 (g) CONSUMER OPT-OUT.—

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

16 (2) CREDIT FREEZE.—Upon the request of a  
17 consumer, a covered entity that is a consumer re-  
18 porting agency that compiles or maintains a file on  
19 the consumer and has received appropriate proof of  
20 the identity of the requester shall place or lift a  
21 credit freeze in the file of the consumer without  
22 charge to the consumer.

23 (h) RULEMAKING.—Not later than 1 year after the  
24 date of enactment of this Act, the Federal Trade Commis-  
25 sion shall issue regulations in accordance with section 553



1 of title 5, United States Code, to implement subsections  
2 (a) through (g).

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

9 **SEC. 203. FEDERAL ENFORCEMENT.**

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

13 (b) CIVIL ACTIONS BY THE ATTORNEY GENERAL OF  
14 THE UNITED STATES.—

15 (1) IN GENERAL.—The Attorney General may  
16 bring a civil action in the appropriate United States  
17 district court against any covered entity that en-  
18 gages in conduct constituting a violation of this sub-  
19 title and, upon proof of such conduct by a prepon-  
20 derance of the evidence, such covered entity shall be  
21 subject to a civil penalty in an amount that is not  
22 greater than the product of the number of individ-  
23 uals whose sensitive personally identifiable informa-  
24 tion was placed at risk as a result of the violation  
25 and \$16,500.

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

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

16           (c) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-  
17 ERAL.—

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

23                   (A) enjoining such act or practice; or

24                   (B) enforcing compliance with this subtitle.

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

5           (d) CIVIL ACTIONS BY THE FEDERAL TRADE COM-  
6           MISSION.—

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

17          (2) CIVIL PENALTIES.—

18                (A) IN GENERAL.—Any covered entity that  
19                violates the provisions of this subtitle shall be  
20                subject to a civil penalty in the amount that is  
21                not greater than the product of the number of  
22                individuals whose sensitive personally identifi-  
23                able information was placed at risk as a result  
24                of the violation and \$16,500.

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

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

18          (3) UNFAIR OR DECEPTIVE ACTS OR PRAC-  
19          TICES.—For the purpose of the exercise by the Fed-  
20          eral Trade Commission of its functions and powers  
21          under the Federal Trade Commission Act, a viola-  
22          tion of any requirement or prohibition imposed  
23          under this title shall constitute an unfair or decep-  
24          tive act or practice in commerce in violation of a  
25          regulation under section 18(a)(1)(B) of the Federal

1 Trade Commission Act (15 U.S.C. 57a(a)(I)(B)) re-  
2 garding unfair or deceptive acts or practices and  
3 shall be subject to enforcement by the Federal Trade  
4 Commission under that Act with respect to any busi-  
5 ness entity, irrespective of whether that business en-  
6 tity is engaged in commerce or meets any other ju-  
7 risdictional tests in the Federal Trade Commission  
8 Act.

9 (e) COORDINATION OF ENFORCEMENT.—

10 (1) IN GENERAL.—When opening an investiga-  
11 tion, the Federal Trade Commission shall consult  
12 with the Attorney General.

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

18 (3) COORDINATION AGREEMENT.—

19 (A) IN GENERAL.—In order to avoid con-  
20 flicts and promote consistency regarding the en-  
21 forcement and litigation of matters under this  
22 Act, not later than 180 days after the date of  
23 enactment of this Act, the Attorney General  
24 and the Federal Trade Commission shall enter

1           into an agreement for coordination regarding  
2           the enforcement of this Act.

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

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

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

16          (a) STATE ENFORCEMENT.—

17                  (1) CIVIL ACTIONS.—In any case in which the  
18                  attorney general of a State or any State or local law  
19                  enforcement agency authorized by the State attorney  
20                  general or by State statute to prosecute violations of  
21                  consumer protection law, has reason to believe that  
22                  a covered entity has violated section 201 or 202, the  
23                  State, as *parens patriae*, may bring a civil action on  
24                  behalf of the residents of that State to—

25                          (A) enjoin that act or practice;

1 (B) enforce compliance with section 201 or  
2 202; or

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

8 (2) PENALTY DETERMINATION.—

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

19 (B) ADDITIONAL PENALTY LIMIT.—If a  
20 court determines under subparagraph (A) that  
21 a violation of a provision of this subtitle was  
22 willful or intentional and imposes an additional  
23 penalty, the court may not impose an additional  
24 penalty in an amount that exceeds  
25 \$10,000,000.

1 (3) NOTICE.—

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

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

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

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

17 (C) NOTIFICATION WHEN PRACTICABLE.—

18 In an action described under subparagraph (B),  
19 the attorney general of a State shall provide the  
20 written notice and the copy of the complaint to  
21 the Attorney General of the United States and  
22 the Federal Trade Commission as soon after  
23 the filing of the complaint as practicable.

24 (4) FEDERAL PROCEEDINGS.—Upon receiving  
25 notice under paragraph (2), the Attorney General of



1 the United States and the Federal Trade Commis-  
2 sion shall have the right to—

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

6 (B) initiate an action in the appropriate  
7 United States district court under section 203  
8 and move to consolidate all pending actions, in-  
9 cluding State actions, in such court;

10 (C) intervene in an action brought under  
11 paragraph (1); and

12 (D) file petitions for appeal.

13 (5) PENDING PROCEEDINGS.—If the Attorney  
14 General of the United States or the Federal Trade  
15 Commission initiates a Federal civil action for a vio-  
16 lation of this subtitle, or any regulations thereunder,  
17 no attorney general of a State may bring an action  
18 for a violation of this subtitle that resulted from the  
19 same or related acts or omissions against a defend-  
20 ant named in the Federal civil action initiated by the  
21 Attorney General of the United States or the Fed-  
22 eral Trade Commission.

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

1 attorney general of a State from exercising the pow-  
2 ers conferred on the attorney general by the laws of  
3 that State to—

4 (A) conduct investigations;

5 (B) administer oaths and affirmations; or

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

9 (7) VENUE; SERVICE OF PROCESS.—

10 (A) VENUE.—Any action brought under  
11 subsection (a) may be brought in—

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

16 (ii) another court of competent juris-  
17 diction.

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

21 (i) is an inhabitant; or

22 (ii) may be found.

23 (b) NO PRIVATE CAUSE OF ACTION.—Nothing in  
24 this subtitle establishes a private cause of action against

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

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

4 (a) PREEMPTION.—For any covered entity that is  
5 subject to this subtitle, the provisions of this subtitle shall  
6 supersede any other provision of Federal law, or any provi-  
7 sions of the law of any State or political subdivision of  
8 a State, requiring data security practices that are less  
9 stringent than the requirements of this subtitle.

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

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

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

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

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

24 (e) PRESERVATION OF FCC AUTHORITY.—Nothing  
25 in this Act may be construed in any way to limit the au-

1 thority of the Federal Communications Commission under  
2 any other provision of law.

3           **Subtitle B—Security Breach**  
4           **Notification and Protection**

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

6           (a) IN GENERAL.—Except as provided in section 212,  
7 a covered entity shall, following the discovery of a security  
8 breach of sensitive personally identifiable information held  
9 by that covered entity or any third-party entity contracted  
10 to maintain or process data in electronic form containing  
11 sensitive personally identifiable information for that cov-  
12 ered entity—

13                 (1) notify any resident of the United States  
14 whose sensitive personally identifiable information  
15 has been, or is reasonably believed to have been,  
16 accessed or acquired; and

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

22                         (A) automatically enrolled, without the  
23 consent of the individual, into a fee-based iden-  
24 tity theft prevention and mitigation service at  
25 the end of the 5-year period; or

1 (B) required to seek arbitration of any  
2 claim arising from the identity theft prevention  
3 and mitigation service described in subpara-  
4 graph (A).

5 (b) OBLIGATION OF THIRD-PARTY ENTITIES.—

6 (1) IN GENERAL.—In the event of a breach of  
7 security of a system maintained by a third-party en-  
8 tity that has been contracted to maintain or process  
9 data in electronic form containing sensitive person-  
10 ally identifiable information on behalf of a covered  
11 entity who owns or possesses such data, the third-  
12 party entity shall notify the covered entity of the  
13 breach of security. Upon receiving notification from  
14 the third-party entity, such covered entity shall pro-  
15 vide the notification and identify theft prevention  
16 and mitigation service required under subsection (a).

17 (2) NOTICE BY THIRD-PARTY ENTITIES.—Noth-  
18 ing in this subtitle shall prevent or abrogate an  
19 agreement between a covered entity required to give  
20 notice under this section and a third-party entity  
21 that has been contracted to maintain or process data  
22 in electronic form containing sensitive personally  
23 identifiable information for a covered entity, to pro-  
24 vide the notifications required under subsection

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

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

19 (c) TIMELINESS OF NOTIFICATION.—

20 (1) IN GENERAL.—All notifications and identity  
21 theft prevention and mitigation services required  
22 under this section shall be made as expediently as  
23 possible and without unreasonable delay following  
24 the discovery by the covered entity of a security  
25 breach.

1           (2) REASONABLE DELAY.—Reasonable delay  
2 under this subsection may include any reasonable  
3 time necessary to determine the scope of the security  
4 breach, prevent further disclosures, and provide no-  
5 tice to law enforcement when required. Except as  
6 provided in subsection (d), delay of notification or  
7 provision of identity theft prevention and mitigation  
8 service shall not exceed 7 days following the dis-  
9 covery of a security breach.

10           (3) BURDEN OF PRODUCTION.—The covered  
11 entity required to provide notice and identity theft  
12 prevention and mitigation service under this subtitle  
13 shall, upon the request of the Attorney General of  
14 the United States or the Federal Trade Commission  
15 provide records or other evidence of the notifications  
16 and identity theft prevention and mitigation service  
17 required under this subtitle, including to the extent  
18 applicable, the reasons for any delay of notification  
19 or provision of identity theft prevention and mitiga-  
20 tion service.

21           (d) DELAY AUTHORIZED FOR LAW ENFORCEMENT  
22 OR NATIONAL SECURITY PURPOSES.—

23           (1) IN GENERAL.—If a Federal law enforce-  
24 ment agency or intelligence agency determines that  
25 the notification or provision of identity theft preven-

1       tion and mitigation service required under this sec-  
2       tion would impede a criminal investigation, or na-  
3       tional security activity, such notification or provision  
4       of identity theft prevention and mitigation service,  
5       as the case may be, shall be delayed upon written  
6       notice from a Federal law enforcement agency or in-  
7       telligence agency to the covered entity that experi-  
8       enced the security breach. The notification from a  
9       Federal law enforcement agency or intelligence agen-  
10      cy shall specify in writing the period of delay re-  
11      quested for law enforcement or national security  
12      purposes.

13           (2) EXTENDED DELAY.—If the notification or  
14      provision of identity theft prevention and mitigation  
15      service required under subsection (a) is delayed pur-  
16      suant to paragraph (1), a covered entity shall give  
17      notice or identity theft prevention and mitigation  
18      service, as the case may be, 15 days after the day  
19      such law enforcement or national security delay was  
20      invoked unless a Federal law enforcement or intel-  
21      ligence agency provides written notification that fur-  
22      ther delay is necessary.

23           (3) LAW ENFORCEMENT IMMUNITY.—No non-  
24      constitutional cause of action shall lie in any court  
25      against any agency for acts relating to the delay of



1 notification for law enforcement or national security  
2 purposes under this subtitle.

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

6 (1) FINANCIAL INSTITUTIONS.—Financial insti-  
7 tutions—

8 (A) subject to and in compliance with the  
9 data security requirements and standards under  
10 section 501(b) of the Gramm-Leach-Bliley Act  
11 (15 U.S.C. 6801(b)); and

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

15 (2) HIPAA AND HITECH REGULATED ENTI-  
16 TIES.—An entity that is subject to and in compli-  
17 ance with the data breach notification of the fol-  
18 lowing, with respect to data that is subject to such  
19 requirements:

20 (A) Section 13401 of the Health Informa-  
21 tion Technology for Economic and Clinical  
22 Health Act (42 U.S.C. 17931).

23 (B) Part 160 or 164 of title 45, Code of  
24 Federal Regulations (or any successor regula-  
25 tions).

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

5 (D) In the case of a business entity, the  
6 applicable data breach notification requirements  
7 of part 1 of subtitle D of title XIII of division  
8 A of the American Reinvestment and Recovery  
9 Act of 2009 (42 U.S.C. 17931 et seq.), if such  
10 business entity is acting as a covered entity, a  
11 business associate, or a vendor of personal  
12 health records, as those terms are defined in  
13 section 13400 of the Health Information Tech-  
14 nology for Economic and Clinical Health Act  
15 (42 U.S.C. 17921).

16 (E) In the case of a third-party service  
17 provider, section 13407 of the Health Informa-  
18 tion Technology for Economic and Clinical  
19 Health Act (42 U.S.C. 17937).

20 **SEC. 212. EXEMPTIONS.**

21 (a) NATIONAL SECURITY AND LAW ENFORCEMENT  
22 EXEMPTION.—

23 (1) IN GENERAL.—Section 211 shall not apply  
24 to a covered entity if a Federal law enforcement  
25 agency or intelligence agency—

1 (A) determines that notification of the se-  
2 curity breach—

3 (i) could be expected to reveal sen-  
4 sitive sources and methods or similarly im-  
5 pede the ability of the Government to con-  
6 duct law enforcement investigations; or

7 (ii) could be expected to cause damage  
8 to the national security;

9 (B) communicates the determination made  
10 under subparagraph (A) to the covered entity;  
11 and

12 (C) orders that notification required under  
13 section 211 not be made.

14 (2) IMMUNITY.—No nonconstitutional cause of  
15 action shall lie in any court against any Federal  
16 agency for acts relating to the exemption from noti-  
17 fication for law enforcement or national security  
18 purposes under this title.

19 (b) SAFE HARBOR EXEMPTION.—A covered entity  
20 shall be exempt from the notice and identity theft preven-  
21 tion and mitigation service requirements under section  
22 211 if the covered entity reasonably determines that sen-  
23 sitive personally identifiable information is rendered unus-  
24 able, unreadable, or indecipherable through data security  
25 technology or methodology, including encryption or redac-

1 tion, that is generally accepted by experts in the field of  
2 information security, such that there is no reasonable like-  
3 lihood that a security breach has resulted in, or will result  
4 in, the misuse of data.

5 **SEC. 213. METHODS OF NOTICE.**

6 A covered entity shall be in compliance with section  
7 211 if the covered entity provides the following:

8 (1) **INDIVIDUAL NOTICE.**—Notice to individuals  
9 by one of the following means if the method of noti-  
10 fication selected can most likely be expected to reach  
11 the intended individual:

12 (A) Written notification to the last known  
13 home mailing address of the individual in the  
14 records of the covered entity.

15 (B) Telephone notice to the individual per-  
16 sonally, provided that the telephone notice is  
17 made directly to each affected consumer, and is  
18 not made through a prerecorded message.

19 (C) E-mail notice, if—

20 (i)(I) the covered entity's primary  
21 method of communication with the indi-  
22 vidual is by e-mail; or

23 (II) the individual has consented to  
24 receive such notice and the notice is con-  
25 sistent with the provisions permitting elec-

1           tronic transmission of notices under sec-  
2           tion 101 of the Electronic Signatures in  
3           Global and National Commerce Act (15  
4           U.S.C. 7001); and

5           (ii) the e-mail notice does not request,  
6           or contain a hypertext link to a request,  
7           that the consumer provide personal infor-  
8           mation in response to the notice.

9           (2) MEDIA, WEBSITE, AND SOCIAL MEDIA NO-  
10          TICE.—In the event notice is required to more than  
11          5,000 individuals in 1 State and individual notice is  
12          not feasible due to lack of sufficient contact informa-  
13          tion for the individuals required to be notified, a cov-  
14          ered entity shall—

15               (A) provide notice to the major media out-  
16               lets serving the State or jurisdiction of the indi-  
17               viduals believed to be affected;

18               (B) place notice in a clear and conspicuous  
19               place on the website of the covered entity if the  
20               covered entity operates a website; and

21               (C) place notice on each social media plat-  
22               form on which the covered entity maintains a  
23               social media presence, if any.

1 **SEC. 214. CONTENT OF NOTIFICATION.**

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

5 (1) a general description of the incident and the  
6 date or estimated date of the security breach and  
7 the date range during which the sensitive personally  
8 identifiable information was compromised;

9 (2) a description of the categories of sensitive  
10 personally identifiable information that was, or is  
11 reasonably believed to have been, accessed or ac-  
12 quired by an unauthorized person;

13 (3) the acts the covered entity, or the agent of  
14 the covered entity, has taken to protect sensitive  
15 personally identifiable information from further se-  
16 curity breach;

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

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

23 (6) a toll-free number—

24 (A) that the individual may use to contact  
25 the covered entity, or the agent of the covered  
26 entity; and

1 (B) from which the individual may learn  
2 what types of sensitive personally identifiable  
3 information the covered entity maintained about  
4 that individual; and

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

10 (b) **DIRECT BUSINESS RELATIONSHIP.**—Regardless  
11 of whether a covered entity or a designated third party  
12 provides the notice required pursuant to section 211(b),  
13 such notice shall include the name of the covered entity  
14 that has the most direct relationship with the individual  
15 being notified.

16 **SEC. 215. COORDINATION OF NOTIFICATION WITH CREDIT**  
17 **REPORTING AGENCIES.**

18 If a covered entity is required to provide notification  
19 to more than 5,000 individuals under section 211(a) and  
20 the sensitive personally identifiable information that was  
21 breached could be used to commit financial fraud or iden-  
22 tity theft, the covered entity shall also notify all consumer  
23 reporting agencies that compile and maintain files on con-  
24 sumers on a nationwide basis (as defined in section 603(p)  
25 of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)))

1 of the timing and distribution of the notices. Such notice  
2 shall be given to the consumer credit reporting agencies  
3 without unreasonable delay and, if it will not delay notice  
4 to the affected individuals, prior to the distribution of no-  
5 tices to the affected individuals.

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

7 (a) IN GENERAL.—A covered entity required to pro-  
8 vide notification under section 211(a) shall provide a copy  
9 of the notification to the Federal Trade Commission not  
10 later than the date on which notice is provided to individ-  
11 uals required to be notified. The Federal Trade Commis-  
12 sion shall establish procedures to ensure the attorneys  
13 general of each State with affected residents receives a  
14 copy of the notice provided to it under this section.

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

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

20 (2) on an annual basis, submit a report to Con-  
21 gress on the notifications received under subsection

22 (a).

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

24 (a) DESIGNATION OF GOVERNMENT ENTITY TO RE-  
25 CEIVE NOTICE.—



1           (1) IN GENERAL.—Not later than 60 days after  
2           the date of enactment of this Act, the Secretary of  
3           Homeland Security, in consultation with the Attor-  
4           ney General, shall designate a Federal Government  
5           entity to receive the notices required under section  
6           211 and this section.

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

9                   (A) promptly provide the information that  
10                  it receives to the United States Secret Service  
11                  or the Federal Bureau of Investigation for law  
12                  enforcement purposes; and

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

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

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

24                   (2) the security breach involves a database,  
25                  networked or integrated databases, or other data

1 system containing the sensitive personally identifi-  
2 able information of more than 500,000 individuals  
3 nationwide;

4 (3) the security breach involves databases  
5 owned by the Federal Government; or

6 (4) the security breach involves primarily sen-  
7 sitive personally identifiable information of individ-  
8 uals known to the covered entity to be employees  
9 and contractors of the Federal Government involved  
10 in national security or law enforcement.

11 (c) DEPARTMENT OF JUSTICE REVIEW OF THRESH-  
12 OLDS FOR NOTICE.—The Attorney General, in consulta-  
13 tion with the Secretary of Homeland Security, after notice  
14 and the opportunity for public comment, and in a manner  
15 consistent with this section, shall promulgate regulations,  
16 as necessary, under section 553 of title 5, United States  
17 Code, to adjust the thresholds for notice to law enforce-  
18 ment and national security authorities under subsection  
19 (a) and to facilitate the purposes of this section.

20 (d) TIMING.—The notice required under subsection  
21 (b) shall be provided as promptly as possible, but such  
22 notice must be provided not less than 48 hours before no-  
23 tice is provided to an individual pursuant to section 211,  
24 or not later than 7 days after the discovery of the events  
25 requiring notice, whichever occurs first. For each breach

1 requiring notice under this subsection, a copy of the notice  
2 to individuals required under section 211 shall also be pro-  
3 vided to the designated entity not later than the date on  
4 which the notice is provided to affected individuals.

5 **SEC. 218. FEDERAL ENFORCEMENT.**

6 (a) IN GENERAL.—The Attorney General and the  
7 Federal Trade Commission may enforce civil violations of  
8 this subtitle.

9 (b) CIVIL ACTIONS BY THE ATTORNEY GENERAL OF  
10 THE UNITED STATES.—

11 (1) IN GENERAL.—The Attorney General may  
12 bring a civil action in the appropriate United States  
13 district court against any covered entity that en-  
14 gages in conduct constituting a violation of this sub-  
15 title and, upon proof of such conduct by a prepon-  
16 derance of the evidence, the covered entity shall be  
17 subject to a civil penalty in an amount not greater  
18 than the product of the number of violations of this  
19 subtitle and \$16,500. Each failure to provide notifi-  
20 cation to an individual as required under this sub-  
21 title shall be treated as a separate violation.

22 (2) DETERMINATIONS.—The determination of  
23 whether a violation of a provision of this subtitle has  
24 occurred, and if so, the amount of the penalty to be  
25 imposed, if any, shall be made by the court sitting

1 as the finder of fact. The determination of whether  
2 a violation of a provision of this subtitle was willful  
3 or intentional, and if so, the amount of the addi-  
4 tional penalty to be imposed, if any, shall be made  
5 by the court sitting as the finder of fact.

6 (3) ADDITIONAL PENALTY LIMIT.—If a court  
7 determines under paragraph (2) that a violation of  
8 a provision of this subtitle was willful or intentional  
9 and imposes an additional penalty, the court may  
10 not impose an additional penalty in an amount that  
11 exceeds \$10,000,000.

12 (c) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-  
13 ERAL.—

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

19 (A) enjoining such act or practice; or

20 (B) enforcing compliance with this subtitle.

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

1 (d) CIVIL ACTIONS BY THE FEDERAL TRADE COM-  
2 MISSION.—

3 (1) IN GENERAL.—Compliance with the require-  
4 ments imposed under this subtitle may be enforced  
5 under the Federal Trade Commission Act (15  
6 U.S.C. 41 et seq.) by the Federal Trade Commission  
7 with respect to business entities subject to this Act.  
8 All of the functions and powers of the Federal Trade  
9 Commission under the Federal Trade Commission  
10 Act are available to the Commission to enforce com-  
11 pliance by any person with the requirements imposed  
12 under this title.

13 (2) CIVIL PENALTIES.—

14 (A) IN GENERAL.—Any covered entity that  
15 violates this subtitle shall be subject to a civil  
16 penalty in the amount that is not greater than  
17 the product of the number of violations of this  
18 subtitle and \$16,500. Each failure to provide  
19 notification to an individual as required under  
20 this subtitle shall be treated as a separate viola-  
21 tion.

22 (B) DETERMINATIONS.—The determina-  
23 tion of whether a violation of a provision of this  
24 subtitle has occurred, and if so, the amount of  
25 the penalty to be imposed, if any, shall be made

1 by the court sitting as the finder of fact. The  
2 determination of whether a violation of a provi-  
3 sion of this subtitle was willful or intentional,  
4 and if so, the amount of the additional penalty  
5 to be imposed, if any, shall be made by the  
6 court sitting as the finder of fact.

7 (C) ADDITIONAL PENALTY LIMIT.—If a  
8 court determines under subparagraph (B) that  
9 a violation of a provision of this subtitle was  
10 willful or intentional and imposes an additional  
11 penalty, the court may not impose an additional  
12 penalty in an amount that exceeds  
13 \$10,000,000.

14 (3) UNFAIR OR DECEPTIVE ACTS OR PRAC-  
15 TICES.—For the purpose of the exercise by the Fed-  
16 eral Trade Commission of its functions and powers  
17 under the Federal Trade Commission Act, a viola-  
18 tion of any requirement or prohibition imposed  
19 under this title shall constitute an unfair or decep-  
20 tive act or practice in commerce in violation of a  
21 regulation under section 18(a)(1)(B) of the Federal  
22 Trade Commission Act (15 U.S.C. 57a(a)(I)(B)) re-  
23 garding unfair or deceptive acts or practices and  
24 shall be subject to enforcement by the Federal Trade  
25 Commission under that Act with respect to any busi-

1       ness entity, irrespective of whether that business en-  
2       tity is engaged in commerce or meets any other ju-  
3       risdictional tests in the Federal Trade Commission  
4       Act.

5       (e) COORDINATION OF ENFORCEMENT.—

6           (1) IN GENERAL.—When opening an investiga-  
7       tion, the Federal Trade Commission shall consult  
8       with the Attorney General.

9           (2) LIMITATION.—The Federal Trade Commis-  
10      sion may initiate investigations under this subsection  
11      unless the Attorney General determines that such an  
12      investigation would impede an ongoing criminal in-  
13      vestigation or national security activity.

14      (3) COORDINATION AGREEMENT.—

15           (A) IN GENERAL.—In order to avoid con-  
16      flicts and promote consistency regarding the en-  
17      forcement and litigation of matters under this  
18      Act, not later than 180 days after the enact-  
19      ment of this Act, the Attorney General and the  
20      Federal Trade Commission shall enter into an  
21      agreement for coordination regarding the en-  
22      forcement of this Act.

23           (B) REQUIREMENT.—The coordination  
24      agreement entered into under subparagraph (A)  
25      shall include provisions to ensure that parallel

1 investigations and proceedings under this sec-  
2 tion are conducted in a manner that avoids con-  
3 flicts and does not impede the ability of the At-  
4 torney General to prosecute violations of Fed-  
5 eral criminal laws.

6 (f) RULEMAKING.—The Federal Trade Commission  
7 may, in consultation with the Attorney General, issue such  
8 other regulations as it determines to be necessary to carry  
9 out this subtitle. All regulations promulgated under this  
10 Act shall be issued in accordance with section 553 of title  
11 5, United States Code.

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

16 (h) FRAUD ALERT.—Section 605A(b)(1) of the Fair  
17 Credit Reporting Act (15 U.S.C. 1681e–1(b)(1)) is  
18 amended by inserting “, or evidence that the consumer  
19 has received notice that the consumer’s financial informa-  
20 tion has or may have been compromised,” after “identity  
21 theft report”.

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

23 (a) IN GENERAL.—

24 (1) CIVIL ACTIONS.—



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

10 (i) enjoin that practice;

11 (ii) enforce compliance with this sub-  
12 title; or

13 (iii) impose a civil penalty in an  
14 amount not greater than the product of  
15 the number of violations of this subtitle  
16 and \$16,500.

17 (B) FAILURE TO PROVIDE NOTIFICA-  
18 TION.—For purposes of subparagraph (A)(iii),  
19 each failure to provide notification to an indi-  
20 vidual as required under this subtitle shall be  
21 treated as a separate violation.

22 (2) PENALTY DETERMINATIONS.—

23 (A) DETERMINATIONS.—The determina-  
24 tion of whether a violation of a provision of this  
25 subtitle has occurred, and if so, the amount of

1 the penalty to be imposed, if any, shall be made  
2 by the court sitting as the finder of fact. The  
3 determination of whether a violation of a provi-  
4 sion of this subtitle was willful or intentional,  
5 and if so, the amount of the additional penalty  
6 to be imposed, if any, shall be made by the  
7 court sitting as the finder of fact.

8 (B) ADDITIONAL PENALTY LIMIT.—If a  
9 court determines under subparagraph (A) that  
10 a violation of a provision of this subtitle was  
11 willful or intentional and imposes an additional  
12 penalty, the court may not impose an additional  
13 penalty in an amount that exceeds  
14 \$10,000,000.

15 (3) NOTICE.—

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

21 (i) written notice of the action; and

22 (ii) a copy of the complaint for the ac-  
23 tion.

24 (B) EXEMPTION.—

1 (i) IN GENERAL.—Subparagraph (A)  
2 shall not apply with respect to the filing of  
3 an action by an attorney general of a State  
4 under this subtitle, if the State attorney  
5 general determines that it is not feasible to  
6 provide the notice described in such sub-  
7 paragraph before the filing of the action.

8 (ii) NOTIFICATION.—In an action de-  
9 scribed in clause (i), the attorney general  
10 of a State shall provide notice and a copy  
11 of the complaint to the Attorney General  
12 of the United States and the Federal  
13 Trade Commission at the time the State  
14 attorney general files the action.

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

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

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

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

3           (4) file petitions for appeal.

4           (c) PENDING PROCEEDINGS.—If the Attorney Gen-  
5           eral or the Federal Trade Commission initiates a criminal  
6           proceeding or civil action for a violation of a provision of  
7           this subtitle, or any regulations thereunder, no attorney  
8           general of a State may bring an action for a violation of  
9           a provision of this subtitle against a defendant named in  
10          the Federal criminal proceeding or civil action.

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

17                  (1) conduct investigations;

18                  (2) administer oaths or affirmations; or

19                  (3) compel the attendance of witnesses or the  
20          production of documentary and other evidence.

21          (e) VENUE; SERVICE OF PROCESS.—

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

24                          (A) the district court of the United States  
25          that meets applicable requirements relating to

1 venue under section 1391 of title 28, United  
2 States Code; or

3 (B) another court of competent jurisdic-  
4 tion.

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

8 (A) is an inhabitant; or

9 (B) may be found.

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

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

15 (a) PREEMPTION.—For a covered entity that is sub-  
16 ject to this subtitle, the provisions of this subtitle shall  
17 supersede any other provision of Federal law, or any provi-  
18 sions of the law of any State or political subdivision of  
19 a State requiring notification of a security breach of sen-  
20 sitive personally identifiable information, which is less  
21 stringent than the requirements of this subtitle.

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

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

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

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

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

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

15 **SEC. 221. REPORTING ON EXEMPTIONS.**

16          Not later than 18 months after the date of enactment  
17 of this Act, and upon the request by Congress thereafter,  
18 the Attorney General, in consultation with the Secretary  
19 of Homeland Security, shall submit a report to Congress  
20 on the number and nature of security breaches subject to  
21 the national security and law enforcement exemptions  
22 under section 212(a).

1 **SEC. 222. 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—COMPLIANCE WITH**  
6 **STATUTORY PAY-AS-YOU-GO ACT**

7 **SEC. 301. BUDGET COMPLIANCE.**

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

○