

113TH CONGRESS
2D SESSION

S. 1897

To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

IN THE SENATE OF THE UNITED STATES

JANUARY 8, 2014

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

A BILL

To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

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

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

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Personal Data Privacy and Security Act of 2014”.

6 (b) TABLE OF CONTENTS.—The table of contents of
7 this Act is as follows:

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

TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND
 OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY

- Sec. 101. Organized criminal activity in connection with unauthorized access to personally identifiable information.
 Sec. 102. Concealment of security breaches involving sensitive personally identifiable information.
 Sec. 103. Penalties for fraud and related activity in connection with computers.
 Sec. 104. Trafficking in passwords.
 Sec. 105. Conspiracy and attempted computer fraud offenses.
 Sec. 106. Criminal and civil forfeiture for fraud and related activity in connection with computers.
 Sec. 107. Limitation on civil actions involving unauthorized use.
 Sec. 108. Reporting of certain criminal cases.
 Sec. 109. Damage to critical infrastructure computers.
 Sec. 110. Limitation on actions involving unauthorized use.

TITLE II—PRIVACY AND SECURITY OF PERSONALLY
 IDENTIFIABLE INFORMATION

Subtitle A—A Data Privacy and Security Program

- Sec. 201. Purpose and applicability of data privacy and security program.
 Sec. 202. Requirements for a personal data privacy and security program.
 Sec. 203. Enforcement.
 Sec. 204. 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 law enforcement.
 Sec. 217. Enforcement.
 Sec. 218. Enforcement by State attorneys general.
 Sec. 219. Effect on Federal and State law.
 Sec. 220. Reporting on exemptions.
 Sec. 221. 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 personally identifiable informa-
4 tion are increasingly prime targets of hackers, iden-

1 tity thieves, rogue employees, and other criminals,
2 including organized and sophisticated criminal oper-
3 ations;

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

8 (3) security breaches are a serious threat to
9 consumer confidence, homeland security, national se-
10 curity, e-commerce, and economic stability;

11 (4) it is important for business entities that
12 own, use, or license personally identifiable informa-
13 tion to adopt reasonable procedures to ensure the se-
14 curity, privacy, and confidentiality of that personally
15 identifiable information;

16 (5) individuals whose personal information has
17 been compromised or who have been victims of iden-
18 tity theft should receive the necessary information
19 and assistance to mitigate their damages and to re-
20 store the integrity of their personal information and
21 identities;

22 (6) data misuse and use of inaccurate data have
23 the potential to cause serious or irreparable harm to
24 an individual's livelihood, privacy, and liberty and

1 undermine efficient and effective business and gov-
2 ernment operations;

3 (7) government access to commercial data can
4 potentially improve safety, law enforcement, and na-
5 tional security; and

6 (8) because government use of commercial data
7 containing personal information potentially affects
8 individual privacy, and law enforcement and national
9 security operations, there is a need for Congress to
10 exercise oversight over government use of commer-
11 cial data.

12 **SEC. 3. DEFINITIONS.**

13 In this Act, the following definitions shall apply:

14 (1) **AFFILIATE.**—The term “affiliate” means
15 persons related by common ownership or by cor-
16 porate control.

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

20 (3) **BUSINESS ENTITY.**—The term “business
21 entity” means any organization, corporation, trust,
22 partnership, sole proprietorship, unincorporated as-
23 sociation, or venture established to make a profit, or
24 nonprofit.

1 (4) DATA SYSTEM COMMUNICATION INFORMA-
2 TION.—The term “data system communication in-
3 formation” means dialing, routing, addressing, or
4 signaling information that identifies the origin, di-
5 rection, destination, processing, transmission, or ter-
6 mination of each communication initiated, at-
7 tempted, or received.

8 (5) DESIGNATED ENTITY.—The term “des-
9 ignated entity” means the Federal Government enti-
10 ty designated by the Secretary of Homeland Security
11 under section 216(a).

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

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

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

4 (8) PERSONALLY IDENTIFIABLE INFORMA-
5 TION.—The term “personally identifiable informa-
6 tion” means any information, or compilation of in-
7 formation, in electronic or digital form that is a
8 means of identification, as defined by section
9 1028(d)(7) of title 18, United States Code.

10 (9) PUBLIC RECORD SOURCE.—The term “pub-
11 lic record source” means the Congress, any agency,
12 any State or local government agency, the govern-
13 ment of the District of Columbia and governments
14 of the territories or possessions of the United States,
15 and Federal, State or local courts, courts martial
16 and military commissions, that maintain personally
17 identifiable information in records available to the
18 public.

19 (10) SECURITY BREACH.—

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

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

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

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

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

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

23 (iii) any lawfully authorized investiga-
24 tive, protective, or intelligence activity of a
25 law enforcement or intelligence agency of

1 the United States, a State, or a political
2 subdivision of a State.

3 (11) SENSITIVE PERSONALLY IDENTIFIABLE IN-
4 FORMATION.—The term “sensitive personally identi-
5 fiable information” means any information or com-
6 pilation of information, in electronic or digital form
7 that includes the following:

8 (A) An individual’s first and last name or
9 first initial and last name in combination with
10 any two of the following data elements:

11 (i) Home address or telephone num-
12 ber.

13 (ii) Mother’s maiden name.

14 (iii) Month, day, and year of birth.

15 (B) A non-truncated social security num-
16 ber, driver’s license number, passport number,
17 or alien registration number or other govern-
18 ment-issued unique identification number.

19 (C) Unique biometric data such as a fin-
20 gerprint, voice print, a retina or iris image, or
21 any other unique physical representation.

22 (D) A unique account identifier, including
23 a financial account number or credit or debit
24 card number, electronic identification number,
25 user name, or routing code.

1 (E) Any combination of the following data
2 elements:

3 (i) An individual's first and last name
4 or first initial and last name.

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

10 (iii) Any security code, access code, or
11 password, or source code that could be
12 used to generate such codes or passwords.

13 (12) SERVICE PROVIDER.—The term “service
14 provider” means a business entity that provides elec-
15 tronic data transmission, routing, intermediate and
16 transient storage, or connections to its system or
17 network, where the business entity providing such
18 services does not select or modify the content of the
19 electronic data, is not the sender or the intended re-
20 cipient of the data, and the business entity trans-
21 mits, routes, stores, or provides connections for per-
22 sonal information in a manner that personal infor-
23 mation is undifferentiated from other types of data
24 that such business entity transmits, routes, stores,
25 or provides connections. Any such business entity

1 shall be treated as a service provider under this Act
 2 only to the extent that it is engaged in the provision
 3 of such transmission, routing, intermediate and
 4 transient storage or connections.

5 **TITLE I—ENHANCING PUNISH-**
 6 **MENT FOR IDENTITY THEFT**
 7 **AND OTHER VIOLATIONS OF**
 8 **DATA PRIVACY AND SECU-**
 9 **RITY**

10 **SEC. 101. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION**
 11 **WITH UNAUTHORIZED ACCESS TO PERSON-**
 12 **ALLY IDENTIFIABLE INFORMATION.**

13 Section 1961(1) of title 18, United States Code, is
 14 amended by inserting “section 1030 (relating to fraud and
 15 related activity in connection with computers) if the act
 16 is a felony,” before “section 1084”.

17 **SEC. 102. 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 Personal Data Pri-
7 vacy and Security Act of 2014, intentionally and willfully
8 conceals the fact of such security breach, shall, in the
9 event that such security breach results in economic harm
10 to any individual in the amount of \$1,000 or more, be
11 fined under this title or imprisoned for not more than 5
12 years, or both.

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

16 “(c) NOTICE REQUIREMENT.—Any person seeking
17 an exemption under section 212(b) of the Personal Data
18 Privacy and Security Act of 2014 shall be immune from
19 prosecution under this section if the Federal Trade Com-
20 mission does not indicate, in writing, that such notice be
21 given under section 212(b)(3) of such Act.”.

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

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

1 (c) ENFORCEMENT AUTHORITY.—

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

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

10 **SEC. 103. PENALTIES FOR FRAUD AND RELATED ACTIVITY**
11 **IN CONNECTION WITH COMPUTERS.**

12 Section 1030(c) of title 18, United States Code, is
13 amended to read as follows:

14 “(c) The punishment for an offense under subsection
15 (a) or (b) of this section is—

16 “(1) a fine under this title or imprisonment for
17 not more than 20 years, or both, in the case of an
18 offense under subsection (a)(1) of this section;

19 “(2)(A) except as provided in subparagraph
20 (B), a fine under this title or imprisonment for not
21 more than 3 years, or both, in the case of an offense
22 under subsection (a)(2); or

1 “(B) a fine under this title or imprisonment for
2 not more than ten years, or both, in the case of an
3 offense under paragraph (a)(2) of this section, if—

4 “(i) the offense was committed for pur-
5 poses of commercial advantage or private finan-
6 cial gain;

7 “(ii) the offense was committed in the fur-
8 therance of any criminal or tortious act in viola-
9 tion of the Constitution or laws of the United
10 States, or of any State; or

11 “(iii) the value of the information obtained,
12 or that would have been obtained if the offense
13 was completed, exceeds \$5,000;

14 “(3) a fine under this title or imprisonment for
15 not more than 1 year, or both, in the case of an of-
16 fense under subsection (a)(3) of this section;

17 “(4) a fine under this title or imprisonment of
18 not more than 20 years, or both, in the case of an
19 offense under subsection (a)(4) of this section;

20 “(5)(A) except as provided in subparagraph
21 (D), a fine under this title, imprisonment for not
22 more than 20 years, or both, in the case of an of-
23 fense under subsection (a)(5)(A) of this section, if
24 the offense caused—

1 “(i) loss to 1 or more persons during any
2 1-year period (and, for purposes of an inves-
3 tigation, prosecution, or other proceeding
4 brought by the United States only, loss result-
5 ing from a related course of conduct affecting
6 1 or more other protected computers) aggre-
7 gating at least \$5,000 in value;

8 “(ii) the modification or impairment, or
9 potential modification or impairment, of the
10 medical examination, diagnosis, treatment, or
11 care of 1 or more individuals;

12 “(iii) physical injury to any person;

13 “(iv) a threat to public health or safety;

14 “(v) damage affecting a computer used by,
15 or on behalf of, an entity of the United States
16 Government in furtherance of the administra-
17 tion of justice, national defense, or national se-
18 curity; or

19 “(vi) damage affecting 10 or more pro-
20 tected computers during any 1-year period;

21 “(B) a fine under this title, imprisonment for
22 not more than 10 years, or both, in the case of an
23 offense under subsection (a)(5)(B), if the offense
24 caused a harm provided in clauses (i) through (vi)
25 of subparagraph (A) of this subsection;

1 “(C) if the offender attempts to cause or know-
2 ingly or recklessly causes death from conduct in vio-
3 lation of subsection (a)(5)(A), a fine under this title,
4 imprisonment for any term of years or for life, or
5 both; or

6 “(D) a fine under this title, imprisonment for
7 not more than 1 year, or both, for any other offense
8 under subsection (a)(5);

9 “(6) a fine under this title or imprisonment for
10 not more than 10 years, or both, in the case of an
11 offense under subsection (a)(6) of this section; or

12 “(7) a fine under this title or imprisonment for
13 not more than 10 years, or both, in the case of an
14 offense under subsection (a)(7) of this section.”.

15 **SEC. 104. TRAFFICKING IN PASSWORDS.**

16 Section 1030(a) of title 18, United States Code, is
17 amended by striking paragraph (6) and inserting the fol-
18 lowing:

19 “(6) knowingly and with intent to defraud traf-
20 fics (as defined in section 1029) in—

21 “(A) any password or similar information
22 through which a protected computer as defined
23 in subparagraphs (A) and (B) of subsection
24 (e)(2) may be accessed without authorization;
25 or

1 “(B) any means of access through which a
2 protected computer as defined in subsection
3 (e)(2)(A) may be accessed without authoriza-
4 tion.”.

5 **SEC. 105. CONSPIRACY AND ATTEMPTED COMPUTER**
6 **FRAUD OFFENSES.**

7 Section 1030(b) of title 18, United States Code, is
8 amended by inserting “for the completed offense” after
9 “punished as provided”.

10 **SEC. 106. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD**
11 **AND RELATED ACTIVITY IN CONNECTION**
12 **WITH COMPUTERS.**

13 Section 1030 of title 18, United States Code, is
14 amended by striking subsections (i) and (j) and inserting
15 the following:

16 “(i) CRIMINAL FORFEITURE.—

17 “(1) The court, in imposing sentence on any
18 person convicted of a violation of this section, or
19 convicted of conspiracy to violate this section, shall
20 order, in addition to any other sentence imposed and
21 irrespective of any provision of State law, that such
22 person forfeit to the United States—

23 “(A) such person’s interest in any prop-
24 erty, real or personal, that was used, or in-

1 tended to be used, to commit or facilitate the
2 commission of such violation; and

3 “(B) any property, real or personal, consti-
4 tuting or derived from any gross proceeds, or
5 any property traceable to such property, that
6 such person obtained, directly or indirectly, as
7 a result of such violation.

8 “(2) The criminal forfeiture of property under
9 this subsection, including any seizure and disposition
10 of the property, and any related judicial or adminis-
11 trative proceeding, shall be governed by the provi-
12 sions of section 413 of the Comprehensive Drug
13 Abuse Prevention and Control Act of 1970 (21
14 U.S.C. 853), except subsection (d) of that section.

15 “(j) CIVIL FORFEITURE.—

16 “(1) The following shall be subject to forfeiture
17 to the United States and no property right, real or
18 personal, shall exist in them:

19 “(A) Any property, real or personal, that
20 was used, or intended to be used, to commit or
21 facilitate the commission of any violation of this
22 section, or a conspiracy to violate this section.

23 “(B) Any property, real or personal, con-
24 stituting or derived from any gross proceeds ob-
25 tained directly or indirectly, or any property

1 traceable to such property, as a result of the
2 commission of any violation of this section, or
3 a conspiracy to violate this section.

4 “(2) Seizures and forfeitures under this sub-
5 section shall be governed by the provisions in chap-
6 ter 46 relating to civil forfeitures, except that such
7 duties as are imposed on the Secretary of the Treas-
8 ury under the customs laws described in section
9 981(d) shall be performed by such officers, agents
10 and other persons as may be designated for that
11 purpose by the Secretary of Homeland Security or
12 the Attorney General.”.

13 **SEC. 107. LIMITATION ON CIVIL ACTIONS INVOLVING UNAU-**
14 **THORIZED USE.**

15 Section 1030(g) of title 18, United States Code, is
16 amended—

17 (1) by inserting “(1)” before “Any person”;
18 and

19 (2) by adding at the end the following:

20 “(2) No action may be brought under this subsection
21 if a violation of a contractual obligation or agreement,
22 such as an acceptable use policy or terms of service agree-
23 ment, constitutes the sole basis for determining that ac-
24 cess to the protected computer is unauthorized, or in ex-
25 cess of authorization.”.

1 **SEC. 108. REPORTING OF CERTAIN CRIMINAL CASES.**

2 Section 1030 of title 18, United States Code, is
3 amended by adding at the end the following:

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

11 “(1) the defendant—

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

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

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

1 **SEC. 109. DAMAGE TO CRITICAL INFRASTRUCTURE COM-**
2 **PUTERS.**

3 (a) IN GENERAL.—Chapter 47 of title 18, United
4 States Code, is amended by inserting after section 1030
5 the following:

6 **“§ 1030A. Aggravated damage to a critical infrastruc-**
7 **ture computer**

8 “(a) DEFINITIONS.—In this section—

9 “(1) the terms ‘computer’ and ‘damage’ have
10 the meanings given such terms in section 1030; and

11 “(2) the term ‘critical infrastructure computer’
12 means a computer that manages or controls systems
13 or assets vital to national defense, national security,
14 national economic security, public health or safety,
15 or any combination of those matters, whether pub-
16 licly or privately owned or operated, including—

17 “(A) gas and oil production, storage, and
18 delivery systems;

19 “(B) water supply systems;

20 “(C) telecommunication networks;

21 “(D) electrical power delivery systems;

22 “(E) finance and banking systems;

23 “(F) emergency services;

24 “(G) transportation systems and services;

25 and

1 “(H) government operations that provide
2 essential services to the public.

3 “(b) OFFENSE.—It shall be unlawful to, during and
4 in relation to a felony violation of section 1030, inten-
5 tionally cause or attempt to cause damage to a critical
6 infrastructure computer, and such damage results in (or,
7 in the case of an attempt, would, if completed have re-
8 sulted in) the substantial impairment—

9 “(1) of the operation of the critical infrastruc-
10 ture computer; or

11 “(2) of the critical infrastructure associated
12 with the computer.

13 “(c) PENALTY.—Any person who violates subsection
14 (b) shall be fined under this title, imprisoned for not less
15 than 3 years nor more than 20 years, or both.

16 “(d) CONSECUTIVE SENTENCE.—Notwithstanding
17 any other provision of law—

18 “(1) a court shall not place on probation any
19 person convicted of a violation of this section;

20 “(2) except as provided in paragraph (4), no
21 term of imprisonment imposed on a person under
22 this section shall run concurrently with any other
23 term of imprisonment, including any term of impris-
24 onment imposed on the person under any other pro-

1 vision of law, including any term of imprisonment
2 imposed for the felony violation section 1030;

3 “(3) in determining any term of imprisonment
4 to be imposed for a felony violation of section 1030,
5 a court shall not in any way reduce the term to be
6 imposed for such crime so as to compensate for, or
7 otherwise take into account, any separate term of
8 imprisonment imposed or to be imposed for a viola-
9 tion of this section; and

10 “(4) a term of imprisonment imposed on a per-
11 son for a violation of this section may, in the discre-
12 tion of the court, run concurrently, in whole or in
13 part, only with another term of imprisonment that
14 is imposed by the court at the same time on that
15 person for an additional violation of this section,
16 provided that such discretion shall be exercised in
17 accordance with any applicable guidelines and policy
18 statements issued by the United States Sentencing
19 Commission pursuant to section 994 of title 28.”.

20 (b) TECHNICAL AND CONFORMING AMENDMENT.—
21 The table of sections for chapter 47 of title 18, United
22 States Code, is amended by inserting after the item relat-
23 ing to section 1030 the following:

“1030A. Aggravated damage to a critical infrastructure computer.”.

1 **SEC. 110. LIMITATION ON ACTIONS INVOLVING UNAUTHOR-**
 2 **IZED USE.**

3 Section 1030(e)(6) of title 18, United States Code,
 4 is amended by striking “alter;” and inserting “alter, but
 5 does not include access in violation of a contractual obliga-
 6 tion or agreement, such as an acceptable use policy or
 7 terms of service agreement, with an Internet service pro-
 8 vider, Internet website, or non-government employer, if
 9 such violation constitutes the sole basis for determining
 10 that access to a protected computer is unauthorized;”.

11 **TITLE II—PRIVACY AND SECU-**
 12 **RITY OF PERSONALLY IDEN-**
 13 **TIFIABLE INFORMATION**
 14 **Subtitle A—A Data Privacy and**
 15 **Security Program**

16 **SEC. 201. PURPOSE AND APPLICABILITY OF DATA PRIVACY**
 17 **AND SECURITY PROGRAM.**

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

22 (b) **APPLICABILITY.**—A business entity engaging in
 23 interstate commerce that involves collecting, accessing,
 24 transmitting, using, storing, or disposing of sensitive per-
 25 sonally identifiable information in electronic or digital
 26 form on 10,000 or more United States persons is subject

1 to the requirements for a data privacy and security pro-
2 gram under section 202 for protecting sensitive personally
3 identifiable information.

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

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

9 (A) subject to the data security require-
10 ments and standards under section 501(b) of
11 the Gramm-Leach-Bliley Act (15 U.S.C.
12 6801(b)); and

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

16 (2) HIPAA REGULATED ENTITIES.—

17 (A) COVERED ENTITIES.—Covered entities
18 subject to the Health Insurance Portability and
19 Accountability Act of 1996 (42 U.S.C. 1301 et
20 seq.), including the data security requirements
21 and implementing regulations of that Act.

22 (B) BUSINESS ENTITIES.—A business enti-
23 ty shall be deemed in compliance with this Act
24 if the business entity—

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

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

17 (3) SERVICE PROVIDERS.—A service provider
18 for any electronic communication by a third party,
19 to the extent that the service provider is exclusively
20 engaged in the transmission, routing, or temporary,
21 intermediate, or transient storage of that commu-
22 nication.

23 (4) PUBLIC RECORDS.—Public records not oth-
24 erwise subject to a confidentiality or nondisclosure
25 requirement, or information obtained from a public

1 record, including information obtained from a news
2 report or periodical.

3 (d) SAFE HARBORS.—

4 (1) IN GENERAL.—A business entity shall be
5 deemed in compliance with the privacy and security
6 program requirements under section 202 if the busi-
7 ness entity complies with or provides protection
8 equal to industry standards or standards widely ac-
9 cepted as an effective industry practice, as identified
10 by the Federal Trade Commission, that are applica-
11 ble to the type of sensitive personally identifiable in-
12 formation involved in the ordinary course of business
13 of such business entity.

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

21 **SEC. 202. REQUIREMENTS FOR A PERSONAL DATA PRIVACY**
22 **AND SECURITY PROGRAM.**

23 (a) PERSONAL DATA PRIVACY AND SECURITY PRO-
24 GRAM.—A business entity subject to this subtitle shall
25 comply with the following safeguards and any other ad-

1 ministrative, technical, or physical safeguards identified by
2 the Federal Trade Commission in a rulemaking process
3 pursuant to section 553 of title 5, United States Code,
4 for the protection of sensitive personally identifiable infor-
5 mation:

6 (1) SCOPE.—A business entity shall implement
7 a comprehensive personal data privacy and security
8 program that includes administrative, technical, and
9 physical safeguards appropriate to the size and com-
10 plexity of the business entity and the nature and
11 scope of its activities.

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

14 (A) ensure the privacy, security, and con-
15 fidentiality of sensitive personally identifying in-
16 formation;

17 (B) protect against any anticipated
18 vulnerabilities to the privacy, security, or integ-
19 rity of sensitive personally identifying informa-
20 tion; and

21 (C) protect against unauthorized access to
22 use of sensitive personally identifying informa-
23 tion that could create a significant risk of harm
24 or fraud to any individual.

1 (3) RISK ASSESSMENT.—A business entity
2 shall—

3 (A) identify reasonably foreseeable internal
4 and external vulnerabilities that could result in
5 unauthorized access, disclosure, use, or alter-
6 ation of sensitive personally identifiable infor-
7 mation or systems containing sensitive person-
8 ally identifiable information;

9 (B) assess the likelihood of and potential
10 damage from unauthorized access, disclosure,
11 use, or alteration of sensitive personally identifi-
12 able information;

13 (C) assess the sufficiency of its policies,
14 technologies, and safeguards in place to control
15 and minimize risks from unauthorized access,
16 disclosure, use, or alteration of sensitive person-
17 ally identifiable information; and

18 (D) assess the vulnerability of sensitive
19 personally identifiable information during de-
20 struction and disposal of such information, in-
21 cluding through the disposal or retirement of
22 hardware.

23 (4) RISK MANAGEMENT AND CONTROL.—Each
24 business entity shall—

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

4 (B) adopt measures commensurate with
5 the sensitivity of the data as well as the size,
6 complexity, and scope of the activities of the
7 business entity that—

8 (i) control access to systems and fa-
9 cilities containing sensitive personally iden-
10 tifiable information, including controls to
11 authenticate and permit access only to au-
12 thorized individuals;

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

20 (iii) protect sensitive personally identi-
21 fiable information during use, trans-
22 mission, storage, and disposal by
23 encryption, redaction, or access controls
24 that are widely accepted as an effective in-
25 dustry practice or industry standard, or

1 other reasonable means (including as di-
2 rected for disposal of records under section
3 628 of the Fair Credit Reporting Act (15
4 U.S.C. 1681w) and the implementing regu-
5 lations of such Act as set forth in section
6 682 of title 16, Code of Federal Regula-
7 tions);

8 (iv) ensure that sensitive personally
9 identifiable information is properly de-
10 stroyed and disposed of, including during
11 the destruction of computers, diskettes,
12 and other electronic media that contain
13 sensitive personally identifiable informa-
14 tion;

15 (v) trace access to records containing
16 sensitive personally identifiable information
17 so that the business entity can determine
18 who accessed or acquired such sensitive
19 personally identifiable information per-
20 taining to specific individuals; and

21 (vi) ensure that no third party or cus-
22 tomer of the business entity is authorized
23 to access or acquire sensitive personally
24 identifiable information without the busi-
25 ness entity first performing sufficient due

1 diligence to ascertain, with reasonable cer-
2 tainty, that such information is being
3 sought for a valid legal purpose; and

4 (C) establish a plan and procedures for
5 minimizing the amount of sensitive personally
6 identifiable information maintained by such
7 business entity, which shall provide for the re-
8 tention of sensitive personally identifiable infor-
9 mation only as reasonably needed for the busi-
10 ness purposes of such business entity or as nec-
11 essary to comply with any legal obligation.

12 (b) TRAINING.—Each business entity subject to this
13 subtitle shall take steps to ensure employee training and
14 supervision for implementation of the data security pro-
15 gram of the business entity.

16 (c) VULNERABILITY TESTING.—

17 (1) IN GENERAL.—Each business entity subject
18 to this subtitle shall take steps to ensure regular
19 testing of key controls, systems, and procedures of
20 the personal data privacy and security program to
21 detect, prevent, and respond to attacks or intrusions,
22 or other system failures.

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

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

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

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

19 (2) require the person or entity by contract to
20 implement and maintain appropriate measures de-
21 signed to meet the objectives and requirements gov-
22 erning entities subject to section 201, this section,
23 and subtitle B.

24 (e) PERIODIC ASSESSMENT AND PERSONAL DATA
25 PRIVACY AND SECURITY MODERNIZATION.—Each busi-

1 ness entity subject to this subtitle shall on a regular basis
2 monitor, evaluate, and adjust, as appropriate its data pri-
3 vacy and security program in light of any relevant changes
4 in—

5 (1) technology;

6 (2) the sensitivity of personally identifiable in-
7 formation;

8 (3) internal or external threats to personally
9 identifiable information; and

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

12 (A) mergers and acquisitions;

13 (B) alliances and joint ventures;

14 (C) outsourcing arrangements;

15 (D) bankruptcy; and

16 (E) changes to sensitive personally identifi-
17 able information systems.

18 (f) IMPLEMENTATION TIMELINE.—Not later than 1
19 year after the date of enactment of this Act, a business
20 entity subject to the provisions of this subtitle shall imple-
21 ment a data privacy and security program pursuant to this
22 subtitle.

23 **SEC. 203. ENFORCEMENT.**

24 (a) CIVIL PENALTIES.—

1 (1) IN GENERAL.—Any business entity that vio-
2 lates the provisions of section 201 or 202 shall be
3 subject to civil penalties of not more than \$5,000
4 per violation per day while such a violation exists,
5 with a maximum of \$500,000 per violation.

6 (2) INTENTIONAL OR WILLFUL VIOLATION.—A
7 business entity that intentionally or willfully violates
8 the provisions of section 201 or 202 shall be subject
9 to additional penalties in the amount of \$5,000 per
10 violation per day while such a violation exists, with
11 a maximum of an additional \$500,000 per violation.

12 (3) PENALTY LIMITS.—

13 (A) IN GENERAL.—Notwithstanding any
14 other provision of law, the total sum of civil
15 penalties assessed against a business entity for
16 all violations of the provisions of this subtitle
17 resulting from the same or related acts or omis-
18 sions shall not exceed \$500,000, unless such
19 conduct is found to be willful or intentional.

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

1 sion of this subtitle was willful or intentional,
2 and if so, the amount of the additional penalty
3 to be imposed, if any, shall be made by the
4 court sitting as the finder of fact.

5 (C) ADDITIONAL PENALTY LIMIT.—If a
6 court determines under subparagraph (B) that
7 a violation of a provision of this subtitle was
8 willful or intentional and imposes an additional
9 penalty, the court may not impose an additional
10 penalty in an amount that exceeds \$500,000.

11 (4) EQUITABLE RELIEF.—A business entity en-
12 gaged in interstate commerce that violates this sec-
13 tion may be enjoined from further violations by a
14 United States district court.

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

19 (b) FEDERAL TRADE COMMISSION AUTHORITY.—
20 Any business entity shall have the provisions of this sub-
21 title enforced against it by the Federal Trade Commission.

22 (c) STATE ENFORCEMENT.—

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

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

9 (A) enjoin that act or practice;

10 (B) enforce compliance with this subtitle;

11 or

12 (C) obtain civil penalties of not more than
13 \$5,000 per violation per day while such viola-
14 tions persist, up to a maximum of \$500,000 per
15 violation.

16 (2) PENALTY LIMITS.—

17 (A) IN GENERAL.—Notwithstanding any
18 other provision of law, the total sum of civil
19 penalties assessed against a business entity for
20 all violations of the provisions of this subtitle
21 resulting from the same or related acts or omis-
22 sions shall not exceed \$500,000, 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 \$500,000.

15 (3) NOTICE.—

16 (A) IN GENERAL.—Before filing an action
17 under this subsection, the attorney general of
18 the State involved shall provide to the Federal
19 Trade Commission—

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

21 (ii) a copy of the complaint for that
22 action.

23 (B) EXCEPTION.—Subparagraph (A) shall
24 not apply with respect to the filing of an action
25 by an attorney general of a State under this

1 subsection, if the attorney general of a State
2 determines that it is not feasible to provide the
3 notice described in this subparagraph before the
4 filing of the action.

5 (C) NOTIFICATION WHEN PRACTICABLE.—
6 In an action described under subparagraph (B),
7 the attorney general of a State shall provide the
8 written notice and the copy of the complaint to
9 the Federal Trade Commission as soon after
10 the filing of the complaint as practicable.

11 (4) FEDERAL TRADE COMMISSION AUTHOR-
12 ITY.—Upon receiving notice under paragraph (2),
13 the Federal Trade Commission shall have the right
14 to—

15 (A) move to stay the action, pending the
16 final disposition of a pending Federal pro-
17 ceeding or action as described in paragraph (4);

18 (B) intervene in an action brought under
19 paragraph (1); and

20 (C) file petitions for appeal.

21 (5) PENDING PROCEEDINGS.—If the Federal
22 Trade Commission initiates a Federal civil action for
23 a violation of this subtitle, or any regulations there-
24 under, no attorney general of a State may bring an
25 action for a violation of this subtitle that resulted

1 from the same or related acts or omissions against
2 a defendant named in the Federal civil action initi-
3 ated by the Federal Trade Commission.

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

10 (A) conduct investigations;

11 (B) administer oaths and affirmations; or

12 (C) compel the attendance of witnesses or
13 the production of documentary and other evi-
14 dence.

15 (7) VENUE; SERVICE OF PROCESS.—

16 (A) VENUE.—Any action brought under
17 this subsection may be brought in the district
18 court of the United States that meets applicable
19 requirements relating to venue under section
20 1391 of title 28, United States Code.

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

24 (i) is an inhabitant; or

25 (ii) may be found.

1 (d) NO PRIVATE CAUSE OF ACTION.—Nothing in
2 this subtitle establishes a private cause of action against
3 a business entity for violation of any provision of this sub-
4 title.

5 **SEC. 204. RELATION TO OTHER LAWS.**

6 (a) IN GENERAL.—No State may require any busi-
7 ness entity subject to this subtitle to comply with any re-
8 quirements with respect to administrative, technical, and
9 physical safeguards for the protection of personal informa-
10 tion.

11 (b) LIMITATIONS.—Nothing in this subtitle shall be
12 construed to modify, limit, or supersede the operation of
13 the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) or
14 its implementing regulations, including those adopted or
15 enforced by States.

16 **Subtitle B—Security Breach**
17 **Notification**

18 **SEC. 211. NOTICE TO INDIVIDUALS.**

19 (a) IN GENERAL.—Except as provided in section 212,
20 any agency, or business entity engaged in interstate com-
21 merce, other than a service provider, that uses, accesses,
22 transmits, stores, disposes of or collects sensitive person-
23 ally identifiable information shall, following the discovery
24 of a security breach of such information, notify any resi-
25 dent of the United States whose sensitive personally iden-

1 tifiable information has been, or is reasonably believed to
2 have been, accessed, or acquired.

3 (b) OBLIGATION OF OWNER OR LICENSEE.—

4 (1) NOTICE TO OWNER OR LICENSEE.—Any
5 agency, or business entity engaged in interstate com-
6 merce, that uses, accesses, transmits, stores, dis-
7 poses of, or collects sensitive personally identifiable
8 information that the agency or business entity does
9 not own or license shall notify the owner or licensee
10 of the information following the discovery of a secu-
11 rity breach involving such information.

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

21 (3) BUSINESS ENTITY RELIEVED FROM GIVING
22 NOTICE.—A business entity obligated to give notice
23 under subsection (a) shall be relieved of such obliga-
24 tion if an owner or licensee of the sensitive person-
25 ally identifiable information subject to the security

1 breach, or other designated third party, provides
2 such notification.

3 (4) SERVICE PROVIDERS.—If a service provider
4 becomes aware of a security breach of data in elec-
5 tronic form containing sensitive personal information
6 that is owned or possessed by another business enti-
7 ty that connects to or uses a system or network pro-
8 vided by the service provider for the purpose of
9 transmitting, routing, or providing intermediate or
10 transient storage of such data, the service provider
11 shall be required to notify the business entity who
12 initiated such connection, transmission, routing, or
13 storage of the security breach if the business entity
14 can be reasonably identified. Upon receiving such
15 notification from a service provider, the business en-
16 tity shall be required to provide the notification re-
17 quired under subsection (a).

18 (c) TIMELINESS OF NOTIFICATION.—

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

23 (2) REASONABLE DELAY.—

24 (A) IN GENERAL.—Reasonable delay under
25 this subsection may include any time necessary

1 to determine the scope of the security breach,
2 prevent further disclosures, conduct the risk as-
3 sessment described in section 202(a)(3), and re-
4 store the reasonable integrity of the data sys-
5 tem and provide notice to law enforcement
6 when required.

7 (B) EXTENSION.—

8 (i) IN GENERAL.—Except as provided
9 in subsection (d), delay of notification shall
10 not exceed 60 days following the discovery
11 of the security breach, unless the business
12 entity or agency requests an extension of
13 time and the Federal Trade Commission
14 determines in writing that additional time
15 is reasonably necessary to determine the
16 scope of the security breach, prevent fur-
17 ther disclosures, conduct the risk assess-
18 ment, restore the reasonable integrity of
19 the data system, or to provide notice to the
20 designated entity.

21 (ii) APPROVAL OF REQUEST.—If the
22 Federal Trade Commission approves the
23 request for delay, the agency or business
24 entity may delay the time period for notifi-

1 cation for additional periods of up to 30
2 days.

3 (3) BURDEN OF PRODUCTION.—The agency,
4 business entity, owner, or licensee required to pro-
5 vide notice under this subtitle shall, upon the re-
6 quest of the Attorney General or the Federal Trade
7 Commission provide records or other evidence of the
8 notifications required under this subtitle, including
9 to the extent applicable, the reasons for any delay of
10 notification.

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

13 (1) IN GENERAL.—If the United States Secret
14 Service or the Federal Bureau of Investigation de-
15 termines that the notification required under this
16 section would impede a criminal investigation, or na-
17 tional security activity, such notification shall be de-
18 layed upon written notice from the United States
19 Secret Service or the Federal Bureau of Investiga-
20 tion to the agency or business entity that experi-
21 enced the breach. The notification from the United
22 States Secret Service or the Federal Bureau of In-
23 vestigation shall specify in writing the period of
24 delay requested for law enforcement or national se-
25 curity purposes.

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

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

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

17 (1) FINANCIAL INSTITUTIONS.—Financial insti-
18 tutions—

19 (A) subject to the data security require-
20 ments and standards under section 501(b) of
21 the Gramm-Leach-Bliley Act (15 U.S.C.
22 6801(b)); and

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

1 (2) HIPAA REGULATED ENTITIES.—

2 (A) COVERED ENTITIES.—Covered entities
3 subject to the Health Insurance Portability and
4 Accountability Act of 1996 (42 U.S.C. 1301 et
5 seq.), including the data security requirements
6 and implementing regulations of that Act.

7 (B) BUSINESS ENTITIES.—A business enti-
8 ty shall be deemed in compliance with this Act
9 if the business entity—

10 (i)(I) is acting as a covered entity and
11 as a business associate, as those terms are
12 defined under the Health Insurance Port-
13 ability and Accountability Act of 1996 (42
14 U.S.C. 1301 et seq.) and is in compliance
15 with the requirements imposed under that
16 Act and implementing regulations promul-
17 gated under that Act; and

18 (II) is subject to, and currently in
19 compliance, with the data breach notifica-
20 tion, privacy and data security require-
21 ments under the Health Information Tech-
22 nology for Economic and Clinical Health
23 (HITECH) Act, (42 U.S.C. 17932) and
24 implementing regulations promulgated
25 thereunder; or

1 (ii) is acting as a vendor of personal
2 health records and third party service pro-
3 vider, subject to the Health Information
4 Technology for Economic and Clinical
5 Health (HITECH) Act (42 U.S.C. 17937),
6 including the data breach notification re-
7 quirements and implementing regulations
8 of that Act.

9 **SEC. 212. EXEMPTIONS.**

10 (a) EXEMPTION FOR NATIONAL SECURITY AND LAW
11 ENFORCEMENT.—

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

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

21 (B) the Federal Bureau of Investigation
22 determines that notification of the security
23 breach could be expected to cause damage to
24 the national security.

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

6 (b) SAFE HARBOR.—

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

10 (A) a risk assessment conducted by the
11 agency or business entity concludes that, based
12 upon the information available, there is no sig-
13 nificant risk that a security breach has resulted
14 in, or will result in, identity theft, economic loss
15 or harm, or physical harm to the individuals
16 whose sensitive personally identifiable informa-
17 tion was subject to the security breach;

18 (B) without unreasonable delay, but not
19 later than 45 days after the discovery of a secu-
20 rity breach, unless extended by the Federal
21 Trade Commission, the agency or business enti-
22 ty notifies the Federal Trade Commission, in
23 writing, of—

24 (i) the results of the risk assessment;

25 and

1 (ii) its decision to invoke the risk as-
2 sessment exemption; and

3 (C) the Federal Trade Commission does
4 not indicate, in writing, within 10 business days
5 from receipt of the decision, that notice should
6 be given.

7 (2) REBUTTABLE PRESUMPTIONS.—For pur-
8 poses of paragraph (1)—

9 (A) the encryption of sensitive personally
10 identifiable information described in paragraph
11 (1)(A)(i) shall establish a rebuttable presump-
12 tion that no significant risk exists; and

13 (B) the rendering of sensitive personally
14 identifiable information described in paragraph
15 (1)(A)(ii) unusable, unreadable, or indecipher-
16 able through data security technology or meth-
17 odology that is generally accepted by experts in
18 the field of information security, such as redac-
19 tion or access controls shall establish a rebutta-
20 ble presumption that no significant risk exists.

21 (3) VIOLATION.—It shall be a violation of this
22 section to—

23 (A) fail to conduct the risk assessment in
24 a reasonable manner, or according to standards

1 generally accepted by experts in the field of in-
2 formation security; or

3 (B) submit the results of a risk assessment
4 that contains fraudulent or deliberately mis-
5 leading information.

6 (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

7 (1) IN GENERAL.—A business entity will be ex-
8 empt from the notice requirement under section 211
9 if the business entity utilizes or participates in a se-
10 curity program that—

11 (A) effectively blocks the use of the sen-
12 sitive personally identifiable information to ini-
13 tiate unauthorized financial transactions before
14 they are charged to the account of the indi-
15 vidual; and

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

19 (2) LIMITATION.—The exemption in paragraph
20 (1) does not apply if the information subject to the
21 security breach includes an individual's first and last
22 name, or any other type of sensitive personally iden-
23 tifiable information as defined in section 3, unless
24 that information is only a credit card number or
25 credit card security code.

1 **SEC. 213. METHODS OF NOTICE.**

2 An agency or business entity shall be in compliance
3 with section 211 if it provides the following:

4 (1) **INDIVIDUAL NOTICE.**—Notice to individuals
5 by one of the following means:

6 (A) Written notification to the last known
7 home mailing address of the individual in the
8 records of the agency or business entity.

9 (B) Telephone notice to the individual per-
10 sonally.

11 (C) E-mail notice, if the individual has
12 consented to receive such notice and the notice
13 is consistent with the provisions permitting elec-
14 tronic transmission of notices under section 101
15 of the Electronic Signatures in Global and Na-
16 tional Commerce Act (15 U.S.C. 7001).

17 (2) **MEDIA NOTICE.**—Notice to major media
18 outlets serving a State or jurisdiction, if the number
19 of residents of such State whose sensitive personally
20 identifiable information was, or is reasonably be-
21 lieved to have been, accessed or acquired by an un-
22 authorized person exceeds 5,000.

23 **SEC. 214. CONTENT OF NOTIFICATION.**

24 (a) **IN GENERAL.**—Regardless of the method by
25 which notice is provided to individuals under section 213,
26 such notice shall include, to the extent possible—

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

5 (2) a toll-free number—

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

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

13 (3) the toll-free contact telephone numbers and
14 addresses for the major credit reporting agencies.

15 (b) **ADDITIONAL CONTENT.**—Notwithstanding sec-
16 tion 219, a State may require that a notice under sub-
17 section (a) shall also include information regarding victim
18 protection assistance provided for by that State.

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

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

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

14 **SEC. 216. NOTICE TO LAW ENFORCEMENT.**

15 (a) DESIGNATION OF GOVERNMENT ENTITY TO RE-
16 CEIVE NOTICE.—

17 (1) IN GENERAL.—Not later than 60 days after
18 the date of enactment of this Act, the Secretary of
19 Homeland Security shall designate a Federal Gov-
20 ernment entity to receive the notices required under
21 section 212 and this section, and any other reports
22 and information about information security inci-
23 dents, threats, and vulnerabilities.

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

1 (A) be responsible for promptly providing
2 the information that it receives to the United
3 States Secret Service and the Federal Bureau
4 of Investigation, and to the Federal Trade
5 Commission for civil law enforcement purposes;
6 and

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

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

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

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

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

1 (4) the security breach involves primarily sen-
2 sitive personally identifiable information of individ-
3 uals known to the agency or business entity to be
4 employees and contractors of the Federal Govern-
5 ment involved in national security or law enforce-
6 ment.

7 (c) FTC RULEMAKING AND REVIEW OF THRESH-
8 OLDS.—

9 (1) REPORTS.—Not later than 1 year after the
10 date of the enactment of this Act, the Federal Trade
11 Commission, in consultation with the Attorney Gen-
12 eral of the United States and the Secretary of
13 Homeland Security, shall promulgate regulations
14 under section 553 of title 5, United States Code, re-
15 garding the reports required under subsection (a).

16 (2) THRESHOLDS FOR NOTICE.—The Federal
17 Trade Commission, in consultation with the Attor-
18 ney General and the Secretary of Homeland Secu-
19 rity, after notice and the opportunity for public com-
20 ment, and in a manner consistent with this section,
21 shall promulgate regulations, as necessary, under
22 section 553 of title 5, United States Code, to adjust
23 the thresholds for notice to law enforcement and na-
24 tional security authorities under subsection (a) and
25 to facilitate the purposes of this section.

1 (d) TIMING.—The notice required under subsection
2 (a) shall be provided as promptly as possible, but such
3 notice must be provided either 72 hours before notice is
4 provided to an individual pursuant to section 211, or not
5 later than 10 days after the business entity or agency dis-
6 covers the security breach or discovers that the nature of
7 the security breach requires notice to law enforcement
8 under this section, whichever occurs first.

9 **SEC. 217. ENFORCEMENT.**

10 (a) IN GENERAL.—The Attorney General and the
11 Federal Trade Commission may enforce civil violations of
12 section 211.

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 business 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 business entity shall be
21 subject to a civil penalty of not more than \$11,000
22 per day per security breach.

23 (2) PENALTY LIMITATION.—Notwithstanding
24 any other provision of law, the total amount of the
25 civil penalty assessed against a business entity for

1 conduct involving the same or related acts or omis-
2 sions that results in a violation of this subtitle may
3 not exceed \$1,000,000.

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

13 (4) ADDITIONAL PENALTY LIMIT.—If a court
14 determines under paragraph (3) that a violation of
15 a provision of this subtitle was willful or intentional
16 and imposes an additional penalty, the court may
17 not impose an additional penalty in an amount that
18 exceeds \$1,000,000.

19 (c) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-
20 ERAL.—

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

1 (A) enjoining such act or practice; or

2 (B) enforcing compliance with this subtitle.

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

7 (d) CIVIL ACTIONS BY THE FEDERAL TRADE COM-
8 MISSION.—

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

19 (2) PENALTY LIMITATION.—

20 (A) IN GENERAL.—Notwithstanding any
21 other provision of law, the total sum of civil
22 penalties assessed against a business entity for
23 all violations of the provisions of this subtitle
24 resulting from the same or related acts or omis-

1 sions may not exceed \$1,000,000, unless such
2 conduct is found to be willful or intentional.

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

13 (C) ADDITIONAL PENALTY LIMIT.—If a
14 court determines under subparagraph (B) that
15 a violation of a provision of this subtitle was
16 willful or intentional and imposes an additional
17 penalty, the court may not impose an additional
18 penalty in an amount that exceeds \$1,000,000.

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

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

10 (e) COORDINATION OF ENFORCEMENT.—

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

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

19 (3) COORDINATION AGREEMENT.—

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

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

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

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

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

11 **SEC. 218. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

12 (a) IN GENERAL.—

13 (1) CIVIL ACTIONS.—In any case in which the
14 attorney general of a State or any State or local law
15 enforcement agency authorized by the State attorney
16 general or by State statute to prosecute violations of
17 consumer protection law, has reason to believe that
18 an interest of the residents of that State has been
19 or is threatened or adversely affected by the engage-
20 ment of a business entity in a practice that is pro-
21 hibited under this subtitle, the State or the State or
22 local law enforcement agency on behalf of the resi-
23 dents of the agency’s jurisdiction, may bring a civil
24 action on behalf of the residents of the State or ju-

1 jurisdiction in a district court of the United States of
2 appropriate jurisdiction to—

3 (A) enjoin that practice;

4 (B) enforce compliance with this subtitle;

5 or

6 (C) civil penalties of not more than
7 \$11,000 per day per security breach up to a
8 maximum of \$1,000,000 per violation, unless
9 such conduct is found to be willful or inten-
10 tional.

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 business 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 \$1,000,000, 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 \$1,000,000.

10 (3) NOTICE.—

11 (A) IN GENERAL.—Before filing an action
12 under paragraph (1), the attorney general of
13 the State involved shall provide to the Attorney
14 General of the United States—

15 (i) written notice of the action; and

16 (ii) a copy of the complaint for the ac-
17 tion.

18 (B) EXEMPTION.—

19 (i) IN GENERAL.—Subparagraph (A)
20 shall not apply with respect to the filing of
21 an action by an attorney general of a State
22 under this subtitle, if the State attorney
23 general determines that it is not feasible to
24 provide the notice described in such sub-
25 paragraph before the filing of the action.

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

7 (b) FEDERAL PROCEEDINGS.—Upon receiving notice
8 under subsection (a)(2), the Attorney General shall have
9 the right to—

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

13 (2) initiate an action in the appropriate United
14 States district court under section 217 and move to
15 consolidate all pending actions, including State ac-
16 tions, in such court;

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

19 (4) file petitions for appeal.

20 (c) PENDING PROCEEDINGS.—If the Attorney Gen-
21 eral or the Federal Trade Commission initiate a criminal
22 proceeding or civil action for a violation of a provision of
23 this subtitle, or any regulations thereunder, no attorney
24 general of a State may bring an action for a violation of

1 a provision of this subtitle against a defendant named in
2 the Federal criminal proceeding or civil action.

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

9 (1) conduct investigations;

10 (2) administer oaths or affirmations; or

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

13 (e) VENUE; SERVICE OF PROCESS.—

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

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

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

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

25 (A) is an inhabitant; or

1 (B) may be found.

2 (f) NO PRIVATE CAUSE OF ACTION.—Nothing in this
3 subtitle establishes a private cause of action against a
4 business entity for violation of any provision of this sub-
5 title.

6 **SEC. 219. EFFECT ON FEDERAL AND STATE LAW.**

7 For any entity, or agency that is subject to this sub-
8 title, the provisions of this subtitle shall supersede any
9 other provision of Federal law, or any provisions of the
10 law of any State, relating to notification of a security
11 breach, except as provided in section 214(b). Nothing in
12 this subtitle shall be construed to modify, limit, or super-
13 sede the operation of the Gramm-Leach-Bliley Act (15
14 U.S.C. 6801 et seq.) or its implementing regulations, in-
15 cluding those regulations adopted or enforced by States,
16 the Health Insurance Portability and Accountability Act
17 of 1996 (42 U.S.C. 1301 et seq.) or its implementing reg-
18 ulations, or the Health Information Technology for Eco-
19 nomic and Clinical Health Act (42 U.S.C. 17937) or its
20 implementing regulations.

21 **SEC. 220. REPORTING ON EXEMPTIONS.**

22 (a) FTC REPORT.—Not later than 18 months after
23 the date of enactment of this Act, and upon request by
24 Congress thereafter, the Federal Trade Commission shall
25 submit a report to Congress on the number and nature

1 of the security breaches described in the notices filed by
2 those business entities invoking the risk assessment ex-
3 emption under section 212(b) and their response to such
4 notices.

5 (b) LAW ENFORCEMENT REPORT.—

6 (1) IN GENERAL.—Not later than 18 months
7 after the date of enactment of this Act, and upon
8 the request by Congress thereafter, the United
9 States Secret Service and Federal Bureau of Inves-
10 tigation shall submit a report to Congress on the
11 number and nature of security breaches subject to
12 the national security and law enforcement exemp-
13 tions under section 212(a).

14 (2) REQUIREMENT.—The report required under
15 paragraph (1) shall not include the contents of any
16 risk assessment provided to the United States Secret
17 Service and the Federal Bureau of Investigation
18 under this subtitle.

19 **SEC. 221. EFFECTIVE DATE.**

20 This subtitle shall take effect on the expiration of the
21 date which is 90 days after the date of enactment of this
22 Act.

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

3 **SEC. 301. BUDGET COMPLIANCE.**

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

○