

114TH CONGRESS
1ST SESSION

S. 1158

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

APRIL 30, 2015

Mr. LEAHY (for himself, Mr. FRANKEN, Ms. WARREN, Mr. BLUMENTHAL, Mr. WYDEN, and Mr. MARKEY) 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 2015”.

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

- Sec. 211. Notice to individuals.
- 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, identity thieves, rogue employees, and other
6 criminals, including organized and sophisticated
7 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) **COVERED ENTITY.**—The term “covered en-
23 tity” means any business entity, other than a service
24 provider, that collects, uses, accesses, transmits,

1 stores, or disposes of sensitive personally identifiable
2 information.

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

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

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

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

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

22 (9) SECURITY BREACH.—

23 (A) IN GENERAL.—The term “security
24 breach” means compromise of the privacy or se-
25 curity of computerized data that results in, or

1 that there is a reasonable basis to conclude has
2 resulted in, unauthorized access to or acquisi-
3 tion of sensitive personally identifiable informa-
4 tion.

5 (B) EXCLUSION.—The term “security
6 breach” does not include—

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

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

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

22 (10) SENSITIVE PERSONALLY IDENTIFIABLE IN-
23 FORMATION.—The term “sensitive personally identi-
24 fiable information” means any information or com-

1 pilation of information, in electronic or digital form
2 that includes the following:

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

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

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

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

24 (E) An individual's first and last name or
25 first initial and last name in combination with

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

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

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

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

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

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

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

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

1 **“§ 1041. Concealment of security breaches involving**
 2 **sensitive personally identifiable informa-**
 3 **tion**

4 “(a) IN GENERAL.—Whoever, having knowledge of a
 5 security breach and of the fact that notice of such security
 6 breach is required under title II of the Consumer Privacy
 7 Protection Act of 2015, intentionally and willfully conceals
 8 the fact of such security breach, shall, in the event that
 9 such security breach results in economic harm to any indi-
 10 vidual in the amount of \$1,000 or more, be fined under
 11 this title or imprisoned for not more than 5 years, or both.

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

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

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

19 (c) ENFORCEMENT AUTHORITY.—

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

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

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

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

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

15 “(1) the defendant—

16 “(A) exceeded authorized access to a non-
17 governmental computer; or

18 “(B) accessed a non-governmental com-
19 puter without authorization; and

20 “(2) the sole basis for the Government deter-
21 mining that access to the non-governmental com-
22 puter was unauthorized, or in excess of authoriza-
23 tion, was that the defendant violated a contractual
24 obligation or agreement with a service provider or

1 employer, such as an acceptable use policy or terms
2 of service agreement.”.

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

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

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

8 (2) in subsection (a)—

9 (A) in paragraph (1)—

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

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

14 (iii) by inserting after subparagraph
15 (C) the following:

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

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

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

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

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

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

15 “(2) may, upon application of the Attorney
16 General—

17 “(A) specify that no cause of action shall
18 lie in any court against a person for complying
19 with the restraining order, prohibition, or other
20 action; and

21 “(B) provide that the United States shall
22 pay to such person a fee for reimbursement for
23 such costs as are reasonably necessary and
24 which have been directly incurred in complying

1 with the restraining order, prohibition, or other
2 action.

3 “(d) There are authorized to be appropriated to the
4 Department of Justice, the Department of Homeland Se-
5 curity, and the Department of the Treasury such sums
6 as are necessary to implement this section, including pay-
7 ments made by the United States of a fee for reimburse-
8 ment.”.

9 (b) TECHNICAL AND CONFORMING AMENDMENT.—
10 The table of section for chapter 63 is amended by striking
11 the item relating to section 1345 and inserting the fol-
12 lowing:

“1345. Injunctions against fraud and abuse.”.

13 **SEC. 104. DETERRING THE DEVELOPMENT AND SALE OF**
14 **COMPUTER AND CELL PHONE SPYING DE-**
15 **VICES.**

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

1 **TITLE II—CONSUMER PRIVACY**
2 **AND SECURITY OF SENSITIVE**
3 **PERSONALLY IDENTIFIABLE**
4 **INFORMATION**

5 **Subtitle A—Consumer Privacy and**
6 **Data Security Program**

7 **SEC. 201. PURPOSE AND APPLICABILITY OF CONSUMER**
8 **PRIVACY AND DATA SECURITY PROGRAM.**

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

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

21 (c) **LIMITATIONS.**—Notwithstanding any other obli-
22 gation under this subtitle, this subtitle does not apply to
23 the following:

24 (1) **FINANCIAL INSTITUTIONS.**—Financial insti-
25 tutions—

1 (A) subject to and in compliance with the
2 data security requirements and standards under
3 section 501(b) of the Gramm-Leach-Bliley Act
4 (15 U.S.C. 6801(b)); and

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

8 (2) HIPAA AND HITECH REGULATED ENTI-
9 TIES.—An entity that is subject to and in compli-
10 ance with the data security requirements of the fol-
11 lowing, with respect to data that is subject to such
12 requirements:

13 (A) Section 13401 of the Health Informa-
14 tion Technology for Economic and Clinical
15 Health Act (42 U.S.C. 17931).

16 (B) Part 160 or 164 of title 45, Code of
17 Federal Regulations (or any successor regula-
18 tions).

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

23 (D) In the case of a business associate, as
24 defined in section 13400 of the Health Informa-
25 tion Technology for Economic and Clinical

1 Health Act (42 U.S.C. 17921), the applicable
2 privacy and data security requirements of part
3 1 of subtitle D of title XIII of division A of the
4 American Reinvestment and Recovery Act of
5 2009 (42 U.S.C. 17931 et seq.).

6 (3) SERVICE PROVIDERS.—A service provider
7 for any electronic communication by a third-party,
8 to the extent that the service provider is engaged
9 solely in the transmission, routing, or temporary, in-
10 termediate, or transient storage of that communica-
11 tion.

12 **SEC. 202. REQUIREMENTS FOR CONSUMER PRIVACY AND**
13 **DATA SECURITY PROGRAM.**

14 (a) CONSUMER PRIVACY AND DATA SECURITY PRO-
15 GRAM.—A covered entity subject to this subtitle shall com-
16 ply with the following safeguards and any other adminis-
17 trative, technical, or physical safeguards identified by the
18 Federal Trade Commission in a rulemaking process pursu-
19 ant to section 553 of title 5, United States Code, for the
20 protection of sensitive personally identifiable information:

21 (1) SCOPE.—A covered entity shall implement a
22 comprehensive consumer privacy and data security
23 program that includes administrative, technical, and
24 physical safeguards appropriate to the size and com-

1 plexity, and the nature and scope, of the activities
2 of the covered entity.

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

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

7 (B) protect against any anticipated
8 vulnerabilities to the privacy and security of
9 sensitive personally identifying information; and

10 (C) protect against unauthorized access,
11 acquisition, disclosure, or use of sensitive per-
12 sonally identifying information.

13 (3) RISK ASSESSMENT.—A covered entity
14 shall—

15 (A) identify reasonably foreseeable internal
16 and external vulnerabilities and internal and ex-
17 ternal threats that could result in unauthorized
18 access, disclosure, or use of sensitive personally
19 identifiable information or of systems con-
20 taining sensitive personally identifiable informa-
21 tion;

22 (B) assess the likelihood of and potential
23 damage from unauthorized access, acquisition,
24 disclosure, or use of sensitive personally identi-
25 fiable information;

1 (C) assess the sufficiency of its technical,
2 physical, and administrative controls in place to
3 control and minimize risks from unauthorized
4 access, acquisition, disclosure, or use of sen-
5 sitive personally identifiable information; and

6 (D) assess the vulnerability of sensitive
7 personally identifiable information during de-
8 struction and disposal of such information, in-
9 cluding through the disposal or retirement of
10 hardware.

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

13 (A) design its consumer privacy and data
14 security program to control the risks identified
15 under paragraph (3);

16 (B) adopt measures commensurate with
17 the sensitivity of the data as well as the size,
18 complexity, nature, and scope of the activities
19 of the covered entity that—

20 (i) controls access to sensitive person-
21 ally identifiable information, including con-
22 trols to authenticate and permit access
23 only to authorized individuals;

24 (ii) detect, record, and preserve infor-
25 mation relevant to actual and attempted

1 fraudulent, unlawful, or unauthorized ac-
2 cess, acquisition, disclosure, or use of sen-
3 sitive personally identifiable information,
4 including by employees and other individ-
5 uals otherwise authorized to have access;

6 (iii) protect sensitive personally identi-
7 fiable information during use, trans-
8 mission, storage, and disposal by
9 encryption, redaction, disclosure limitation
10 methodologies, or access controls, that are
11 widely accepted as an effective industry
12 practice or industry standard, or other rea-
13 sonable means;

14 (iv) ensure that sensitive personally
15 identifiable information is properly de-
16 stroyed and disposed of, including during
17 the destruction of computers and other
18 electronic media that contain sensitive per-
19 sonally identifiable information; and

20 (v) ensure that no third party is au-
21 thorized to access or acquire sensitive per-
22 sonally identifiable information in its pos-
23 session without the covered entity first per-
24 forming sufficient due diligence to ascer-
25 tain, with reasonable certainty, that such

1 information is being sought for a valid
2 legal purpose; and

3 (C) establish a plan and procedures for
4 minimizing the amount of sensitive personally
5 identifiable information maintained by the cov-
6 ered entity, which shall provide for the reten-
7 tion of sensitive personally identifiable informa-
8 tion only as reasonably needed for the business
9 purposes of such business entity or as necessary
10 to comply with any legal obligation.

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

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

22 (c) VULNERABILITY TESTING.—

23 (1) IN GENERAL.—Covered entities subject to
24 this subtitle shall take steps to ensure regular test-
25 ing of key technical, physical, and administrative

1 controls for information and information systems of
2 the consumer privacy and data security program to
3 detect, prevent, and respond to attacks or intrusions,
4 or other system failures.

5 (2) FREQUENCY.—The frequency and nature of
6 the tests required under paragraph (1) shall be de-
7 termined by the risk assessment of the covered enti-
8 ty under subsection (a)(3).

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

17 (1) exercise appropriate due diligence in select-
18 ing the person or entity for responsibilities related to
19 sensitive personally identifiable information, and
20 take reasonable steps to select and retain a person
21 or entity that is capable of maintaining appropriate
22 controls for the privacy and security of the sensitive
23 personally identifiable information at issue; and

24 (2) require the person or entity by contract to
25 implement and maintain appropriate measures de-

1 signed to meet the objectives and requirements gov-
2 erning subtitle A.

3 (e) PERIODIC ASSESSMENT AND CONSUMER PRIVACY
4 AND DATA SECURITY MODERNIZATION.—Each covered
5 entity subject to this subtitle shall on a regular basis mon-
6 itor, evaluate, and adjust, as appropriate its consumer pri-
7 vacy and data security program in light of any relevant
8 changes in—

9 (1) technology;

10 (2) internal or external threats and
11 vulnerabilities to sensitive personally identifiable in-
12 formation; and

13 (3) the changing business arrangements of the
14 covered entity, such as—

15 (A) mergers and acquisitions;

16 (B) alliances and joint ventures;

17 (C) outsourcing arrangements;

18 (D) bankruptcy; and

19 (E) changes to sensitive personally identifi-
20 able information systems.

21 (f) IMPLEMENTATION TIMELINE.—Not later than 1
22 year after the date of enactment of this Act, a covered
23 entity subject to the provisions of this subtitle shall imple-
24 ment a consumer privacy and data security program pur-
25 suant to this subtitle.

1 **SEC. 203. FEDERAL ENFORCEMENT.**

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

5 (b) CIVIL ACTIONS BY THE ATTORNEY GENERAL OF
6 THE UNITED STATES.—

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

18 (2) PENALTY LIMITATION.—Notwithstanding
19 any other provision of law, the total amount of the
20 civil penalty assessed against a covered entity for
21 conduct involving the same or related acts or omis-
22 sions that results in a violation of this subtitle may
23 not exceed \$5,000,000, unless such conduct is found
24 to be willful or intentional.

25 (3) DETERMINATIONS.—The determination of
26 whether a violation of a provision of this subtitle has

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

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

14 (c) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-
15 ERAL.—

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

21 (A) enjoining such act or practice; or

22 (B) enforcing compliance with this subtitle.

23 (2) ISSUANCE OF ORDER.—A court may issue
24 an order under paragraph (1), if the court finds that

1 the conduct in question constitutes a violation of this
2 subtitle.

3 (d) CIVIL ACTIONS BY THE FEDERAL TRADE COM-
4 MISSION.—

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

15 (2) CIVIL PENALTIES.—

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

23 (B) PENALTY LIMITATION.—Notwith-
24 standing any other provision of law, the total
25 amount of the civil penalty assessed against a

1 covered entity for conduct involving the same or
2 related acts or omissions that results in a viola-
3 tion of this subtitle may not exceed \$5,000,000,
4 unless such conduct is found to be willful or in-
5 tentional.

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

16 (D) ADDITIONAL PENALTY LIMIT.—If a
17 court determines under subparagraph (C) that
18 a violation of a provision of this subtitle was
19 willful or intentional and imposes an additional
20 penalty, the court may not impose an additional
21 penalty in an amount that exceeds \$5,000,000.

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 date of
2 enactment of this Act, the Attorney General
3 and the Federal Trade Commission shall enter
4 into an agreement for coordination regarding
5 the enforcement 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) OTHER RIGHTS AND REMEDIES.—The rights and
15 remedies available under this section are cumulative and
16 shall not affect any other rights and remedies available
17 under law.

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

19 (a) STATE ENFORCEMENT.—

20 (1) CIVIL ACTIONS.—In any case in which the
21 attorney general of a State or any State or local law
22 enforcement agency authorized by the State attorney
23 general or by State statute to prosecute violations of
24 consumer protection law, has reason to believe that
25 a covered entity has violated section 201 or 202, the

1 State, as *parens patriae*, may bring a civil action on
2 behalf of the residents of that State to—

3 (A) enjoin that act or practice;

4 (B) enforce compliance with section 201 or
5 202; or

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

11 (2) PENALTY LIMITATION.—

12 (A) IN GENERAL.—Notwithstanding any
13 other provision of law, the total sum of civil
14 penalties assessed against a covered entity for
15 all violations of the provisions of this subtitle
16 resulting from the same or related acts or omis-
17 sions may not exceed \$5,000,000, unless such
18 conduct is found to be willful or intentional.

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

1 and if so, the amount of the additional penalty
2 to be imposed, if any, shall be made by the
3 court sitting as the finder of fact.

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

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

10 **SEC. 211. NOTICE TO INDIVIDUALS.**

11 (a) IN GENERAL.—Except as provided in section 212,
12 a covered entity shall, following the discovery of a security
13 breach of such information, notify any resident of the
14 United States whose sensitive personally identifiable infor-
15 mation has been, or is reasonably believed to have been,
16 accessed or acquired.

17 (b) OBLIGATION OF THIRD PARTY ENTITIES.—

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

1 the third party entity, such covered entity shall pro-
2 vide the notification required under subsection (a).

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

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 required under
25 subsection (a).

1 (c) TIMELINESS OF NOTIFICATION.—

2 (1) IN GENERAL.—All notifications required
3 under this section shall be made as expediently as
4 possible and without unreasonable delay following
5 the discovery by the covered entity of a security
6 breach.

7 (2) REASONABLE DELAY.—Reasonable delay
8 under this subsection may include any reasonable
9 time necessary to determine the scope of the security
10 breach, prevent further disclosures, and provide no-
11 tice to law enforcement when required. Except as
12 provided in subsection (d), delay of notification shall
13 not exceed 30 days following the discovery of a secu-
14 rity breach.

15 (3) BURDEN OF PRODUCTION.—The covered
16 entity required to provide notice under this subtitle
17 shall, upon the request of the Attorney General of
18 the United States or the Federal Trade Commission
19 provide records or other evidence of the notifications
20 required under this subtitle, including to the extent
21 applicable, the reasons for any delay of notification.

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

24 (1) IN GENERAL.—If a Federal law enforce-
25 ment agency or intelligence agency determines that

1 the notification required under this section would
2 impede a criminal investigation, or national security
3 activity, such notification shall be delayed upon writ-
4 ten notice from a Federal law enforcement agency or
5 intelligence agency to the covered entity that experi-
6 enced the security breach. The notification from a
7 Federal law enforcement agency or intelligence agen-
8 cy shall specify in writing the period of delay re-
9 quired for law enforcement or national security
10 purposes.

11 (2) EXTENDED DELAY OF NOTIFICATION.—If
12 the notification required under subsection (a) is de-
13 layed pursuant to paragraph (1), a covered entity
14 shall give notice 15 days after the day such law en-
15 forcement or national security delay was invoked un-
16 less a Federal law enforcement or intelligence agency
17 provides written notification that further delay is
18 necessary.

19 (3) LAW ENFORCEMENT IMMUNITY.—No non-
20 constitutional cause of action shall lie in any court
21 against any agency for acts relating to the delay of
22 notification for law enforcement or national security
23 purposes under this subtitle.

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

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

18 **SEC. 212. EXEMPTIONS.**

19 (a) NATIONAL SECURITY AND LAW ENFORCEMENT
20 EXEMPTION.—

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

24 (A) determines that notification of the se-
25 curity breach—

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

5 (ii) could be expected to cause damage
6 to the national security;

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

10 (C) orders that notification required under
11 section 211 not be made.

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

17 (b) SAFE HARBOR EXEMPTION.—A covered entity
18 shall be exempt from the notice requirements under sec-
19 tion 211 if the covered entity reasonably determines that
20 sensitive personally identifiable information is rendered
21 unusable, unreadable, or indecipherable through data se-
22 curity technology or methodology, including encryption or
23 redaction, that is generally accepted by experts in the field
24 of information security, such that there is no reasonable

1 likelihood that a security breach has resulted in, or will
2 result in, the misuse of data.

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

4 A covered entity shall be in compliance with section
5 211 if it provides the following:

6 (1) **INDIVIDUAL NOTICE.**—Notice to individuals
7 by 1 of the following means if the method of notifi-
8 cation selected can most likely be expected to reach
9 the intended individual:

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

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

17 (C) E-mail notice, if—

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

21 (II) the individual has consented to
22 receive such notice and the notice is con-
23 sistent with the provisions permitting elec-
24 tronic transmission of notices under sec-
25 tion 101 of the Electronic Signatures in

1 Global and National Commerce Act (15
2 U.S.C. 7001); and

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

7 (2) MEDIA AND WEBSITE NOTICE.—In the
8 event notice is required to more than 5,000 individ-
9 uals in 1 State and individual notice is not feasible
10 due to lack of sufficient contact information for the
11 individuals required to be notified, a covered entity
12 shall—

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

16 (B) place notice in a clear and conspicuous
17 place on the website of the covered entity if the
18 covered entity operates a website.

19 **SEC. 214. CONTENT OF NOTIFICATION.**

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

23 (1) a general description of the incident and the
24 date or estimated date of the security breach and

1 the date range during which the sensitive personally
2 identifiable information was compromised;

3 (2) a description of the categories of sensitive
4 personally identifiable information that was, or is
5 reasonably believed to have been, accessed or ac-
6 quired by an unauthorized person;

7 (3) the acts the covered entity, or the agent of
8 the covered entity, has taken to protect sensitive
9 personally identifiable information from further se-
10 curity breach;

11 (4) a toll-free number—

12 (A) that the individual may use to contact
13 the covered entity, or the agent of the covered
14 entity; and

15 (B) from which the individual may learn
16 what types of sensitive personally identifiable
17 information the covered entity maintained about
18 that individual; and

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

24 (b) DIRECT BUSINESS RELATIONSHIP.—Regardless
25 of whether a covered entity or a designated third party

1 provides the notice required pursuant to section 211(b),
2 such notice shall include the name of the covered entity
3 that has the most direct relationship with the individual
4 being notified.

5 **SEC. 215. COORDINATION OF NOTIFICATION WITH CREDIT**
6 **REPORTING AGENCIES.**

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

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

21 A covered entity required to provide notification
22 under section 211(a) shall provide a copy of the notifica-
23 tion to the Federal Trade Commission not later than the
24 date on which notice is provided to individuals required
25 to be notified. The Federal Trade Commission shall estab-

1 lish procedures to ensure the attorneys general of each
2 State with affected residents receives a copy of the notice
3 provided to it under this section.

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

5 (a) DESIGNATION OF GOVERNMENT ENTITY TO RE-
6 CEIVE NOTICE.—

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

13 (2) RESPONSIBILITIES OF THE DESIGNATED
14 ENTITY.—The designated entity shall—

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

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

23 (b) NOTICE.—A covered entity shall notify the des-
24 igned entity of the fact that a security breach has oc-
25 curred if—

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

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

10 (3) the security breach involves databases
11 owned by the Federal Government; or

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

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

1 (d) TIMING.—The notice required under subsection
2 (b) shall be provided as promptly as possible, but such
3 notice must be provided not less than 72 hours before no-
4 tice is provided to an individual pursuant to section 211,
5 or not later than 10 days after the discovery of the events
6 requiring notice, whichever occurs first. For each breach
7 requiring notice under this subsection, a copy of the notice
8 to individuals required under section 211 shall also be pro-
9 vided to the designated entity not later than the date on
10 which the notice is provided to affected individuals.

11 **SEC. 218. FEDERAL ENFORCEMENT.**

12 (a) IN GENERAL.—The Attorney General and the
13 Federal Trade Commission may enforce civil violations of
14 this subtitle.

15 (b) CIVIL ACTIONS BY THE ATTORNEY GENERAL OF
16 THE UNITED STATES.—

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

1 cation to an individual as required under this sub-
2 title shall be treated as a separate violation.

3 (2) PENALTY LIMITATION.—Notwithstanding
4 any other provision of law, the total amount of the
5 civil penalty assessed against a covered entity for
6 conduct involving the same or related acts or omis-
7 sions that results in a violation of this subtitle may
8 not exceed \$5,000,000, unless such conduct is found
9 to be willful or intentional.

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

19 (4) ADDITIONAL PENALTY LIMIT.—If a court
20 determines under paragraph (3) that a violation of
21 a provision of this subtitle was willful or intentional
22 and imposes an additional penalty, the court may
23 not impose an additional penalty in an amount that
24 exceeds \$5,000,000.

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

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

8 (A) enjoining such act or practice; or

9 (B) enforcing compliance with this subtitle.

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

14 (d) CIVIL ACTIONS BY THE FEDERAL TRADE COM-
15 MISSION.—

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

1 (2) CIVIL PENALTIES.—

2 (A) IN GENERAL.—Any covered entity that
3 violates this subtitle shall be subject to a civil
4 penalty in the amount that is not greater than
5 the product of the number of violations of this
6 subtitle and \$16,500. Each failure to provide
7 notification to an individual as required under
8 this subtitle shall be treated as a separate viola-
9 tion.

10 (B) PENALTY LIMITATION.—Notwith-
11 standing any other provision of law, the total
12 sum of civil penalties assessed against a covered
13 entity for all violations of the provisions of this
14 subtitle resulting from the same or related acts
15 or omissions may not exceed \$5,000,000, unless
16 such conduct is found to be willful or inten-
17 tional.

18 (C) 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 (D) ADDITIONAL PENALTY LIMIT.—If a
4 court determines under subparagraph (C) 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 \$5,000,000.

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

25 (e) COORDINATION OF ENFORCEMENT.—

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

4 (2) LIMITATION.—The Federal Trade Commis-
5 sion may initiate investigations under this subsection
6 unless the Attorney General determines that such an
7 investigation would impede an ongoing criminal in-
8 vestigation or national security activity.

9 (3) COORDINATION AGREEMENT.—

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

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

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

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

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

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

18 (a) IN GENERAL.—

19 (1) CIVIL ACTIONS.—

20 (A) IN GENERAL.—In any case in which
21 the attorney general of a State or any State or
22 local law enforcement agency authorized by the
23 State attorney general or by State statute to
24 prosecute violations of consumer protection law,
25 has reason to believe that a covered entity has

1 violated this subtitle, the State, as *parens*
2 *patriae*, may bring a civil action on behalf of
3 the residents of the State to—

4 (i) enjoin that practice;

5 (ii) enforce compliance with this sub-
6 title; or

7 (iii) impose a civil penalty in an
8 amount not greater than the product of
9 the number of violations of this subtitle
10 and \$16,500.

11 (B) FAILURE TO PROVIDE NOTIFICA-
12 TION.—For purposes of subparagraph (A)(iii),
13 each failure to provide notification to an indi-
14 vidual as required under this subtitle shall be
15 treated as a separate violation.

16 (2) PENALTY LIMITATION.—

17 (A) IN GENERAL.—Notwithstanding any
18 other provision of law, the total sum of civil
19 penalties assessed against a covered entity for
20 all violations of the provisions of this subtitle
21 resulting from the same or related acts or omis-
22 sions may not exceed \$5,000,000, unless such
23 conduct is found to be willful or intentional.

24 (B) DETERMINATIONS.—The determina-
25 tion of whether a violation of a provision of this

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

9 (C) ADDITIONAL PENALTY LIMIT.—If a
10 court determines under subparagraph (B) that
11 a violation of a provision of this subtitle was
12 willful or intentional and imposes an additional
13 penalty, the court may not impose an additional
14 penalty in an amount that exceeds \$5,000,000.

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 that are 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.

○