

Calendar No. 182112TH CONGRESS
1ST SESSION**S. 1535**

To protect consumers by mitigating the vulnerability of personally identifiable information to theft through a security breach, providing notice and remedies to consumers in the wake of such a breach, holding companies accountable for preventable breaches, facilitating the sharing of post-breach technical information between companies, and enhancing criminal and civil penalties and other protections against the unauthorized collection or use of personally identifiable information.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 8, 2011

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

SEPTEMBER 22, 2011

Reported by Mr. LEAHY, with an amendment

[Strike out all after the enacting clause and insert the part printed in *italic*]

A BILL

To protect consumers by mitigating the vulnerability of personally identifiable information to theft through a security breach, providing notice and remedies to consumers in the wake of such a breach, holding companies accountable for preventable breaches, facilitating the sharing of post-breach technical information between companies, and enhancing criminal and civil penalties and other

protections against the unauthorized collection or use of personally identifiable information.

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

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

4 (a) **SHORT TITLE.**—This Act may be cited as the
 5 “Personal Data Protection and Breach Accountability Act
 6 of 2011”.

7 (b) **TABLE OF CONTENTS.**—The table of contents of
 8 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. False notification.
 Sec. 105. Unauthorized installation of personal information collection features on a user’s computer.

**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. Federal enforcement.
 Sec. 204. Enforcement by State Attorneys General.
 Sec. 205. Supplemental enforcement by individuals.

Subtitle B—Security Breach Notification

Sec. 211. Notice to individuals.
 Sec. 212. Exemptions from notice to individuals.
 Sec. 213. Methods of notice to individuals.
 Sec. 214. Content of notice to individuals.
 Sec. 215. Remedies for security breach.
 Sec. 216. Notice to credit reporting agencies.

Sec. 217. Notice to law enforcement.
 Sec. 218. Federal enforcement.
 Sec. 219. Enforcement by State attorneys general.
 Sec. 220. Supplemental enforcement by individuals.
 Sec. 221. Relation to other laws.
 Sec. 222. Authorization of appropriations.
 Sec. 223. Reporting on risk assessment exemptions.

Subtitle C—Post-Breach Technical Information Clearinghouse

Sec. 230. Clearinghouse information collection, maintenance, and access.
 Sec. 231. Protections for clearinghouse participants.
 Sec. 232. Effective date.

TITLE III—ACCESS TO AND USE OF COMMERCIAL DATA

Sec. 301. General services administration review of contracts.
 Sec. 302. Requirement to audit information security practices of contractors and third party business entities.
 Sec. 303. Privacy impact assessment of government use of commercial information services containing personally identifiable information.
 Sec. 304. FBI report on reported breaches and compliance.
 Sec. 305. Department of Justice report on enforcement actions.
 Sec. 306. Department of Justice report on enforcement actions.
 Sec. 307. FBI report on notification effectiveness.

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

Sec. 401. Budget compliance.

1 **SEC. 2. FINDINGS.**

2 Congress finds that—

3 (1) databases of personally identifiable informa-
 4 tion are increasingly prime targets of hackers, iden-
 5 tity thieves, rogue employees, and other criminals,
 6 including organized and sophisticated criminal oper-
 7 ations;

8 (2) identity theft is a serious threat to the Na-
 9 tion's economic stability, homeland security, the de-
 10 velopment of e-commerce, and the privacy rights of
 11 Americans;

1 (3) over 9,300,000 individuals were victims of
2 identity theft in America last year;

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

6 (5) it is important for business entities that
7 own, use, or license personally identifiable informa-
8 tion to adopt reasonable procedures to ensure the se-
9 curity, privacy, and confidentiality of that personally
10 identifiable information;

11 (6) individuals whose personal information has
12 been compromised or who have been victims of iden-
13 tity theft should receive the necessary information
14 and assistance to mitigate their damages and to re-
15 store the integrity of their personal information and
16 identities;

17 (7) data brokers have assumed a significant
18 role in providing identification, authentication, and
19 screening services, and related data collection and
20 analyses for commercial, nonprofit, and government
21 operations;

22 (8) 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 (9) there is a need to ensure that data brokers
4 conduct their operations in a manner that prioritizes
5 fairness, transparency, accuracy, and respect for the
6 privacy of consumers;

7 (10) government access to commercial data can
8 potentially improve safety, law enforcement, and na-
9 tional security;

10 (11) because government use of commercial
11 data containing personal information potentially af-
12 fects individual privacy, and law enforcement and
13 national security operations, there is a need for Con-
14 gress to exercise oversight over government use of
15 commercial data;

16 (12) over 22,960,000 cases of data breaches in-
17 volving personally identifiable information were re-
18 ported through July of 2011, and in 2009 through
19 2010, over 230,900,000 cases of personal data
20 breaches were reported;

21 (13) facilitating information sharing among
22 business entities and across sectors in the event of
23 a breach can assist in remediating the breach and
24 preventing similar breaches in the future;

1 (14) because the Federal Government has lim-
 2 ited resources, consumers themselves play a vital
 3 and complementary role in facilitating prompt notifi-
 4 cation and protecting against future breaches of se-
 5 curity;

6 (15) in addition to the immediate damages
 7 caused by security breaches, the lack of basic reme-
 8 dial requirements often forces individuals whose sen-
 9 sitive personally identifiable information is com-
 10 promised as a result of a security breach to incur
 11 the economic costs of litigation to seek remedies, and
 12 the economic costs of fees required in many States
 13 to freeze compromised accounts; and

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

18 **SEC. 3. DEFINITIONS.**

19 In this Act, the following definitions shall apply:

20 (1) **AFFILIATE.**—The term “affiliate” means
 21 persons related by common ownership or by cor-
 22 porate control.

23 (2) **AGENCY.**—The term “agency” has the
 24 meaning given such term in section 551 of title 5,
 25 United States Code.

1 (3) BUSINESS ENTITY.—The term “business
2 entity” means any organization, corporation, trust,
3 partnership, sole proprietorship, unincorporated as-
4 sociation, or venture established to make a profit, or
5 nonprofit.

6 (4) CREDIT RATING AGENCY.—The term “cred-
7 it rating agency” has the meaning given such term
8 in section 3(a)(61) of the Securities Exchange Act
9 of 1934 (12 U.S.C. 78c(a)(61)).

10 (5) CREDIT REPORT.—The term “credit report”
11 means a consumer report, as that term is defined in
12 section 603 of the Fair Credit Reporting Act (15
13 U.S.C. 1681a).

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

23 (7) DATA FURNISHER.—The term “data fur-
24 nisher” means any agency, organization, corpora-
25 tion, trust, partnership, sole proprietorship, unincor-

1 porated association, or nonprofit that serves as a
2 source of information for a data broker.

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

4 (A) means the protection of data in elec-
5 tronic form, in storage or in transit, using an
6 encryption technology that has been adopted by
7 a widely accepted standards setting body or,
8 has been widely accepted as an effective indus-
9 try practice which renders such data indecipher-
10 able in the absence of associated cryptographic
11 keys necessary to enable decryption of such
12 data; and

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

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

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

21 (A) The Office of the Director of National
22 Intelligence.

23 (B) The Central Intelligence Agency.

24 (C) The National Security Agency.

25 (D) The Defense Intelligence Agency.

1 (~~E~~) The National Geospatial-Intelligence
2 Agency.

3 (~~F~~) The National Reconnaissance Office.

4 (~~G~~) Other offices within the Department of
5 Defense for the collection of specialized national
6 intelligence through reconnaissance programs.

7 (~~H~~) The intelligence elements of the Army,
8 the Navy, the Air Force, the Marine Corps, the
9 Federal Bureau of Investigation, and the De-
10 partment of Energy.

11 (~~I~~) The Bureau of Intelligence and Re-
12 search of the Department of State.

13 (~~J~~) The Office of Intelligence and Analysis
14 of the Department of the Treasury.

15 (~~K~~) The elements of the Department of
16 Homeland Security concerned with the analysis
17 of intelligence information, including the Office
18 of Intelligence of the Coast Guard.

19 (~~L~~) Such other elements of any other de-
20 partment or agency as may be designated by
21 the President, or designated jointly by the Di-
22 rector of National Intelligence and the head of
23 the department or agency concerned, as an ele-
24 ment of the intelligence community.

25 (~~11~~) PERSONAL ELECTRONIC RECORD.—

1 (A) IN GENERAL.—The term “personal
2 electronic record” means data associated with
3 an individual contained in a database,
4 networked or integrated databases, or other
5 data system that is provided by a data broker
6 to nonaffiliated third parties and includes per-
7 sonally identifiable information about that indi-
8 vidual.

9 (B) EXCLUSIONS.—The term “personal
10 electronic record” does not include—

11 (i) any data related to an individual’s
12 past purchases of consumer goods; or

13 (ii) any proprietary assessment or
14 evaluation of an individual or any propri-
15 etary assessment or evaluation of informa-
16 tion about an individual.

17 (12) PERSONALLY IDENTIFIABLE INFORMA-
18 TION.—The term “personally identifiable informa-
19 tion” means any information, or compilation of in-
20 formation, in electronic or digital form that is a
21 means of identification (as defined in section
22 1028(d)(7) of title 18, United State Code).

23 (13) PREDISPUTE ARBITRATION AGREEMENT.—
24 The term “predispute arbitration agreement” means
25 any agreement to arbitrate a dispute that had not

1 yet arisen at the time of the making of the agree-
 2 ment.

3 (14) PUBLIC RECORD SOURCE.—The term
 4 “public record source” means the Congress, any
 5 agency, any State or local government agency, the
 6 government of the District of Columbia and govern-
 7 ments of the territories or possessions of the United
 8 States, and Federal, State or local courts, courts
 9 martial and military commissions, that maintain
 10 personally identifiable information in records avail-
 11 able to the public.

12 (15) SECURITY BREACH.—

13 (A) IN GENERAL.—The term “security
 14 breach” means compromise of the security, con-
 15 fidentiality, or integrity of computerized data
 16 through misrepresentation or actions—

17 (i) that result in, or that there is a
 18 reasonable basis to conclude has resulted
 19 in—

20 (I) the unauthorized acquisition
 21 of sensitive personally identifiable in-
 22 formation; or

23 (II) access to sensitive personally
 24 identifiable information that is for an

1 unauthorized purpose, or in excess of
2 authorization; and

3 (ii) which present a significant risk of
4 harm or fraud to any individual.

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

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

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 criminal
18 investigation or authorized investigative,
19 protective, or intelligence activities that are
20 carried out by or on behalf of any element
21 of the intelligence community and con-
22 ducted in accordance with the United
23 States laws, authorities, and regulations
24 governing such intelligence activities.

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

8 (17) SENSITIVE PERSONALLY IDENTIFIABLE IN-
 9 FORMATION.—The term “sensitive personally identi-
 10 fiable information” means any information or com-
 11 pilation of information, in electronic or digital form
 12 that includes—

13 (A) an individual’s first and last name or
 14 first initial and last name in combination with
 15 any 1 of the following data elements:

16 (i) A nontruncated social security
 17 number, driver’s license number, passport
 18 number, or alien registration number.

19 (ii) Any 2 of the following:

20 (I) Home address.

21 (II) Telephone number.

22 (III) Mother’s maiden name.

23 (IV) Month, day, and year of
 24 birth.

1 (iii) Unique biometric data such as a
2 finger print, voice print, a retina or iris
3 image, or any other unique physical rep-
4 resentation.

5 (iv) A unique account identifier, elec-
6 tronic identification number, user name, or
7 routing code in combination with any asso-
8 ciated security code, access code, or pass-
9 word if the code or password is required
10 for an individual to obtain money, goods,
11 services, or any other thing of value;

12 (B) a financial account number or credit
13 or debit card number in combination with any
14 security code, access code, or password that is
15 required for an individual to obtain credit, with-
16 draw funds, or engage in a financial trans-
17 action; or

18 (C) any other combination of data ele-
19 ments that could allow unauthorized access to
20 or acquisition of the information described in
21 subparagraph (A) or (B), including—

22 (i) a unique account identifier;
23 (ii) an electronic identification num-
24 ber;
25 (iii) a user name;

- 1 (iv) a routing code; or
 2 (v) any associated security code, ac-
 3 cess code, or password or any associated
 4 security questions and answers that could
 5 allow unauthorized access to the account.

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

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

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

18 **SEC. 102. CONCEALMENT OF SECURITY BREACHES INVOLV-**
 19 **ING SENSITIVE PERSONALLY IDENTIFIABLE**
 20 **INFORMATION.**

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

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

4 “(a) Whoever, having knowledge of a security breach
 5 and having the obligation to provide notice of such breach
 6 to individuals under the Personal Data Protection and
 7 Breach Accountability Act of 2011, and having not other-
 8 wise qualified for an exemption from providing notice
 9 under section 212 of the Personal Data Protection and
 10 Breach Accountability Act of 2011, intentionally or will-
 11 fully conceals the fact of such security breach and which
 12 breach causes economic damage or substantial emotional
 13 distress to 1 or more persons, shall be fined under this
 14 title or imprisoned not more than 5 years, or both.

15 “(b) For purposes of subsection (a), the term ‘person’
 16 has the same meaning as in section 1030(c)(12) of title
 17 18, United States Code.

18 “(c) Any person seeking an exemption under section
 19 212(b) of the Personal Data Protection and Breach Ac-
 20 countability Act of 2011 shall be immune from prosecution
 21 under this section if the United States Secret Service does
 22 not indicate, in writing, that such notice be given under
 23 section 212(b)(3) of the Personal Data Protection and
 24 Breach Accountability Act of 2011.”.

25 (b) CONFORMING AND TECHNICAL AMENDMENTS.—
 26 The table of sections for chapter 47 of title 18, United

1 States Code, is amended by adding at the end the fol-
 2 lowing:

“1041. Concealment of security breaches involving personally identifiable infor-
 mation.”.

3 (e) ENFORCEMENT AUTHORITY.—

4 (1) IN GENERAL.—The United States Secret
 5 Service shall have the authority to investigate of-
 6 fenses under this section.

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(e) of title 18, United States Code, is
 13 amended—

14 (1) by inserting “or conspiracy” after “or an
 15 attempt” each place it appears, except for paragraph
 16 (4);

17 (2) in paragraph (2)(B)—

18 (A) in clause (i), by inserting “, or attempt
 19 or conspiracy or conspiracy to commit an of-
 20 fense,” after “the offense”;

21 (B) in clause (ii), by inserting “, or at-
 22 tempt or conspiracy or conspiracy to commit an
 23 offense,” after “the offense”; and

1 (C) in clause (iii), by inserting “(or, in the
2 ease of an attempted offense, would, if com-
3 pleted, have obtained)” after “information ob-
4 tained”; and

5 (3) in paragraph (4)—

6 (A) in subparagraph (A)—

7 (i) by striking clause (ii);

8 (ii) by striking “in the ease of—” and
9 all that follows through “an offense under
10 subsection (a)(5)(B)” and inserting “in the
11 ease of an offense, or an attempt or con-
12 spiracy to commit an offense, under sub-
13 section (a)(5)(B)”;

14 (iii) by inserting “or conspiracy” after
15 “if the offense”;

16 (iv) by redesignating subclauses (I)
17 through (VI) as clauses (i) through (vi),
18 respectively, and adjusting the margin ac-
19 cordingly; and

20 (v) in clause (vi), as so redesignated,
21 by striking “; or” and inserting a semi-
22 colon;

23 (B) in subparagraph (B)—

24 (i) by striking clause (ii);

1 (ii) by striking “in the case of—” and
2 all that follows through “an offense under
3 subsection (a)(5)(A)” and inserting “in the
4 case of an offense, or an attempt or con-
5 spiracy to commit an offense, under sub-
6 section (a)(5)(A)”;

7 (iii) by inserting “or conspiracy” after
8 “if the offense”; and

9 (iv) by striking “; or” and inserting a
10 semicolon;

11 (C) in subparagraph (C)—

12 (i) by striking clause (ii);

13 (ii) by striking “in the case of—” and
14 all that follows through “an offense or an
15 attempt to commit an offense” and insert-
16 ing “in the case of an offense, or an at-
17 tempt or conspiracy to commit an of-
18 fense,”; and

19 (iii) by striking “; or” and inserting a
20 semicolon;

21 (D) in subparagraph (D)—

22 (i) by striking clause (ii);

23 (ii) by striking “in the case of—” and
24 all that follows through “an offense or an
25 attempt to commit an offense” and insert-

1 ing “in the case of an offense, or an at-
 2 tempt or conspiracy to commit an of-
 3 fense,”; and

4 (iii) by striking “; or” and inserting a
 5 semicolon;

6 (E) in subparagraph (E), by inserting “or
 7 conspires” after “offender attempts”;

8 (F) in subparagraph (F), by inserting “or
 9 conspires” after “offender attempts”; and

10 (G) in subparagraph (G)(ii), by inserting
 11 “or conspiracy” after “an attempt”.

12 **SEC. 104. FALSE NOTIFICATION.**

13 (a) **IN GENERAL.**—It shall be unlawful for an indi-
 14 vidual to send a notification of a breach of security that
 15 is false or intentionally misleading in order to obtain sen-
 16 sitive personally identifiable information in an effort to de-
 17 fraud an individual.

18 (b) **PENALTY.**—Any person that violates subsection
 19 (a) shall be fined not more than \$1,000,000, imprisoned
 20 not more than 5 years, or both.

21 (c) **RULE OF CONSTRUCTION.**—For purposes of this
 22 section, any single action or conduct that violates sub-
 23 section (a) with respect to multiple protected computers
 24 shall be construed to be a single violation.

1 **SEC. 105. UNAUTHORIZED INSTALLATION OF PERSONAL IN-**
2 **FORMATION COLLECTION FEATURES ON A**
3 **USER'S COMPUTER.**

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

7 (b) IN GENERAL.—It shall be unlawful for a person
8 that is not an authorized user of a protected computer
9 to cause the installation on the protected computer of soft-
10 ware that collects sensitive personally identifiable informa-
11 tion from an authorized user, unless the person—

12 (1) provides a clear and conspicuous disclosure
13 of such collection; and

14 (2) obtains the consent of an authorized user of
15 the protected computer prior to any collection of
16 sensitive personally identifiable information.

17 (c) COLLECTION AND USE OF PERSONAL INFORMA-
18 TION IN WEB SEARCHES.—It shall be unlawful for an
19 Internet service provider or proxy server to knowingly or
20 intentionally—

21 (1) bypass the display of search engine results
22 and redirect web searches or queries entered by an
23 authorized user of a protected computer directly to
24 a commercial website, counterfeit web page, or tar-
25 geted advertisement and derive an economic benefit
26 from such activity; or

1 (2) monitor, manipulate, aggregate, and market
 2 the data collected in the process of intercepting a
 3 web search or query entered by an authorized user
 4 of a protected computer and derive an economic ben-
 5 efit from such activity.

6 (d) OTHER COLLECTION OF PERSONAL INFORMA-
 7 TION.—

8 (1) IN GENERAL.—It shall be unlawful for a
 9 person who is not an authorized user of a protected
 10 computer to cause the installation on the protected
 11 computer of software that engages in any of the col-
 12 lection practices described in paragraph (2), unless
 13 the person—

14 (A) provides a clear and conspicuous dis-
 15 closure of such collection; and

16 (B) obtains the consent of an authorized
 17 user of the protected computer prior to any
 18 such collection of information.

19 (2) COLLECTION PRACTICES DESCRIBED.—The
 20 collection practices described in this paragraph
 21 are—

22 (A) the use of a keystroke-logging function
 23 that records all or substantially all keystrokes
 24 made by an owner or operator of a computer

1 and transfers that information from the com-
2 puter to another person;

3 ~~(B)~~ the collection of data in a manner
4 that—

5 (i) correlates sensitive personally iden-
6 tifiable information with a history of—

7 (I) all, or substantially all, of the
8 websites visited by an owner or oper-
9 ator, other than websites operated by
10 the person providing such software; or

11 (II) all, or substantially all, of
12 the web searches conducted by an
13 owner or operator other than search
14 data collected by a search engine; and

15 (ii) uses the information described in
16 clause (i) to deliver advertising to, or dis-
17 play advertising on, the computer; and

18 ~~(C)~~ the extracting from the hard drive or
19 other storage medium of the computer—

20 (i) the substantive contents of files,
21 data, software, or other information know-
22 ingly saved or installed by the authorized
23 user of a protected computer; or

24 (ii) the substantive contents of com-
25 munications sent by an authorized user of

1 a protected computer to any other com-
2 puter.

3 (e) EXCEPTION.—This section shall not restrict a
4 person from causing the installation of software that col-
5 lects information for the provider of an online service or
6 website knowingly used or subscribed to by an authorized
7 user if the information collected is used only to affect the
8 experience of the user while using that online service or
9 website.

10 (f) UNINSTALL FUNCTIONALITY.—

11 (1) IN GENERAL.—Software that performs any
12 function described in subsection (b) or (c) shall have
13 the capability to subsequently be uninstalled or dis-
14 abled by an authorized user through a program re-
15 moval function that is usual and customary with the
16 operating system of the computer or otherwise as
17 clearly and conspicuously disclosed to the user.

18 (2) AUTHORITY TO UNINSTALL.—Software that
19 enables an authorized user of a protected computer,
20 such as a parent, employer, or system administrator,
21 to choose to prevent another user of the same com-
22 puter from uninstalling or disabling the software
23 shall not be considered to prevent reasonable efforts
24 to uninstall or disable the software within the mean-
25 ing of paragraph (1) if not less than 1 authorized

1 user retains the ability to uninstall or disable the
2 software.

3 ~~(g) LIMITATIONS ON LIABILITY.—~~

4 ~~(1) IN GENERAL.—~~The restrictions imposed
5 under this section do not apply to any monitoring of,
6 or interaction with, a subscriber's Internet or other
7 network connection or service, or a protected com-
8 puter, by or at the direction of a telecommunications
9 carrier, cable operator, computer hardware or soft-
10 ware provider, financial institution or provider of in-
11 formation services or interactive computer service
12 for—

13 ~~(A) network or computer security pur-~~
14 ~~poses;~~

15 ~~(B) diagnostics;~~

16 ~~(C) technical support;~~

17 ~~(D) repair;~~

18 ~~(E) network management;~~

19 ~~(F) authorized updates of software or sys-~~
20 ~~tem firmware;~~

21 ~~(G) authorized remote system manage-~~
22 ~~ment;~~

23 ~~(H) authorized provision of protection for~~
24 ~~users of the computer from objectionable con-~~
25 ~~tent;~~

1 (I) authorized scanning for computer soft-
2 ware used in violation of this section for re-
3 moval by an authorized user; or

4 (J) detection or prevention of the unau-
5 thorized use of software fraudulent or other ille-
6 gal activities.

7 (2) MANUFACTURER'S LIABILITY FOR THIRD-
8 PARTY SOFTWARE.—A manufacturer or retailer of a
9 computer shall not be liable under any provision of
10 this section for causing the installation on the com-
11 puter, prior to the first retail sale and delivery of the
12 computer, of third-party branded software, unless
13 the manufacturer or retailer knowingly allows the in-
14 stallation of such third-party branded software and
15 derives a benefit from the operation of such soft-
16 ware.

17 (3) EXCEPTION FOR AUTHORIZED INVESTIGA-
18 TIVE AGENCIES.—Nothing in this section prohibits
19 any lawfully authorized criminal investigation or au-
20 thorized investigative, protective, or intelligence ac-
21 tivities that are carried out by or on behalf of any
22 element of the intelligence community and conducted
23 in accordance with the United States laws, authori-
24 ties, and regulations governing such intelligence ac-
25 tivities, of a law enforcement agency of the United

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

3 (h) ENFORCEMENT BY THE ATTORNEY GENERAL.—

4 (1) LIABILITY AND PENALTY FOR VIOLA-
5 TIONS.—Any person who engages in an activity in
6 violation of this section shall be fined not more than
7 \$500,000, imprisoned not more than 5 years, or
8 both.

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

11 (A) IN GENERAL.—Any person who en-
12 gages in a pattern or practice of activity that
13 violates the provisions of this section shall be
14 fined not more than \$1,000,000, imprisoned not
15 more than 5 years, or both.

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

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

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

- 1 (B) any history of prior such conduct;
- 2 (C) the ability of the defendant to pay any
- 3 fine imposed;
- 4 (D) the effect on the ability of the defend-
- 5 ant to continue to do business; and
- 6 (E) such other matters as justice may re-
- 7 quire.

8 **TITLE II—PRIVACY AND SECU-**

9 **RITY OF PERSONALLY IDEN-**

10 **TIFIABLE INFORMATION**

11 **Subtitle A—A Data Privacy and**

12 **Security Program**

13 **SEC. 201. PURPOSE AND APPLICABILITY OF DATA PRIVACY**

14 **AND SECURITY PROGRAM.**

15 (a) **PURPOSE.**—The purpose of this subtitle is to en-

16 sure standards for developing and implementing adminis-

17 trative, technical, and physical safeguards to protect the

18 security of sensitive personally identifiable information.

19 (b) **IN GENERAL.**—A business entity engaging in

20 interstate commerce that involves collecting, accessing,

21 transmitting, using, storing, or disposing of sensitive per-

22 sonally identifiable information in electronic or digital

23 form on 10,000 or more United States persons is subject

24 to the requirements for a data privacy and security pro-

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

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

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

7 (A) subject to the data security require-
 8 ments and implementing regulations under the
 9 Gramm-Leach-Bliley Act (15 U.S.C. 6801 et
 10 seq.); and

11 (B) subject to—

12 (i) examinations for compliance with
 13 the requirements of this Act by a Federal
 14 Functional Regulator or State Insurance
 15 Authority (as those terms are defined in
 16 section 509 of the Gramm-Leach-Bliley
 17 Act (15 U.S.C. 6809)); or

18 (ii) compliance with part 314 of title
 19 16, Code of Federal Regulations.

20 (2) HIPAA REGULATED ENTITIES.—

21 (A) COVERED ENTITIES.—Covered entities
 22 subject to the Health Insurance Portability and
 23 Accountability Act of 1996 (42 U.S.C. 1301 et
 24 seq.); including the data security requirements
 25 and implementing regulations of that Act.

1 (B) BUSINESS ENTITIES.—A business enti-
2 ty shall be deemed in compliance with this Act
3 if the business entity—

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

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

20 (3) PUBLIC RECORDS.—Public records not oth-
21 erwise subject to a confidentiality or nondisclosure
22 requirement, or information obtained from a news
23 report or periodical.

24 (d) RULE OF CONSTRUCTION.—Nothing in this sub-
25 title shall be construed to modify, limit, or supersede the

1 operation of the provisions of the Gramm-Leach-Bliley Act
2 (15 U.S.C. 6801 et seq.); or its implementing regulations,
3 including such regulations adopted or enforced by the
4 States.

5 **SEC. 202. REQUIREMENTS FOR A PERSONAL DATA PRIVACY**
6 **AND SECURITY PROGRAM.**

7 (a) **PERSONAL DATA PRIVACY AND SECURITY PRO-**
8 **GRAM.**—A business entity subject to this subtitle shall
9 comply with the following safeguards and any other ad-
10 ministrative, technical, or physical safeguards identified by
11 the Federal Trade Commission in a rulemaking process
12 pursuant to section 553 of title 5, United States Code,
13 for the protection of sensitive personally identifiable infor-
14 mation:

15 (1) **SCOPE.**—A business entity shall implement
16 a comprehensive personal data privacy and security
17 program that includes administrative, technical, and
18 physical safeguards appropriate to the size and com-
19 plexity of the business entity and the nature and
20 scope of its activities.

21 (2) **DESIGN.**—The personal data privacy and
22 security program shall be designed to—

23 (A) ensure the privacy, security, and con-
24 fidentiality of sensitive personally identifiable
25 information;

1 (B) protect against any anticipated
2 vulnerabilities to the privacy, security, or integ-
3 rity of sensitive personally identifiable informa-
4 tion; and

5 (C) protect against unauthorized access or
6 use of sensitive personally identifiable informa-
7 tion that could create a significant risk of harm
8 or fraud to any individual.

9 (3) RISK ASSESSMENT.—A business entity
10 shall—

11 (A) identify reasonably foreseeable internal
12 and external vulnerabilities that could result in
13 unauthorized access, disclosure, use, or alter-
14 ation of sensitive personally identifiable infor-
15 mation or systems containing sensitive person-
16 ally identifiable information;

17 (B) assess the likelihood of and potential
18 damage from unauthorized access, disclosure,
19 use, or alteration of sensitive personally identifi-
20 able information;

21 (C) assess the sufficiency of its policies,
22 technologies, and safeguards in place to control
23 and minimize risks from unauthorized access,
24 disclosure, use, or alteration of sensitive person-
25 ally identifiable information; and

1 (D) assess the vulnerability of sensitive
2 personally identifiable information during de-
3 struction and disposal of such information, in-
4 cluding through the disposal or retirement of
5 hardware.

6 (4) RISK MANAGEMENT AND CONTROL.—Each
7 business entity shall—

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

11 (B) adopt measures commensurate with
12 the sensitivity of the data as well as the size,
13 complexity, and scope of the activities of the
14 business entity that—

15 (i) control access to systems and fa-
16 cilities containing sensitive personally iden-
17 tifiable information, including controls to
18 authenticate and permit access only to au-
19 thorized individuals;

20 (ii) detect, record, and preserve infor-
21 mation relevant to actual and attempted
22 fraudulent, unlawful, or unauthorized ac-
23 cess, disclosure, use, or alteration of sen-
24 sitive personally identifiable information;

1 including by employees and other individ-
2 uals otherwise authorized to have access;

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

16 (iv) ensure that sensitive personally
17 identifiable information is properly de-
18 stroyed and disposed of, including during
19 the destruction of computers, diskettes,
20 and other electronic media that contain
21 sensitive personally identifiable informa-
22 tion;

23 (v) trace access to records containing
24 sensitive personally identifiable information
25 so that the business entity can determine

1 who accessed or acquired such sensitive
2 personally identifiable information per-
3 taining to specific individuals;

4 (vi) ensure that no third party or cus-
5 tomer of the business entity is authorized
6 to access or acquire sensitive personally
7 identifiable information without the busi-
8 ness entity first performing sufficient due
9 diligence to ascertain, with reasonable cer-
10 tainty, that such information is being
11 sought for a valid legal purpose; and

12 (vii) minimize the amount of personal
13 information maintained by the business en-
14 tity, providing for the retention of such
15 personal information only as reasonably
16 needed for the business purposes of the
17 business entity or as necessary to comply
18 with any other provision of law.

19 (b) TRAINING.—Each business entity subject to this
20 subtitle shall take steps to ensure employee training and
21 supervision for implementation of the data security pro-
22 gram of the business entity.

23 (c) VULNERABILITY TESTING.—

24 (1) IN GENERAL.—Each business entity subject
25 to this subtitle shall take steps to ensure regular

1 testing of key controls, systems, and procedures of
2 the personal data privacy and 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 business enti-
8 ty under subsection (a)(3).

9 (d) RELATIONSHIP TO SERVICE PROVIDERS.—In the
10 event a business entity subject to this subtitle engages
11 service providers not subject to this subtitle, such business
12 entity shall—

13 (1) exercise appropriate due diligence in select-
14 ing those service providers for responsibilities related
15 to sensitive personally identifiable information, and
16 take reasonable steps to select and retain service
17 providers that are capable of maintaining appro-
18 priate safeguards for the security, privacy, and in-
19 tegrity of the sensitive personally identifiable infor-
20 mation at issue; and

21 (2) require those service providers by contract
22 to implement and maintain appropriate measures de-
23 signed to meet the objectives and requirements gov-
24 erning entities subject to section 201, this section,
25 and subtitle B.

1 (e) PERIODIC ASSESSMENT AND PERSONAL DATA
2 PRIVACY AND SECURITY MODERNIZATION.—Each busi-
3 ness entity subject to this subtitle shall on a regular basis
4 monitor, evaluate, and adjust, as appropriate its data pri-
5 vacy and security program in light of any relevant changes
6 in—

- 7 (1) technology;
- 8 (2) the sensitivity of personally identifiable in-
9 formation;
- 10 (3) internal or external threats to personally
11 identifiable information; and
- 12 (4) the changing business arrangements of the
13 business entity, such as—
- 14 (A) mergers and acquisitions;
- 15 (B) alliances and joint ventures;
- 16 (C) outsourcing arrangements;
- 17 (D) bankruptcy; and
- 18 (E) changes to sensitive personally identifi-
19 able information systems.

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

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

2 (a) **CIVIL PENALTIES.**—

3 (1) **IN GENERAL.**—The Attorney General may
4 bring a civil action in the appropriate United States
5 district court against any business entity that en-
6 gages in conduct constituting a violation of this sub-
7 title and, upon proof of such conduct by a prepon-
8 derance of the evidence, such business entity shall be
9 subject to a civil penalty of not more than \$5,000
10 per violation per day while such a violation exists,
11 with a maximum of \$20,000,000 per violation, un-
12 less such conduct is found to be willful or inten-
13 tional.

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

19 (3) **CONSIDERATIONS.**—In determining the
20 amount of a civil penalty under this subsection, the
21 court shall take into account—

22 (A) the degree of culpability of the busi-
23 ness entity;

24 (B) any prior violations of this subtitle by
25 the business entity;

1 (C) the ability of the business entity to pay
2 a civil penalty;

3 (D) the effect on the ability of the business
4 entity to continue to do business;

5 (E) the number of individuals whose per-
6 sonally identifiable information was com-
7 promised by the breach;

8 (F) the relative cost of compliance with
9 this subtitle; and

10 (G) such other matters as justice may re-
11 quire.

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

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

19 (A) enjoining such act or practice; or

20 (B) enforcing compliance with this subtitle.

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

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

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

6 (a) CIVIL ACTIONS.—

7 (1) IN GENERAL.—In any case in which the at-
 8 torney general of a State or any State or local law
 9 enforcement agency authorized by the State attorney
 10 general or by State statute to prosecute violations of
 11 consumer protection law, has reason to believe that
 12 an interest of the residents of that State has been
 13 or is threatened or adversely affected by the acts or
 14 practices of a business entity that violate this sub-
 15 title, the State may bring a civil action on behalf of
 16 the residents of that State in a district court of the
 17 United States of appropriate jurisdiction, or any
 18 other court of competent jurisdiction, to—

19 (A) enjoin that act or practice;

20 (B) enforce compliance with this subtitle;

21 or

22 (C) obtain civil penalties of not more than
 23 \$5,000 per violation per day while such viola-
 24 tions persist, up to a maximum of \$20,000,000
 25 per violation.

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

4 (A) the degree of culpability of the busi-
5 ness entity;

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

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

10 (D) the effect on the ability of the business
11 entity to continue to do business;

12 (E) the number of individuals whose per-
13 sonally identifiable information was com-
14 promised by the breach;

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

17 (G) such other matters as justice may re-
18 quire.

19 (3) NOTICE.—

20 (A) IN GENERAL.—Before filing an action
21 under this subsection, the attorney general of
22 the State involved shall provide to the Attorney
23 General—

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

1 (ii) a copy of the complaint for that
2 action.

3 ~~(B) EXEMPTION.—~~

4 (i) ~~IN GENERAL.—~~Subparagraph (A)
5 shall not apply with respect to the filing of
6 an action by an attorney general of a State
7 under this subsection, if the attorney gen-
8 eral of a State determines that it is not
9 feasible to provide the notice described in
10 this subparagraph before the filing of the
11 action.

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

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

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

24 ~~(2)~~ initiate an action in the appropriate United
25 States district court under section 217 and move to

1 consolidate all pending actions, including State ac-
2 tions, in such court;

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

5 ~~(4) file petitions for appeal.~~

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

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

20 ~~(1) conduct investigations;~~

21 ~~(2) administer oaths or affirmations; or~~

22 ~~(3) compel the attendance of witnesses or the~~
23 ~~production of documentary and other evidence.~~

24 ~~(e) VENUE; SERVICE OF PROCESS.—~~

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

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

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

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

12 (A) is an inhabitant; or

13 (B) may be found.

14 **SEC. 205. SUPPLEMENTAL ENFORCEMENT BY INDIVIDUALS.**

15 (a) IN GENERAL.—Any person aggrieved by a viola-
16 tion of the provisions of this subtitle by a business entity
17 may bring a civil action in a court of appropriate jurisdic-
18 tion to recover for personal injuries sustained as a result
19 of the violation.

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

25 (c) REMEDIES IN A CITIZEN SUIT.—

1 (1) DAMAGES.—Any individual harmed by a
2 failure of a business entity to comply with the provi-
3 sions of this subtitle, shall be able to collect damages
4 of not more than \$10,000 per violation per day while
5 such violations persist, up to a maximum of
6 \$20,000,000 per violation.

7 (2) PUNITIVE DAMAGES.—A business entity
8 may be liable for punitive damages if the business
9 entity intentionally or willfully violates the provisions
10 of this subtitle.

11 (3) EQUITABLE RELIEF.—A business entity
12 that violates the provisions of this subtitle may be
13 enjoined to comply with the provisions of those sec-
14 tions.

15 (d) OTHER RIGHTS AND REMEDIES.—The rights and
16 remedies available under this subsection are cumulative
17 and shall not affect any other rights and remedies avail-
18 able under law.

19 (e) ACCESS TO JUSTICE.—The rights and remedies
20 afforded by this section shall not be abridged or precluded
21 by any predispute arbitration agreement, and any claims
22 under this section that arise from the same security
23 breach are presumed to meet the commonality require-
24 ment under rule 23(a)(2) of the Federal Rules of Civil
25 Procedure.

1 **Subtitle B—Security Breach**
2 **Notification**

3 **SEC. 211. NOTICE TO INDIVIDUALS.**

4 (a) **IN GENERAL.**—Any agency, or business entity en-
5 gaged in interstate commerce, that uses, accesses, trans-
6 mits, stores, disposes of or collects sensitive personally
7 identifiable information that experiences a security breach
8 of such information, shall, following the discovery of such
9 security breach of such information, notify any resident
10 of the United States whose sensitive personally identifiable
11 information has been, or is reasonably believed to have
12 been, accessed, or acquired.

13 (b) **OBLIGATION OF OWNER OR LICENSEE.**—

14 (1) **NOTICE TO OWNER OR LICENSEE.**—Any
15 agency, or business entity engaged in interstate com-
16 merce, that uses, accesses, transmits, stores, dis-
17 poses of, or collects sensitive personally identifiable
18 information that the agency or business entity does
19 not own or license shall notify the owner or licensee
20 of the information following the discovery of a secu-
21 rity breach involving such information.

22 (2) **NOTICE BY OWNER, LICENSEE OR OTHER**
23 **DESIGNATED THIRD PARTY.**—Nothing in this sub-
24 title shall prevent or abrogate an agreement between
25 an agency or business entity required to give notice

1 under this section and a designated third party, in-
2 cluding an owner or licensee of the sensitive person-
3 ally identifiable information subject to the security
4 breach, to provide the notifications required under
5 subsection (a).

6 ~~(3) BUSINESS ENTITY RELIEVED FROM GIVING~~
7 ~~NOTICE.~~—A business entity obligated to give notice
8 under subsection (a) shall be relieved of such obliga-
9 tion if an owner or licensee of the sensitive person-
10 ally identifiable information subject to the security
11 breach, or other designated third party, provides
12 such notification.

13 ~~(c) TIMELINESS OF NOTIFICATION.~~—

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

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

24 ~~(3) BURDEN OF PRODUCTION.~~—The agency,
25 business entity, owner, or licensee required to pro-

1 vide notice under this subtitle shall, upon the re-
2 quest of the Attorney General or the attorney gen-
3 eral of a State or any State or local law enforcement
4 agency authorized by the attorney general of the
5 State or by State statute to prosecute violations of
6 consumer protection law, provide records or other
7 evidence of the notifications required under this sub-
8 title, including to the extent applicable, the reasons
9 for any delay of notification.

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

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

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 delay was invoked unless a
 6 Federal law enforcement or intelligence agency pro-
 7 vides written notification that further delay is nec-
 8 essary.

9 ~~(3) LAW ENFORCEMENT IMMUNITY.—No cause~~
 10 of action shall lie in any court against any law en-
 11 forcement agency for acts relating to the delay of
 12 notification for law enforcement or intelligence pur-
 13 poses under this subtitle.

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

15 ~~(a) EXEMPTION FOR NATIONAL SECURITY AND LAW~~
 16 ~~ENFORCEMENT.—~~

17 ~~(1) IN GENERAL.—Section 211 shall not apply~~
 18 to an agency or business entity if the agency or busi-
 19 ness entity certifies, in writing, that notification of
 20 the security breach as required by section 211 rea-
 21 sonably could be expected to—

22 ~~(A) cause damage to the national security;~~
 23 or

1 ~~(B)~~ hinder a law enforcement investigation
2 or the ability of the agency to conduct law en-
3 forcement investigations.

4 ~~(2) LIMITS ON CERTIFICATIONS.—~~An agency or
5 business entity may not execute a certification under
6 paragraph ~~(1)~~ to—

7 ~~(A)~~ conceal violations of law, inefficiency,
8 or administrative error;

9 ~~(B)~~ prevent embarrassment to a business
10 entity, organization, or agency;

11 ~~(C)~~ restrain competition; or

12 ~~(D)~~ delay notification under section 211
13 for any other reason, except where the agency
14 or business entity reasonably believes an exemp-
15 tion under paragraph ~~(1)~~ applies.

16 ~~(3) NOTICE.—~~In every case in which an agency
17 or business agency issues a certification under para-
18 graph ~~(1)~~, the certification, accompanied by a de-
19 scription of the factual basis for the certification,
20 shall be immediately provided to the United States
21 Secret Service and the Federal Bureau of Investiga-
22 tion.

23 ~~(4) SECRET SERVICE AND FBI REVIEW OF CER-~~
24 ~~TIFICATIONS.—~~

1 (A) ~~IN GENERAL.~~—The United States Se-
2 cret Service or the Federal Bureau of Investiga-
3 tion may review a certification provided by an
4 agency under paragraph (3), and shall review a
5 certification provided by a business entity under
6 paragraph (3), to determine whether an exemp-
7 tion under paragraph (1) is merited. Such re-
8 view shall be completed not later than 7 busi-
9 ness days after the date of receipt of the certifi-
10 cation, except as provided in paragraph (5)(C).

11 (B) ~~NOTICE.~~—Upon completing a review
12 under subparagraph (A) the United States Se-
13 cret Service or the Federal Bureau of Investiga-
14 tion shall immediately notify the agency or
15 business entity, in writing, of its determination
16 of whether an exemption under paragraph (1)
17 is merited.

18 (C) ~~EXEMPTION.~~—The exemption under
19 paragraph (1) shall not apply if the United
20 States Secret Service or the Federal Bureau of
21 Investigation determines under this paragraph
22 that the exemption is not merited.

23 (5) ~~ADDITIONAL AUTHORITY OF THE SECRET~~
24 SERVICE AND FBI.—

1 (A) ~~IN GENERAL.~~—In determining under
2 paragraph (4) whether an exemption under
3 paragraph (1) is merited, the United States Se-
4 cret Service or the Federal Bureau of Investiga-
5 tion may request additional information from
6 the agency or business entity regarding the
7 basis for the claimed exemption, if such addi-
8 tional information is necessary to determine
9 whether the exemption is merited.

10 (B) ~~REQUIRED COMPLIANCE.~~—Any agency
11 or business entity that receives a request for
12 additional information under subparagraph (A)
13 shall cooperate with any such request.

14 (C) ~~TIMING.~~—If the United States Secret
15 Service or the Federal Bureau of Investigation
16 requests additional information under subpara-
17 graph (A), the United States Secret Service or
18 the Federal Bureau of Investigation shall notify
19 the agency or business entity not later than 7
20 business days after the date of receipt of the
21 additional information whether an exemption
22 under paragraph (1) is merited.

23 (b) ~~SAFE HARBOR.~~—

1 (1) IN GENERAL.—An agency or business entity
2 will be exempt from the notice requirements under
3 section 211, if—

4 (A) a risk assessment conducted by the
5 agency or business entity concludes that there
6 is no significant risk that a security breach has
7 resulted in, or will result in harm to the individ-
8 uals whose sensitive personally identifiable in-
9 formation was subject to the security breach;
10 and

11 (B) the United States Secret Service or the
12 Federal Bureau of Investigation does not indi-
13 cate within 7 business days from the receipt of
14 written notification from an agency or business
15 entity pursuant to subsection (b)(2), that the
16 agency or business entity should not be exempt
17 from the notice requirements of section 211.

18 (2) RISK ASSESSMENT REQUIREMENTS.—

19 (A) CONDUCTING A RISK ASSESSMENT.—
20 Upon discovery of a security breach of an agen-
21 cy or business entity, the agency or business en-
22 tity shall conduct a risk assessment to deter-
23 mine if there is a significant risk that the secu-
24 rity breach resulted in, or will result in, harm
25 to the individuals whose sensitive personally

1 identifiable information was subject to the secu-
2 rity breach.

3 (i) PRESUMPTION OF NO SIGNIFICANT
4 RISK.—It is presumed that there is no sig-
5 nificant risk that the security breach has
6 resulted in, or will result in, harm to the
7 individuals whose sensitive personally iden-
8 tifiable information was subject to the se-
9 curity breach, if such sensitive personally
10 identifiable information has been rendered
11 indecipherable through the use of best
12 practices or methods as described by the
13 Federal Trade Commission, such as redac-
14 tion, access controls, or other such mecha-
15 nisms, which are widely accepted as an ef-
16 fective industry practice, or an effective in-
17 dustry standard, or other such mechanisms
18 establishing a presumption that no signifi-
19 cant risk exists.

20 (ii) PRESUMPTION OF SIGNIFICANT
21 RISK.—It is presumed that there is a sig-
22 nificant risk that the security breach has
23 resulted in, or will result in, harm to indi-
24 viduals whose sensitive personally identifi-
25 able information was subject to the secu-

1 rity breach if the agency or business entity
2 failed to render such sensitive personally
3 identifiable information indecipherable
4 through the use of best practices or meth-
5 ods, such as redaction, access controls, or
6 other such mechanisms which are widely
7 accepted as an effective industry practice
8 or an effective industry standard, or other
9 such mechanisms establishing a presump-
10 tion that a significant risk exists.

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

20 (i) the results of the risk assessment;

21 and

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

24 (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

1 (1) ~~IN GENERAL.~~—A business entity shall be
2 exempt from the notice requirement under section
3 ~~211~~ if the business entity utilizes or participates in
4 a security program that—

5 (A) is designed to block the use of the sen-
6 sitive personally identifiable information to ini-
7 tiate unauthorized financial transactions before
8 they are charged to the account of the indi-
9 vidual; and

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

13 (2) ~~LIMITATION.~~—Paragraph (1) does not
14 apply to a business entity if—

15 (A) the information subject to the security
16 breach includes sensitive personally identifiable
17 information, other than a credit card or credit
18 card security code, of any type of the sensitive
19 personally identifiable information identified in
20 section 3; or

21 (B) the security breach includes both the
22 individual's credit card number and the individ-
23 ual's first and last name.

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

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

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

6 (A) Individual written notification to the
7 last known home mailing address of the indi-
8 vidual in the records of the agency or business
9 entity.

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

17 (2) **TELEPHONE NOTICE.**—Telephone notice to
18 the individual personally.

19 (3) **PUBLIC NOTICE.**—

20 (A) **ELECTRONIC NOTICE.**—Prominent no-
21 tice via all reasonable means of electronic con-
22 tact between the individual and the agency or
23 business entity, including any website,
24 networked devices, or other interface through
25 which the agency or business entity regularly
26 interacts with the consumer, if the number of

1 individuals whose personally identifiable infor-
2 mation was or is reasonably believed to have
3 been accessed or acquired by an unauthorized
4 person exceeds 5,000.

5 (B) MEDIA NOTICE.—Notice to major
6 media outlets serving a State or jurisdiction, if
7 the number of residents of such State whose
8 sensitive personally identifiable information
9 was, or is reasonably believed to have been,
10 accessed or acquired by an unauthorized person
11 exceeds 5,000.

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

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

16 (1) a description of the categories of sensitive
17 personally identifiable information that was, or is
18 reasonably believed to have been, accessed or ac-
19 quired by an unauthorized person, and how the
20 agency or business entity came into possession the
21 sensitive personally identifiable information at issue;

22 (2) a toll-free number—

23 (A) that the individual may use to contact
24 the agency or business entity, or the agent of
25 the agency or business entity; and

1 (B) from which the individual may learn
2 what types of sensitive personally identifiable
3 information the agency or business entity main-
4 tained about that individual;

5 (3) the toll-free contact telephone numbers,
6 websites, and addresses for the major credit report-
7 ing agencies;

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

11 (5) notice that the individual is entitled to re-
12 ceive, at no cost to such individual, consumer credit
13 reports on a quarterly basis for a period of 2 years,
14 credit monitoring or any other service that enables
15 consumers to detect the misuse of sensitive person-
16 ally identifiable information for a period of 2 years,
17 and instructions to the individual on requesting such
18 reports or service from the agency or business enti-
19 ty;

20 (6) notice that the individual is entitled to re-
21 ceive a security freeze and that the agency or busi-
22 ness entity will be liable for any costs associated
23 with the security freeze for 2 years and the nec-
24 essary instructions for requesting a security freeze;
25 and

1 (7) notice that any costs or damages incurred
2 by an individual as a result of a security breach will
3 be paid by the business entity or agency that experi-
4 enced the security breach.

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

8 (1) notification that a security breach has oc-
9 curred and that the individual's sensitive personally
10 identifiable information may have been com-
11 promised;

12 (2) a description of the categories of sensitive
13 personally identifiable information that were, or are
14 reasonably believed to have been, accessed or ac-
15 quired by an unauthorized person;

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

17 (A) that the individual may use to contact
18 the agency or business entity, or the authorized
19 agent of the agency or business entity; and

20 (B) from which the individual may learn
21 what types of sensitive personally identifiable
22 information the agency or business entity main-
23 tained about that individual and remedies avail-
24 able to that individual; and

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

5 (e) PUBLIC NOTICE.—Public notice described in sec-
6 tion 213(3) shall include—

7 (1) electronic notice, which includes—

8 (A) notification that a security breach has
9 occurred and that the individual's sensitive per-
10 sonally identifiable information may have been
11 compromised;

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

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

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

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

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

3 ~~(2)~~ media notice, which includes—

4 (A) a description of the categories of sen-
5 sitive personally identifiable information that
6 was, or is reasonably believed to have been,
7 accessed or acquired by an unauthorized per-
8 son;

9 (B) a toll-free number—

10 (i) that the individual may use to con-
11 tact the agency or business entity, or the
12 authorized agent of the agency or business
13 entity; and

14 (ii) from which the individual may
15 learn what types of sensitive personally
16 identifiable information the agency or busi-
17 ness entity maintained about that indi-
18 vidual and remedies available to that indi-
19 vidual;

20 (C) the toll-free contact telephone num-
21 bers, websites, and addresses for the major
22 credit reporting agencies;

23 (D) the telephone numbers and websites
24 for the relevant Federal agencies that provide

1 information regarding identity theft prevention
2 and protection;

3 ~~(E)~~ notice that the affected individuals are
4 entitled to receive, at no cost to such individ-
5 uals, consumer credit reports on a quarterly
6 basis for a period of 2 years, credit monitoring,
7 or any other service that enables consumers to
8 detect the misuse of sensitive personally identi-
9 fiable information for a period of 2 years;

10 ~~(F)~~ notice that the individual is entitled to
11 receive a security freeze and that the agency or
12 business entity will be liable for any costs asso-
13 ciated with the security freeze for 2 years; and

14 ~~(G)~~ notice that the individual is entitled to
15 receive compensation from the business entity
16 or agency for any costs or damages incurred by
17 the individual resulting from the security
18 breach.

19 ~~(d) ADDITIONAL CONTENT.—~~Notwithstanding sec-
20 tion 221, a State may require that a notice under sub-
21 section (a) shall also include information regarding victim
22 protection assistance provided for by that State.

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

24 ~~(a) CREDIT REPORTS AND CREDIT MONITORING.—~~
25 An agency or business entity required to provide notifica-

1 tion under this subtitle shall, upon request of an individual
 2 whose sensitive personally identifiable information was in-
 3 cluded in the security breach, provide or arrange for the
 4 provision of, to each such individual and at no cost to such
 5 individual—

6 (1) consumer credit reports from not fewer
 7 than 1 of the major credit reporting agencies begin-
 8 ning not later than 60 days following the request of
 9 the individual and continuing on a quarterly basis
 10 for a period of 2 years thereafter; and

11 (2) a credit monitoring or other service that en-
 12 ables consumers to detect the misuse of their per-
 13 sonal information, beginning not later than 60 days
 14 following the request of the individual and con-
 15 tinuing for a period of 2 years.

16 (b) SECURITY FREEZE.—

17 (1) REQUEST.—Any consumer may submit a
 18 written request, by certified mail or such other se-
 19 cure method as authorized by a credit rating agency,
 20 to a credit rating agency to place a security freeze
 21 on the credit report of the consumer.

22 (2) IMPLEMENTATION OF SECURITY FREEZE.—
 23 Upon receipt of a written request under paragraph
 24 (1), a credit rating agency shall—

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

4 (B) not later than 10 business days after
5 placing a security freeze, send a written con-
6 firmation of such security freeze to the con-
7 sumer, which shall provide the consumer with a
8 unique personal identification number or pass-
9 word to be used by the consumer when pro-
10 viding authorization for the release of the credit
11 report of the consumer to a third party or for
12 a specified period of time.

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

18 (4) DISCLOSURE OF CREDIT REPORT TO THIRD
19 PARTY.—

20 (A) IN GENERAL.—If a consumer that has
21 requested a security freeze under this sub-
22 section wishes to authorize the disclosure of the
23 credit report of the consumer to a third party,
24 or for a specified period of time, while such se-

1 security freeze is in effect, the consumer shall
2 contact the credit rating agency and provide—

3 (i) proper identification;

4 (ii) the unique personal identification
5 number or password described in para-
6 graph (2)(B); and

7 (iii) proper information regarding the
8 third party who is to receive the credit re-
9 port or the time period for which the credit
10 report shall be available.

11 (B) REQUIREMENT.—Not later than 3
12 business days after receipt of a request under
13 subparagraph (A), a credit rating agency shall
14 lift the security freeze.

15 (5) PROCEDURES.—

16 (A) IN GENERAL.—A credit rating agency
17 shall develop procedures to receive and process
18 requests from consumers under paragraph (2)
19 of this section.

20 (B) REQUIREMENT.—Procedures developed
21 under subparagraph (A), at a minimum, shall
22 include the ability of a consumer to send such
23 temporary lift or removal request by electronic
24 mail, letter, telephone, or facsimile.

1 (6) REQUESTS BY THIRD PARTY.—If a third
2 party requests access to a credit report of a con-
3 sumer that has been frozen under this subsection
4 and the consumer has not authorized the disclosure
5 of the credit report of the consumer to the third
6 party, the third party may deem such credit applica-
7 tion as incomplete.

8 (7) DETERMINATION BY CREDIT RATING AGEN-
9 CY.—

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

14 (i) the request for a security freeze
15 was made as part of a fraud that the con-
16 sumer participated in, had knowledge of,
17 or that can be demonstrated by cir-
18 cumstantial evidence; or

19 (ii) the consumer credit report was
20 frozen due to a material misrepresentation
21 of fact by the consumer.

22 (B) NOTICE.—If a credit rating agency
23 makes a determination under subparagraph (A)
24 to not implement, or to remove, a security
25 freeze under this subsection, the credit rating

1 agency shall notify the consumer in writing of
2 such determination—

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

7 (ii) in the case of a removal of a secu-
8 rity freeze, prior to removing the freeze on
9 the credit report of the consumer.

10 (8) RULE OF CONSTRUCTION.—Nothing in this
11 section shall be construed to prohibit disclosure of a
12 credit report of a consumer to—

13 (A) a person, or the person's subsidiary,
14 affiliate, agent or assignee with which the con-
15 sumer has or, prior to assignment, had an ac-
16 count, contract or debtor-creditor relationship
17 for the purpose of reviewing the account or col-
18 lecting the financial obligation owing for the ac-
19 count, contract or debt;

20 (B) a subsidiary, affiliate, agent, assignee
21 or prospective assignee of a person to whom ac-
22 cess has been granted under paragraph (4) for
23 the purpose of facilitating the extension of cred-
24 it or other permissible use;

1 (C) any person acting pursuant to a court
2 order, warrant or subpoena;

3 (D) any person for the purpose of using
4 such credit information to prescreen as provided
5 by the Fair Credit Reporting Act (15 U.S.C.
6 ~~1681~~ et seq.);

7 (E) any person for the sole purpose of pro-
8 viding a credit file monitoring subscription serv-
9 ice to which the consumer has subscribed;

10 (F) a credit rating agency for the sole pur-
11 pose of providing a consumer with a copy of the
12 credit report of the consumer upon the request
13 of the consumer; or

14 (G) a Federal, State or local governmental
15 entity, including a law enforcement agency, or
16 court, or their agents or assignees pursuant to
17 their statutory or regulatory duties. For pur-
18 poses of this subsection, “reviewing the ac-
19 count” includes activities related to account
20 maintenance, monitoring, credit line increases
21 and account upgrades and enhancements; and

22 (H) any person for the sole purpose of pro-
23 viding a remedy requested by an individual
24 under this section.

1 (9) ~~EXCEPTIONS.~~—The following persons shall
2 not be required to place a security freeze under this
3 subsection, but shall be subject to any security
4 freeze placed on a credit report by another credit
5 rating agency:

6 ~~(A)~~ A check services or fraud prevention
7 services company that reports on incidents of
8 fraud or issues authorizations for the purpose
9 of approving or processing negotiable instru-
10 ments, electronic fund transfers or similar
11 methods of payment.

12 ~~(B)~~ A deposit account information service
13 company that issues reports regarding account
14 closures due to fraud, substantial overdrafts,
15 automated teller machine abuse, or similar in-
16 formation regarding a consumer to inquiring
17 banks or other financial institutions for use
18 only in reviewing a consumer request for a de-
19 posit account at the inquiring bank or financial
20 institution.

21 ~~(C)~~ A credit rating agency that—

22 (i) acts only to resell credit informa-
23 tion by assembling and merging informa-
24 tion contained in a database of 1 or more
25 credit reporting agencies; and

1 (ii) does not maintain a permanent
2 database of credit information from which
3 new credit reports are produced.

4 (10) FEES.—

5 (A) IN GENERAL.—A credit rating agency
6 may charge reasonable fees for each security
7 freeze, removal of such freeze or temporary lift
8 of such freeze for a period of time, and a tem-
9 porary lift of such freeze for a specific party.

10 (B) REQUIREMENT.—Any fees charged
11 under subparagraph (A) shall be borne by the
12 agency or business entity providing notice under
13 section 214 for 2 years following the establish-
14 ment of the security freeze under this sub-
15 section.

16 (e) COSTS RESULTING FROM A SECURITY
17 BREACH.—

18 (1) IN GENERAL.—A business entity or agency
19 that experiences a security breach and is required to
20 provide notice under this subtitle shall pay, upon re-
21 quest, to any individual whose sensitive personally
22 identifiable information has been, or is reasonably
23 believed to have been, accessed or acquired as a re-
24 sult of such security breach, any costs or damages
25 incurred by the individual as a result of such secu-

1 rity breach, including costs associated with identity
2 theft suffered as a result of such security breach.

3 ~~(2) COMPLIANCE.~~—A business entity or agency
4 shall be deemed in compliance with this subsection
5 if the business entity or agency—

6 ~~(A)~~ provides insurance to any individual
7 whose sensitive personally identifiable informa-
8 tion has been, or is reasonably believed to have
9 been, accessed or acquired as a result of a secu-
10 rity breach and such insurance is sufficient to
11 compensate the consumer for not less than
12 \$25,000 of costs or damages; or

13 ~~(B)~~ pays, without unreasonable delay, any
14 actual costs or damages incurred by an indi-
15 vidual as a result of the security breach.

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

17 If an agency or business entity is required to provide
18 notification to more than 5,000 individuals under section
19 211(a), the agency or business entity shall also notify all
20 consumer reporting agencies that compile and maintain
21 files on consumers on a nationwide basis (as defined in
22 section 603(p) of the Fair Credit Reporting Act (15
23 U.S.C. 1681a(p)) of the timing and distribution of the no-
24 tices. Such notice shall be given to the consumer credit
25 reporting agencies without unreasonable delay and, if it

1 will not delay notice to the affected individuals, prior to
2 the distribution of notices to the affected individuals.

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

4 (a) SECRET SERVICE AND FBI.—Any business entity
5 or agency shall notify the United States Secret Service
6 and the Federal Bureau of Investigation of the fact that
7 a security breach has occurred if—

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

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

17 (3) the security breach involves databases
18 owned by the Federal Government; or

19 (4) the security breach involves primarily sen-
20 sitive personally identifiable information of individ-
21 uals known to the agency or business entity to be
22 employees and contractors of the Federal Govern-
23 ment involved in national security or law enforce-
24 ment.

1 (b) FTC REVIEW OF THRESHOLDS.—The Federal
2 Trade Commission may alter the circumstances under
3 which notification is required under subsection (a) in a
4 matter consistent with the public interest.

5 (c) NOTICE TO OTHER LAW ENFORCEMENT AGEN-
6 CIES.—The United States Secret Service and the Federal
7 Bureau of Investigation shall be responsible for noti-
8 fying—

9 (1) the United States Postal Inspection Service,
10 if the security breach involves mail fraud;

11 (2) the attorney general of each State affected
12 by the security breach; and

13 (3) the Federal Trade Commission, if the secu-
14 rity breach involves consumer reporting agencies
15 subject to the Fair Credit Reporting Act (15 U.S.C.
16 1681 et seq.); or anticompetitive conduct.

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

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

22 (2) Notice under section 211 shall be delivered
23 to individuals not later than 48 hours after the Fed-
24 eral Bureau of Investigation or the Secret Service

1 receives notice of a security breach from an agency
2 or business entity.

3 **SEC. 218. FEDERAL ENFORCEMENT.**

4 (a) CIVIL ACTIONS BY THE ATTORNEY GENERAL.—

5 (1) IN GENERAL.—The Attorney General may
6 bring a civil action in the appropriate United States
7 district court against any business entity that en-
8 gages in conduct constituting a violation of this sub-
9 title and, upon proof of such conduct by a prepon-
10 derance of the evidence, such business entity shall be
11 subject to a civil penalty of not more than \$500 per
12 day per individual whose sensitive personally identi-
13 fiable information was, or is reasonably believed to
14 have been, accessed or acquired by an unauthorized
15 person, up to a maximum of \$20,000,000 per viola-
16 tion, unless such conduct is found to be willful or in-
17 tentional.

18 (2) PRESUMPTION.—A violation of section
19 212(a)(2) shall be presumed to be willful or inten-
20 tional conduct.

21 (b) CONSIDERATIONS.—In determining the amount
22 of a civil penalty under this subsection, the court shall
23 take into account—

24 (1) the degree of culpability of the business en-
25 tity;

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

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

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

7 (5) the number of individuals whose personally
8 identifiable information was compromised by the
9 breach;

10 (6) the relative cost of compliance with this
11 subtitle; and

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

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

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

20 (A) enjoining such act or practice; or

21 (B) enforcing compliance with this subtitle.

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

1 (d) 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 (e) FRAUD ALERT.—Section 605A(b)(1) of the Fair
 6 Credit Reporting Act (~~15 U.S.C. 1681e-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. 219. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

12 (a) IN GENERAL.—

13 (1) CIVIL ACTIONS.—

14 (A) IN GENERAL.—In any case in which
 15 the attorney general of a State or any State or
 16 local law enforcement agency authorized by the
 17 State attorney general or by State statute to
 18 prosecute violations of consumer protection law,
 19 has reason to believe that an interest of the
 20 residents of that State has been or is threat-
 21 ened or adversely affected by the engagement of
 22 a business entity in a practice that is prohibited
 23 under this subtitle, the State or the State or
 24 local law enforcement agency on behalf of the
 25 residents of the agency’s jurisdiction, may bring

1 a civil action on behalf of the residents of the
2 State or jurisdiction in a district court of the
3 United States of appropriate jurisdiction or any
4 other court of competent jurisdiction, including
5 a State court, to—

6 (i) enjoin that practice;

7 (ii) enforce compliance with this sub-
8 title; or

9 (iii) obtain civil penalties of not more
10 than \$500 per day per individual whose
11 sensitive personally identifiable information
12 was, or is reasonably believed to have been,
13 accessed or acquired by an unauthorized
14 person, up to a maximum of \$20,000,000
15 per violation, unless such conduct is found
16 to be willful or intentional.

17 (B) PRESUMPTION.—A violation of section
18 212(a)(2) shall be presumed to be willful or in-
19 tentional.

20 (2) CONSIDERATIONS.—In determining the
21 amount of a civil penalty under this subsection, the
22 court shall take into account—

23 (A) the degree of culpability of the busi-
24 ness entity;

1 ~~(B)~~ any prior violations of this subtitle by
2 the business entity;

3 ~~(C)~~ the ability of the business entity to pay
4 a civil penalty;

5 ~~(D)~~ the effect on the ability of the business
6 entity to continue to do business;

7 ~~(E)~~ the number of individuals whose per-
8 sonally identifiable information was com-
9 promised by the breach;

10 ~~(F)~~ the relative cost of compliance with
11 this subtitle; and

12 ~~(G)~~ such other matters as justice may re-
13 quire.

14 ~~(3)~~ NOTICE.—

15 ~~(A)~~ IN GENERAL.—Before filing an action
16 under paragraph (1), the attorney general of
17 the State involved shall provide to the Attorney
18 General of the United States—

19 (i) written notice of the action; and

20 (ii) a copy of the complaint for the ac-
21 tion.

22 ~~(B)~~ EXEMPTION.—

23 (i) IN GENERAL.—Subparagraph (A)
24 shall not apply with respect to the filing of
25 an action by an attorney general of a State

1 under this subtitle, if the State attorney
2 general determines that it is not feasible to
3 provide the notice described in such sub-
4 paragraph before the filing of the action.

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

11 (b) FEDERAL PROCEEDINGS.—Upon receiving notice
12 under subsection (a)(2), the Attorney General shall have
13 the right to—

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

17 (2) initiate an action in the appropriate United
18 States district court under section 217 and move to
19 consolidate all pending actions, including State ac-
20 tions, in such court;

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

23 (4) file petitions for appeal.

24 (c) PENDING PROCEEDINGS.—If the Attorney Gen-
25 eral has instituted a proceeding or action for a violation

1 of this subtitle or any regulations thereunder, no attorney
 2 general of a State may, during the pendency of such pro-
 3 ceeding or action, bring an action under this subtitle
 4 against any defendant named in such criminal proceeding
 5 or civil action for any violation that is alleged in that pro-
 6 ceeding or action.

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

13 (1) conduct investigations;
 14 (2) administer oaths or affirmations; or
 15 (3) compel the attendance of witnesses or the
 16 production of documentary and other evidence.

17 (e) VENUE; SERVICE OF PROCESS.—

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

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

24 (B) another court of competent jurisdic-
 25 tion.

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

4 (A) is an inhabitant; or

5 (B) may be found.

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

7 (a) IN GENERAL.—Any person aggrieved by a viola-
8 tion of the provisions of section 211, 213, 214, 215, or
9 216 by a business entity may bring a civil action in a court
10 of appropriate jurisdiction to recover for personal injuries
11 sustained as a result of the violation.

12 (b) REMEDIES IN A CITIZEN SUIT.—

13 (1) DAMAGES.—Any individual harmed by a
14 failure of a business entity to comply with the provi-
15 sions of section 211, 213, 214, 215, or 216, shall be
16 able to collect damages of not more than \$500 per
17 day per individual whose sensitive personally identi-
18 fiable information was, or is reasonably believed to
19 have been, accessed or acquired by an unauthorized
20 person, up to a maximum of \$20,000,000 per viola-
21 tion.

22 (2) PUNITIVE DAMAGES.—A business entity
23 may be liable for punitive damages if it—

1 (A) intentionally or willfully violates the
2 provisions of section 211, 213, 214, 215, or
3 216; or

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

6 (3) **EQUITABLE RELIEF.**—A business entity
7 that violates the provisions of section 211, 213, 214,
8 215, or 216 may be enjoined to provide required
9 remedies under section 215 by a court of competent
10 jurisdiction.

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

15 (c) **ACCESS TO JUSTICE.**—The rights and remedies
16 afforded by this section shall not be abridged or precluded
17 by any predispute arbitration agreement, and any claims
18 under this section that arise from the same security
19 breach are presumed to meet the commonality require-
20 ment under rule 23(a)(2) of the Federal Rules of Civil
21 Procedure.

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

23 (a) **IN GENERAL.**—The provisions of this subtitle
24 shall supersede any other provision of Federal law or any
25 provision of law of any State relating to notification by

1 a business entity engaged in interstate commerce or an
2 agency of a security breach, except as provided in section
3 214(c).

4 (b) **RULE OF CONSTRUCTION.**—Nothing in this sub-
5 title shall be construed to exempt any entity from liability
6 under common law, including through the operation of or-
7 dinary preemption principles, for damages caused by the
8 failure to notify an individual following a security breach.

9 (c) **PRESUMPTION OF PER SE NEGLIGENCE.**—If a
10 business entity fails to comply with the requirements in
11 section 211, 212, 213, 214, 215, or 216, there shall be
12 a presumption that the entity was per se negligent.

13 **SEC. 222. AUTHORIZATION OF APPROPRIATIONS.**

14 There are authorized to be appropriated such sums
15 as may be necessary to cover the costs incurred by the
16 United States Secret Service to carry out investigations
17 and risk assessments of security breaches as required
18 under this subtitle.

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

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

24 (1) the number and nature of the security
25 breaches described in the notices filed by those busi-

1 ness entities invoking the risk assessment exemption
 2 under section 212(b) and the response of the United
 3 States Secret Service and the Federal Bureau of In-
 4 vestigation to such notices; and

5 (2) the number and nature of security breaches
 6 subject to the national security and law enforcement
 7 exemptions under section 212(a); provided that such
 8 report may not disclose the contents of any risk as-
 9 sessment provided to the United States Secret Serv-
 10 ice and the Federal Bureau of Investigation pursu-
 11 ant to this subtitle.

12 **Subtitle C—Post-Breach Technical** 13 **Information Clearinghouse**

14 **SEC. 230. CLEARINGHOUSE INFORMATION COLLECTION,** 15 **MAINTENANCE, AND ACCESS.**

16 (a) **IN GENERAL.**—The Attorney General shall main-
 17 tain a clearinghouse of technical information concerning
 18 system vulnerabilities identified in the wake of security
 19 breaches, which shall—

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

22 (2) be accessible to certified entities under sub-
 23 section (c).

24 (b) **POST-BREACH TECHNICAL NOTIFICATION.**—In
 25 any instance where an agency or business entity is re-

1 quired to notify the United States Secret Service and the
2 Federal Bureau of Investigation under section 217, the
3 agency or business entity shall also provide the Attorney
4 General with technical information concerning the nature
5 of the security breach, including—

6 (1) technical information regarding any system
7 vulnerabilities of the agency or business entity re-
8 vealed by or identified as a consequence of the secu-
9 rity breach;

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

13 (3) any other technical information concerning
14 the nature of the security breach deemed appro-
15 priate for collection by the Attorney General in fur-
16 therance of this subtitle.

17 (e) ACCESS TO CLEARINGHOUSE.—Any entity cer-
18 tified under subsection (d) may review information main-
19 tained by the technical information clearinghouse for the
20 purpose of preventing security breaches that threaten the
21 security of sensitive personally identifiable information.

22 (d) CERTIFICATION FOR ACCESS.—The Attorney
23 General shall issue and revoke certifications to agencies
24 and business entities wishing to review information main-
25 tained by the technical information clearinghouse and

1 shall establish conditions for obtaining and maintaining
 2 such certifications, including agreement that any informa-
 3 tion obtained directly or derived indirectly from the review
 4 of information maintained by the technical information
 5 clearinghouse—

6 (1) shall only be used to improve the security
 7 and reduce the vulnerability of networks that use
 8 personally identifiable information;

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

11 (3) may not be shared with any third party, in-
 12 cluding other parties certified for access to the infor-
 13 mation clearinghouse, without the express written
 14 consent of the Attorney General.

15 (c) RULEMAKING.—In consultation with the private
 16 sector, appropriate representatives of State and local gov-
 17 ernments, and other appropriate Federal agencies, the At-
 18 torney General shall promulgate any regulations pursuant
 19 to section 552 of title 5, United States Code, necessary
 20 to carry out the provisions of this section.

21 **SEC. 231. PROTECTIONS FOR CLEARINGHOUSE PARTICI-**
 22 **PANTS.**

23 (a) PROTECTION OF PROPRIETARY INFORMATION.—
 24 To the extent feasible, the Attorney General shall ensure
 25 that any technical information disclosed to the Attorney

1 General under this subtitle shall be stored in a format de-
2 signed to protect proprietary business information from
3 inadvertent disclosure.

4 (b) ANONYMOUS DATA RELEASE.—To the extent fea-
5 sible, the Attorney General shall ensure that all informa-
6 tion stored in the technical information clearinghouse and
7 accessed by certified parties is presented in a form that
8 minimizes the potential for such information to be traced
9 to a particular network, company, or security breach inci-
10 dent.

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

13 (1) security and vulnerability information col-
14 lected under this section and provided to the Federal
15 Government, including aggregated analysis and data,
16 shall be exempt from disclosure under section
17 552(b)(3) of title 5, United States Code; and

18 (2) under section 230(e), security and vulner-
19 ability-related information provided to the Federal
20 Government under this section, including aggregated
21 analysis and data, shall be protected from public dis-
22 closure, except that this paragraph—

23 (A) does not prohibit the sharing of such
24 information, as the Attorney General deter-
25 mines to be appropriate, in order to mitigate

1 cybersecurity threats or further the official
2 functions of a government agency; and

3 (B) does not authorized such information
4 to be withheld from a committee of Congress
5 authorized to request the information.

6 (d) PROTECTION OF CLASSIFIED INFORMATION.—

7 Nothing in this subtitle permits the unauthorized disclo-
8 sure of classified information.

9 **SEC. 232. EFFECTIVE DATE.**

10 This subtitle shall take effect on the expiration of the
11 date which is 90 days after the date of enactment of this
12 Act.

13 **TITLE III—ACCESS TO AND USE** 14 **OF COMMERCIAL DATA**

15 **SEC. 301. GENERAL SERVICES ADMINISTRATION REVIEW**
16 **OF CONTRACTS.**

17 (a) IN GENERAL.—In considering contract awards
18 totaling more than \$500,000 and entered into after the
19 date of enactment of this Act with data brokers, the Ad-
20 ministrators of the General Services Administration shall
21 evaluate—

22 (1) the data privacy and security program of a
23 data broker to ensure the privacy and security of
24 data containing personally identifiable information,
25 including whether such program adequately address-

1 es privacy and security threats created by malicious
2 software or code, or the use of peer-to-peer file shar-
3 ing software;

4 (2) the compliance of a data broker with such
5 program;

6 (3) the extent to which the databases and sys-
7 tems containing personally identifiable information
8 of a data broker have been compromised by security
9 breaches; and

10 (4) the response by a data broker to such
11 breaches, including the efforts by such data broker
12 to mitigate the impact of such security breaches.

13 (b) COMPLIANCE SAFE HARBOR.—The data privacy
14 and security program of a data broker shall be deemed
15 sufficient for the purposes of subsection (a), if the data
16 broker complies with or provides protection equal to indus-
17 try standards, as identified by the Federal Trade Commis-
18 sion, that are applicable to the type of personally identifi-
19 able information involved in the ordinary course of busi-
20 ness of such data broker.

21 (c) PENALTIES.—In awarding contracts with data
22 brokers for products or services related to access, use,
23 compilation, distribution, processing, analyzing, or evalu-
24 ating personally identifiable information, the Adminis-
25 trator of the General Services Administration shall—

1 (1) include monetary or other penalties—

2 (A) for failure to comply with subtitles A
3 and B of title III; or

4 (B) if a contractor knows or has reason to
5 know that the personally identifiable informa-
6 tion being provided is inaccurate, and provides
7 such inaccurate information; and

8 (2) require a data broker that engages service
9 providers not subject to subtitle A of title III for re-
10 sponsibilities related to sensitive personally identifi-
11 able information to—

12 (A) exercise appropriate due diligence in
13 selecting those service providers for responsibil-
14 ities related to personally identifiable informa-
15 tion;

16 (B) take reasonable steps to select and re-
17 tain service providers that are capable of main-
18 taining appropriate safeguards for the security,
19 privacy, and integrity of the personally identifi-
20 able information at issue; and

21 (C) require such service providers, by con-
22 tract, to implement and maintain appropriate
23 measures designed to meet the objectives and
24 requirements in title III.

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

5 **SEC. 302. REQUIREMENT TO AUDIT INFORMATION SECU-**
6 **RITY PRACTICES OF CONTRACTORS AND**
7 **THIRD PARTY BUSINESS ENTITIES.**

8 Section 3544(b) of title 44, United States Code, is
9 amended—

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

12 (2) in paragraph (8), by striking the period and
13 inserting “, and”, and

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

15 “(9) procedures for evaluating and auditing the
16 information security practices of contractors or third
17 party business entities supporting the information
18 systems or operations of the agency involving per-
19 sonally identifiable information (as that term is de-
20 fined in section 3 of the Personal Data Protection
21 and Breach Accountability Act of 2011) and ensur-
22 ing remedial action to address any significant defi-
23 ciencies.”.

1 **SEC. 303. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT**
 2 **USE OF COMMERCIAL INFORMATION SERV-**
 3 **ICES CONTAINING PERSONALLY IDENTIFI-**
 4 **ABLE INFORMATION.**

5 (a) **IN GENERAL.**—Section 208(b)(1) of the ~~E-Gov-~~
 6 ~~ernment Act of 2002 (44 U.S.C. 3501 note)~~ is amended—

7 (1) in subparagraph (A)(i), by striking “or”;

8 (2) in subparagraph (A)(ii), by striking the pe-
 9 riod and inserting “; or”; and

10 (3) by inserting after clause (ii) the following:

11 “(iii) purchasing or subscribing for a
 12 fee to personally identifiable information
 13 from a data broker (as such terms are de-
 14 fined in section 3 of the Personal Data
 15 Protection and Breach Accountability Act
 16 of 2011).”.

17 (b) **LIMITATION.**—Notwithstanding any other provi-
 18 sion of law, commencing 1 year after the date of enact-
 19 ment of this Act, no Federal agency may enter into a con-
 20 tract with a data broker to access for a fee any database
 21 consisting primarily of personally identifiable information
 22 concerning United States persons (other than news report-
 23 ing or telephone directories) unless the head of such de-
 24 partment or agency—

25 (1) completes a privacy impact assessment
 26 under section 208 of the ~~E-Government Act of 2002~~

1 (44 U.S.C. 3501 note), which shall subject to the
2 provision in that Act pertaining to sensitive informa-
3 tion, include a description of—

4 (A) such database;

5 (B) the name of the data broker from
6 whom it is obtained; and

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

8 (2) adopts regulations that specify—

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

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

13 (C) any standards used to ensure that the
14 personally identifiable information accessed,
15 analyzed, or used is the minimum necessary to
16 accomplish the intended legitimate purpose of
17 the Federal agency;

18 (D) standards limiting the retention and
19 redisclosure of personally identifiable informa-
20 tion obtained from such databases;

21 (E) procedures ensuring that such data
22 meet standards of accuracy, relevance, com-
23 pleteness, and timeliness;

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

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

8 (H) mechanisms, if any, for the enforce-
9 ment and independent oversight of existing or
10 planned procedures, policies, or guidelines; and

11 (I) an outline of enforcement mechanisms
12 for accountability to protect individuals and the
13 public against unlawful or illegitimate access or
14 use of databases; and

15 (3) incorporates into the contract or other
16 agreement totaling more than \$500,000, provi-
17 sions—

18 (A) providing for penalties—

19 (i) for failure to comply with title III
20 of this Act; or

21 (ii) if the entity knows or has reason
22 to know that the personally identifiable in-
23 formation being provided to the Federal
24 department or agency is inaccurate, and
25 provides such inaccurate information; and

1 ~~(B)~~ requiring a data broker that engages
 2 service providers not subject to subtitle A of
 3 title III for responsibilities related to sensitive
 4 personally identifiable information to—

5 (i) exercise appropriate due diligence
 6 in selecting those service providers for re-
 7 sponsibilities related to personally identifi-
 8 able information;

9 (ii) take reasonable steps to select and
 10 retain service providers that are capable of
 11 maintaining appropriate safeguards for the
 12 security, privacy, and integrity of the per-
 13 sonally identifiable information at issue;
 14 and

15 (iii) require such service providers, by
 16 contract, to implement and maintain ap-
 17 propriate measures designed to meet the
 18 objectives and requirements in title III.

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

23 ~~(d)~~ STUDY OF GOVERNMENT USE.—

24 (1) SCOPE OF STUDY.—Not later than 180
 25 days after the date of enactment of this Act, the

1 Comptroller General of the United States shall con-
2 duct a study and audit and prepare a report on Fed-
3 eral agency actions to address the recommendations
4 in the Government Accountability Office's April
5 2006 report on agency adherence to key privacy
6 principles in using data brokers or commercial data-
7 bases containing personally identifiable information.

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

10 **SEC. 304. FBI REPORT ON REPORTED BREACHES AND COM-**
11 **PLIANCE.**

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

20 (b) REPORT CONTENT.—Such reporting shall in-
21 clude—

22 (1) the total instances of breaches of security in
23 the previous year;

24 (2) the percentage of breaches described in sub-
25 section (a) that occurred at an agency or business

1 entity that did not comply with the personal data
2 privacy and security program under section 202; and
3 ~~(3)~~ recommendations, if any, for modifying or
4 amending this Act to increase its effectiveness.

5 **SEC. 305. DEPARTMENT OF JUSTICE REPORT ON ENFORCE-**
6 **MENT ACTIONS.**

7 (a) IN GENERAL.—Not later than 1 year after the
8 date of enactment of this Act, and each year thereafter,
9 the Attorney General shall submit to Congress a report
10 on the enforcement actions taken in the previous year in
11 cases of violations of any sections of this Act.

12 (b) REPORT CONTENT.—The report required under
13 subsection (a) shall include—

14 (1) statistics on Federal enforcement actions,
15 State attorneys general enforcement actions, and
16 private enforcement actions related to the provisions
17 of this Act; and

18 ~~(2)~~ recommendations, if any, for modifying or
19 amending this Act to increase the effectiveness of
20 such enforcement actions.

21 **SEC. 306. DEPARTMENT OF JUSTICE REPORT ON ENFORCE-**
22 **MENT ACTIONS.**

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

1 “(c) Not later than 1 year after the date of enactment
2 of the Personal Data Protection and Breach Account-
3 ability Act of 2011, and every fiscal year thereafter, the
4 Attorney General shall submit to Congress a report on the
5 efforts of the Federal Government to enforce the Personal
6 Data Protection and Breach Accountability Act of 2011
7 that shall include a description of the best practices for
8 enforcement of such Act.”.

9 **SEC. 307. FBI REPORT ON NOTIFICATION EFFECTIVENESS.**

10 (a) **IN GENERAL.**—Not later than 1 year after the
11 date of enactment of this Act, and each year thereafter,
12 the Federal Bureau of Investigation, in coordination with
13 the Secret Service, shall submit to the Committee on the
14 Judiciary of the Senate and the Committee on the Judici-
15 ary of the House of Representatives a report regarding
16 the effectiveness of post-breach notification practices by
17 agencies and business entities.

18 (b) **REPORT CONTENT.**—The report required under
19 subsection (a) shall include—

20 (1) in each instance of a breach of security, the
21 amount of time between the instance of the breach
22 and the discovery of the breach by the affected busi-
23 ness entity;

24 (2) in each instance of a breach of security, the
25 amount of time between the discovery of the breach

1 by the affected business entity and the notification
2 to the FBI and Secret Service; and

3 ~~(3)~~ in each instance of a breach of security, the
4 amount of time between the discovery of the breach
5 by the affected business entity and the notification
6 to individuals whose sensitive personally identifiable
7 information was compromised.

8 **TITLE IV—COMPLIANCE WITH**
9 **STATUTORY PAY-AS-YOU-GO ACT**

10 **SEC. 401. BUDGET COMPLIANCE.**

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

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

20 (a) *SHORT TITLE.*—This Act may be cited as the “Per-
21 sonal Data Protection and Breach Accountability Act of
22 2011”.

23 (b) *TABLE OF CONTENTS.*—The table of contents of this
24 Act is as follows:

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

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

- Sec. 101. Concealment of security breaches involving sensitive personally identifiable information.*
Sec. 102. Unauthorized manipulation of Internet traffic on a user's computer.

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

Subtitle A—A Data Privacy and Security Program

- Sec. 201. Purpose and applicability of data privacy and security program.*
Sec. 202. Requirements for a personal data privacy and security program.
Sec. 203. Federal enforcement.
Sec. 204. Enforcement by State Attorneys General.
Sec. 205. Supplemental enforcement by individuals.

Subtitle B—Security Breach Notification

- Sec. 211. Notice to individuals.*
Sec. 212. Exemptions from notice to individuals.
Sec. 213. Methods of notice to individuals.
Sec. 214. Content of notice to individuals.
Sec. 215. Remedies for security breach.
Sec. 216. Notice to credit reporting agencies.
Sec. 217. Notice to law enforcement.
Sec. 218. Federal enforcement.
Sec. 219. Enforcement by State attorneys general.
Sec. 220. Supplemental enforcement by individuals.
Sec. 221. Relation to other laws.
Sec. 222. Authorization of appropriations.
Sec. 223. Reporting on risk assessment exemptions.

Subtitle C—Post-Breach Technical Information Clearinghouse

- Sec. 230. Clearinghouse information collection, maintenance, and access.*
Sec. 231. Protections for clearinghouse participants.
Sec. 232. Effective date.

TITLE III—ACCESS TO AND USE OF COMMERCIAL DATA

- Sec. 301. General services administration review of contracts.*
Sec. 302. Requirement to audit information security practices of contractors and third party business entities.
Sec. 303. Privacy impact assessment of government use of commercial information services containing sensitive personally identifiable information.
Sec. 304. FBI report on reported breaches and compliance.
Sec. 305. Department of Justice report on enforcement actions.
Sec. 306. Report on notification effectiveness.

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

- Sec. 401. Budget compliance.*

1 **SEC. 2. FINDINGS.**

2 *Congress finds that—*

3 *(1) databases of personally identifiable informa-*
4 *tion are increasingly prime targets of hackers, iden-*
5 *tity thieves, rogue employees, and other criminals, in-*
6 *cluding organized and sophisticated criminal oper-*
7 *ations;*

8 *(2) identity theft is a serious threat to the Na-*
9 *tion's economic stability, homeland security, the de-*
10 *velopment of e-commerce, and the privacy rights of*
11 *Americans;*

12 *(3) over 9,300,000 individuals were victims of*
13 *identity theft in America last year;*

14 *(4) security breaches are a serious threat to con-*
15 *sumer confidence, homeland security, e-commerce, and*
16 *economic stability;*

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

22 *(6) individuals whose personal information has*
23 *been compromised or who have been victims of iden-*
24 *tity theft should receive the necessary information and*
25 *assistance to mitigate their damages and to restore*

1 *the integrity of their personal information and identi-*
2 *ties;*

3 *(7) data misuse and use of inaccurate data have*
4 *the potential to cause serious or irreparable harm to*
5 *an individual's livelihood, privacy, and liberty and*
6 *undermine efficient and effective business and govern-*
7 *ment operations;*

8 *(8) there is a need to ensure that data brokers*
9 *conduct their operations in a manner that prioritizes*
10 *fairness, transparency, accuracy, and respect for the*
11 *privacy of consumers;*

12 *(9) government access to commercial data can*
13 *potentially improve safety, law enforcement, and na-*
14 *tional security;*

15 *(10) because government use of commercial data*
16 *containing personal information potentially affects*
17 *individual privacy, and law enforcement and na-*
18 *tional security operations, there is a need for Con-*
19 *gress to exercise oversight over government use of com-*
20 *mercial data;*

21 *(11) over 22,960,000 cases of data breaches in-*
22 *volving personally identifiable information were re-*
23 *ported through July of 2011, and in 2009 through*
24 *2010, over 230,900,000 cases of personal data*
25 *breaches were reported;*

1 (12) *facilitating information sharing among*
2 *business entities and across sectors in the event of a*
3 *breach can assist in remediating the breach and pre-*
4 *venting similar breaches in the future;*

5 (13) *because the Federal Government has limited*
6 *resources, consumers themselves play a vital and com-*
7 *plementary role in facilitating prompt notification*
8 *and protecting against future breaches of security;*

9 (14) *in addition to the immediate damages*
10 *caused by security breaches, the lack of basic remedial*
11 *requirements often forces individuals whose sensitive*
12 *personally identifiable information is compromised as*
13 *a result of a security breach to incur the economic*
14 *costs of litigation to seek remedies, and the economic*
15 *costs of fees required in many States to freeze com-*
16 *promised accounts; and*

17 (15) *victims of personal data breaches may suffer*
18 *debilitating emotional and physical effects and be-*
19 *come depressed or anxious, especially in cases of re-*
20 *peated or unresolved instances of data breaches.*

21 **SEC. 3. DEFINITIONS.**

22 (a) *IN GENERAL.*—*In this Act, the following defini-*
23 *tions shall apply:*

1 (1) *AFFILIATE.*—The term “affiliate” means per-
2 sons related by common ownership or by corporate
3 control.

4 (2) *AGENCY.*—The term “agency” has the mean-
5 ing given such term in section 551 of title 5, United
6 States Code.

7 (3) *BUSINESS ENTITY.*—The term “business enti-
8 ty” means any organization, corporation, trust, part-
9 nership, sole proprietorship, unincorporated associa-
10 tion, or venture established to make a profit, or non-
11 profit.

12 (4) *CREDIT RATING AGENCY.*—The term “credit
13 rating agency” has the meaning given such term in
14 section 3(a)(61) of the Securities Exchange Act of
15 1934 (12 U.S.C. 78c(a)(61)).

16 (5) *CREDIT REPORT.*—The term “credit report”
17 means a consumer report, as that term is defined in
18 section 603 of the Fair Credit Reporting Act (15
19 U.S.C. 1681a).

20 (6) *DATA BROKER.*—The term “data broker”
21 means a business entity which for monetary fees or
22 dues regularly engages in the practice of collecting,
23 transmitting, or providing access to sensitive person-
24 ally identifiable information on more than 5,000 in-
25 dividuals who are not the customers or employees of

1 *that business entity or affiliate primarily for the pur-*
2 *poses of providing such information to nonaffiliated*
3 *third parties on an interstate basis.*

4 (7) *DESIGNATED ENTITY.*—*The term “designated*
5 *entity” means the Federal Government entity des-*
6 *ignated under section 217(a).*

7 (8) *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 ac-*
11 *cepted by experts in the field of information se-*
12 *curity that renders such data indecipherable in*
13 *the absence of associated cryptographic keys nec-*
14 *essary to enable decryption of such data; and*

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

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

21 (10) *INTELLIGENCE COMMUNITY.*—*The term “in-*
22 *telligence community” includes the following:*

23 (A) *The Office of the Director of National*
24 *Intelligence.*

25 (B) *The Central Intelligence Agency.*

1 (C) *The National Security Agency.*

2 (D) *The Defense Intelligence Agency.*

3 (E) *The National Geospatial-Intelligence*
4 *Agency.*

5 (F) *The National Reconnaissance Office.*

6 (G) *Other offices within the Department of*
7 *Defense for the collection of specialized national*
8 *intelligence through reconnaissance programs.*

9 (H) *The intelligence elements of the Army,*
10 *the Navy, the Air Force, the Marine Corps, the*
11 *Federal Bureau of Investigation, and the De-*
12 *partment of Energy.*

13 (I) *The Bureau of Intelligence and Research*
14 *of the Department of State.*

15 (J) *The Office of Intelligence and Analysis*
16 *of the Department of the Treasury.*

17 (K) *The elements of the Department of*
18 *Homeland Security concerned with the analysis*
19 *of intelligence information, including the Office*
20 *of Intelligence of the Coast Guard.*

21 (L) *Such other elements of any other de-*
22 *partment or agency as may be designated by the*
23 *President, or designated jointly by the Director*
24 *of National Intelligence and the head of the de-*

1 *partment or agency concerned, as an element of*
2 *the intelligence community.*

3 (11) *PREDISPUTE ARBITRATION AGREEMENT.*—

4 *The term “predispute arbitration agreement” means*
5 *any agreement to arbitrate a dispute that had not yet*
6 *arisen at the time of the making of the agreement.*

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

15 (13) *SECURITY BREACH.*—

16 (A) *IN GENERAL.*—*The term “security*
17 *breach” means compromise of the security, con-*
18 *fidentiality, or integrity of, or the loss of, com-*
19 *puterized data through misrepresentation or ac-*
20 *tions that result in, or that there is a reasonable*
21 *basis to conclude has resulted in—*

22 (i) *the unauthorized acquisition of sen-*
23 *sitive personally identifiable information;*
24 *or*

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

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

7 (i) a good faith acquisition of sensitive
8 personally identifiable information by a
9 business entity or agency, or an employee or
10 agent of a business entity or agency, if the
11 sensitive personally identifiable information
12 is 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 the release of in-
17 formation obtained from a public record; or

18 (iii) any lawfully authorized criminal
19 investigation or authorized investigative,
20 protective, or intelligence activities that are
21 carried out by or on behalf of any element
22 of the intelligence community and con-
23 ducted in accordance with the United States
24 laws, authorities, and regulations governing
25 such intelligence activities.

1 (14) *SECURITY FREEZE.*—*The term “security*
2 *freeze” means a notice, at the request of the consumer*
3 *and subject to exceptions in section 215(b), that pro-*
4 *hibits the consumer reporting agency from releasing*
5 *all or any part of the consumer’s credit report or any*
6 *information derived from it without the express au-*
7 *thorization of the consumer.*

8 (15) *SENSITIVE PERSONALLY IDENTIFIABLE IN-*
9 *FORMATION.*—*The term “sensitive personally identifi-*
10 *able information” means any information or com-*
11 *pileation of information, in electronic or digital form*
12 *that includes the following:*

13 (A) *An individual’s first and last name or*
14 *first initial and last name in combination with*
15 *any 2 of the following data elements:*

16 (i) *Home address.*

17 (ii) *Telephone number of the indi-*
18 *vidual.*

19 (iii) *Mother’s maiden name.*

20 (iv) *Month, day, and year of birth.*

21 (B) *A non-truncated social security number,*
22 *driver’s license number, passport number, or*
23 *alien registration number or other government-*
24 *issued unique identification number.*

1 (C) *Information about an individual's geo-*
2 *graphic location that is in whole or in part gen-*
3 *erated by or derived from that individual's use*
4 *of a wireless communication device or other elec-*
5 *tronic device, excluding telephone and instru-*
6 *ment numbers and network or Internet Protocol*
7 *addresses.*

8 (D) *Unique biometric data such as a finger*
9 *print, voice print, face print, a retina or iris*
10 *image, or any other unique physical representa-*
11 *tion.*

12 (E) *A unique account identifier, including*
13 *a financial account number or credit or debit*
14 *card number, electronic identification number,*
15 *user name, health insurance policy or subscriber*
16 *identification number, or routing code.*

17 (F) *Not less than 2 of the following data ele-*
18 *ments:*

19 (i) *An individual's first and last name*
20 *or first initial and last name.*

21 (ii) *A unique account identifier, in-*
22 *cluding a financial account number or cred-*
23 *it or debit card number, electronic identi-*
24 *fication number, user name, or routing*
25 *code.*

1 (iii) Any security code, access code, or
2 password, or source code that could be used
3 to generate such codes and passwords.

4 (iv) Information regarding an individ-
5 ual's medical history, mental or physical
6 medical condition, or medical treatment or
7 diagnosis by a health care professional.

8 (G) Any other combination of data elements
9 that could allow unauthorized access to or acqui-
10 sition of the information described in subpara-
11 graph (A), (B), (C), (D), (E), or (F), includ-
12 ing—

13 (i) a unique account identifier;

14 (ii) an electronic identification num-
15 ber;

16 (iii) a user name;

17 (iv) a routing code; or

18 (v) any associated security code, access
19 code, or password or any associated security
20 questions and answers that could allow un-
21 authorized access to the account.

22 (16) SERVICE PROVIDER.—

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

1 (i) *provides electronic data trans-*
2 *mission, routing, intermediate and tran-*
3 *sient storage, or connections to the system*
4 *or network of the business entity;*

5 (ii) *is not the sender or the intended*
6 *recipient of the data;*

7 (iii) *is not ordinarily expected to select*
8 *or modify the content of the electronic data;*
9 *and*

10 (iv) *transmits, routes, stores, or pro-*
11 *vides connections for personal information*
12 *in a manner that personal information is*
13 *undifferentiated from other types of data*
14 *that such business entity transmits, routes,*
15 *stores, or provides connections.*

16 (B) *SAVINGS CLAUSE.—Any such business*
17 *entity shall be treated as a service provider*
18 *under this Act only to the extent that the busi-*
19 *ness entity is engaged in the provision of the*
20 *transmission, routing, intermediate and tran-*
21 *sient storage or connections described in sub-*
22 *paragraph (A).*

23 (b) *MODIFIED DEFINITION BY RULEMAKING.—The*
24 *Federal Trade Commission may, by rule promulgated*
25 *under section 553 of title 5, United States Code, modify*

1 *the definition of “sensitive personally identifiable informa-*
 2 *tion” in a manner consistent with the purposes of this Act*
 3 *and to the extent that such modification will not unreason-*
 4 *ably impede interstate commerce.*

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

9 **SEC. 101. CONCEALMENT OF SECURITY BREACHES INVOLV-**
 10 **ING SENSITIVE PERSONALLY IDENTIFIABLE**
 11 **INFORMATION.**

12 *(a) IN GENERAL.—Chapter 47 of title 18, United*
 13 *States Code, is amended by adding at the end the following:*

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

17 *“(a) Whoever, having knowledge of a security breach*
 18 *and of the fact that notice of such security breach is re-*
 19 *quired under title II of the Personal Data Protection and*
 20 *Breach Accountability Act of 2011, intentionally or will-*
 21 *fully conceals the fact of such security breach and which*
 22 *breach, shall, in the event that such security breach results*
 23 *in economic harm or substantial emotional distress to 1 or*
 24 *more persons, shall be fined under this title or imprisoned*
 25 *not more than 5 years, or both.*

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

4 “(c) Any person seeking an exemption under section
5 212(b) of the Personal Data Protection and Breach Ac-
6 countability Act of 2011 shall be immune from prosecution
7 under this section if the United States Secret Service does
8 not indicate, in writing, that such notice be given under
9 section 212(b)(1)(B) of the Personal Data Protection and
10 Breach Accountability Act of 2011.”.

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

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

14 (c) *ENFORCEMENT AUTHORITY.*—

15 (1) *IN GENERAL.*—The United States Secret
16 Service and the Federal Bureau of Investigation shall
17 have the authority to investigate offenses under this
18 section.

19 (2) *NONEXCLUSIVITY.*—The authority granted in
20 paragraph (1) shall not be exclusive of any existing
21 authority held by any other Federal agency.

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

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

6 (b) *PROHIBITION.*—

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

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

21 (B) *monitor, manipulate, aggregate, and*
22 *market the data collected in the process of inter-*
23 *cepting a web search or query entered by an au-*
24 *thorized user of a protected computer and derive*
25 *an economic benefit from such activity.*

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

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

14 (1) *network or computer security purposes;*

15 (2) *diagnostics;*

16 (3) *technical support;*

17 (4) *repair;*

18 (5) *network management;*

19 (6) *authorized updates of software or system*
20 *firmware;*

21 (7) *authorized remote system management;*

22 (8) *authorized provision of protection for users of*
23 *the computer from objectionable content;*

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

4 (10) *detection or prevention of fraud.*

5 (d) *ENFORCEMENT BY THE ATTORNEY GENERAL.—*

6 (1) *LIABILITY AND PENALTY FOR VIOLATIONS.—*

7 *Any person who engages in an activity in violation*
8 *of this section shall be fined not more than \$500,000.*

9 (2) *ENHANCED LIABILITY AND PENALTIES FOR*

10 *PATTERN OR PRACTICE OF VIOLATIONS.—*

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

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

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

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

25 (B) *any history of prior such conduct;*

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

3 (D) the effect on the ability of the defendant
4 *to continue to do business; and*

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

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

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

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

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

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

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

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

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

20 (2) *HIPAA REGULATED ENTITIES.*—

21 (A) *COVERED ENTITIES.*—A business entity
22 subject to the Health Insurance Portability and
23 Accountability Act of 1996 (42 U.S.C. 1301 et
24 seq.), including the data security requirements
25 and implementing regulations of that Act.

1 (B) *COMPLIANCE.*—A business entity that—

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

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

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

22 (4) *PUBLIC RECORDS.*—Public records not other-
23 wise subject to a confidentiality or nondisclosure re-
24 quirement, or information obtained from a public

1 (A) ensure the privacy, security, and con-
2 fidentiality of sensitive personally identifiable
3 information;

4 (B) protect against any anticipated
5 vulnerabilities to the privacy, security, or integ-
6 rity of sensitive personally identifiable informa-
7 tion; and

8 (C) protect against unauthorized access to
9 or use of sensitive personally identifiable infor-
10 mation that could create a significant risk of
11 harm to any individual.

12 (3) *RISK ASSESSMENT.*—A business entity
13 shall—

14 (A) identify reasonably foreseeable internal
15 and external vulnerabilities that could result in
16 unauthorized access, disclosure, use, or alteration
17 of sensitive personally identifiable information
18 or systems containing sensitive personally identi-
19 fiable information;

20 (B) assess the likelihood of and potential
21 damage from unauthorized access, disclosure,
22 use, or alteration of sensitive personally identifi-
23 able information;

24 (C) assess the sufficiency of its policies,
25 technologies, and safeguards in place to control

1 *and minimize risks from unauthorized access,*
2 *disclosure, use, or alteration of sensitive person-*
3 *ally identifiable information; and*

4 *(D) assess the vulnerability of sensitive per-*
5 *sonally identifiable information during destruc-*
6 *tion and disposal of such information, including*
7 *through the disposal or retirement of hardware.*

8 (4) *RISK MANAGEMENT AND CONTROL.—Each*
9 *business entity shall—*

10 *(A) design its personal data privacy and se-*
11 *curity program to control the risks identified*
12 *under paragraph (3); and*

13 *(B) adopt measures commensurate with the*
14 *sensitivity of the data as well as the size, com-*
15 *plexity, and scope of the activities of the business*
16 *entity that—*

17 *(i) control access to systems and facili-*
18 *ties containing sensitive personally identifi-*
19 *able information, including controls to au-*
20 *thenticate and permit access only to author-*
21 *ized individuals;*

22 *(ii) detect, record, and preserve infor-*
23 *mation relevant to actual and attempted*
24 *fraudulent, unlawful, or unauthorized ac-*
25 *cess, disclosure, use, or alteration of sen-*

1 *sitive personally identifiable information,*
2 *including by employees and other individ-*
3 *uals otherwise authorized to have access;*

4 *(iii) protect sensitive personally identi-*
5 *fiable information during use, transmission,*
6 *storage, and disposal by encryption, redac-*
7 *tion, or access controls that are widely ac-*
8 *cepted as an effective industry practice or*
9 *industry standard, or other reasonable*
10 *means (including as directed for disposal of*
11 *records under section 628 of the Fair Credit*
12 *Reporting Act (15 U.S.C. 1681w) and the*
13 *implementing regulations of such Act as set*
14 *forth in section 682 of title 16, Code of Fed-*
15 *eral Regulations);*

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

22 *(v) trace access to records containing*
23 *sensitive personally identifiable information*
24 *so that the business entity can determine*
25 *who accessed or acquired such sensitive per-*

1 sonally identifiable information pertaining
2 to specific individuals;

3 (vi) ensure that no third party or cus-
4 tomer of the business entity is authorized to
5 access or acquire sensitive personally identi-
6 fiable information without the business enti-
7 ty first performing sufficient due diligence
8 to ascertain, with reasonable certainty, that
9 such information is being sought for a valid
10 legal purpose; and

11 (vii) minimize the amount of personal
12 information maintained by the business en-
13 tity, providing for the retention of such per-
14 sonal information only as reasonably need-
15 ed for the business purposes of the business
16 entity or as necessary to comply with any
17 other provision of law.

18 (b) *TRAINING.*—Each business entity subject to this
19 subtitle shall take steps to ensure employee training and
20 supervision for implementation of the data security pro-
21 gram of the business entity.

22 (c) *VULNERABILITY TESTING.*—

23 (1) *IN GENERAL.*—Each business entity subject
24 to this subtitle shall take steps to ensure regular test-
25 ing of key controls, systems, and procedures of the

1 *personal data privacy and security program to detect,*
2 *prevent, and respond to attacks or intrusions, or other*
3 *system failures.*

4 (2) *FREQUENCY.—The frequency and nature of*
5 *the tests required under paragraph (1) shall be deter-*
6 *mined by the risk assessment of the business entity*
7 *under subsection (a)(3).*

8 (d) *CERTAIN RELATIONSHIP TO PROVIDERS OF SERV-*
9 *ICES.—In the event a business entity subject to this subtitle*
10 *engages a person or entity not subject to this subtitle (other*
11 *than a service provider) to receive sensitive personally iden-*
12 *tifiable information in performing services or functions*
13 *(other than the services or functions provided by a service*
14 *provider) on behalf of and under the instruction of such*
15 *business entity, such business entity shall—*

16 (1) *exercise appropriate due diligence in select-*
17 *ing the person or entity for responsibilities related to*
18 *sensitive personally identifiable information, and take*
19 *reasonable steps to select and retain a person or enti-*
20 *ty that is capable of maintaining appropriate safe-*
21 *guards for the security, privacy, and integrity of the*
22 *sensitive personally identifiable information at issue;*
23 *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 entities subject to section 201, this section, and
3 subtitle B.

4 (e) *PERIODIC ASSESSMENT AND PERSONAL DATA PRI-*
5 *VACY AND SECURITY MODERNIZATION.*—Each business en-
6 *tity subject to this subtitle shall on a regular basis monitor,*
7 *evaluate, and adjust, as appropriate its data privacy and*
8 *security program in light of any relevant changes in—*

9 (1) *technology;*

10 (2) *the sensitivity of sensitive personally identifi-*
11 *able information;*

12 (3) *internal or external threats to sensitive per-*
13 *sonally identifiable information; and*

14 (4) *the changing business arrangements of the*
15 *business entity, such as—*

16 (A) *mergers and acquisitions;*

17 (B) *alliances and joint ventures;*

18 (C) *outsourcing arrangements;*

19 (D) *bankruptcy; and*

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

22 (f) *IMPLEMENTATION TIMELINE.*—Not later than 1
23 *year after the date of enactment of this Act, a business enti-*
24 *ty subject to the provisions of this subtitle shall implement*

1 *a data privacy and security program pursuant to this sub-*
2 *title.*

3 **SEC. 203. FEDERAL ENFORCEMENT.**

4 *(a) CIVIL PENALTIES.—*

5 *(1) IN GENERAL.—The Attorney General may*
6 *bring a civil action in the appropriate United States*
7 *district court against any business entity that engages*
8 *in conduct constituting a violation of this subtitle*
9 *and, upon proof of such conduct by a preponderance*
10 *of the evidence, such business entity shall be subject*
11 *to a civil penalty of not more than \$5,000 per viola-*
12 *tion per day while such a violation exists, with a*
13 *maximum of \$20,000,000 per violation, unless such*
14 *conduct is found to be willful or intentional.*

15 *(2) INTENTIONAL OR WILLFUL VIOLATION.—A*
16 *business entity that intentionally or willfully violates*
17 *the provisions of this subtitle shall be subject to addi-*
18 *tional penalties in the amount of \$5,000 per violation*
19 *per day while such a violation exists.*

20 *(3) CONSIDERATIONS.—In determining the*
21 *amount of a civil penalty under this subsection, the*
22 *court shall take into account—*

23 *(A) the degree of culpability of the business*
24 *entity;*

1 (B) any prior violations of this subtitle by
2 the business entity;

3 (C) the ability of the business entity to pay
4 a civil penalty;

5 (D) the effect on the ability of the business
6 entity to continue to do business;

7 (E) the number of individuals whose sen-
8 sitive personally identifiable information was
9 compromised by the breach;

10 (F) the relative cost of compliance with this
11 subtitle; and

12 (G) such other matters as justice may re-
13 quire.

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

16 (1) *IN GENERAL.*—If it appears that a business
17 entity has engaged, or is engaged, in any act or prac-
18 tice constituting a violation of this subtitle, the Attor-
19 ney General may petition an appropriate district
20 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 an
24 order under paragraph (1), if the court finds that the

1 *conduct in question constitutes a violation of this sub-*
2 *title.*

3 *(c) OTHER RIGHTS AND REMEDIES.—The rights and*
4 *remedies available under this section are cumulative and*
5 *shall not affect any other rights and remedies available*
6 *under law.*

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

8 *(a) CIVIL ACTIONS.—*

9 *(1) IN GENERAL.—In any case in which the at-*
10 *torney general of a State or any State or local law*
11 *enforcement agency authorized by the State attorney*
12 *general or by State statute to prosecute violations of*
13 *consumer protection law, has reason to believe that an*
14 *interest of the residents of that State has been or is*
15 *threatened or adversely affected by the acts or prac-*
16 *tices of a business entity that violate this subtitle, the*
17 *State may bring a civil action on behalf of the resi-*
18 *dents of that State in a district court of the United*
19 *States of appropriate jurisdiction, or any other court*
20 *of competent jurisdiction, to—*

21 *(A) enjoin that act or practice;*

22 *(B) enforce compliance with this subtitle; or*

23 *(C) obtain civil penalties of not more than*
24 *\$5,000 per violation per day while such viola-*

1 *tions persist, up to a maximum of \$20,000,000*
2 *per violation.*

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

6 (A) *the degree of culpability of the business*
7 *entity;*

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

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

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

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

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

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

21 (3) *NOTICE.—*

22 (A) *IN GENERAL.—Before filing an action*
23 *under this subsection, the attorney general of the*
24 *State involved shall provide to the Attorney Gen-*
25 *eral—*

- 1 (i) a written notice of that action; and
2 (ii) a copy of the complaint for that
3 action.

4 (B) *EXCEPTION.*—Subparagraph (A) shall
5 not apply with respect to the filing of an action
6 by an attorney general of a State under this sub-
7 section, if the attorney general of a State deter-
8 mines that it is not feasible to provide the notice
9 described in this subparagraph before the filing
10 of the action.

11 (C) *NOTIFICATION WHEN PRACTICABLE.*—In
12 an action described in subparagraph (B), the at-
13 torney general of a State shall provide the writ-
14 ten notice and a copy of the complaint to the At-
15 torney General as soon after the filing of the
16 complaint as practicable.

17 (b) *FEDERAL PROCEEDINGS.*—Upon receiving notice
18 under subsection (a)(3), the Attorney General shall have the
19 right to—

20 (1) move to stay the action, pending the final
21 disposition of a pending Federal proceeding or action
22 described in subsection (c);

23 (2) initiate an action in the appropriate United
24 States district court under section 218 and move to

1 *consolidate all pending actions, including State ac-*
2 *tions, in such court;*

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

5 (4) *file petitions for appeal.*

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

14 (d) *CONSTRUCTION.—For purposes of bringing any*
15 *civil action under subsection (a), nothing in this section*
16 *shall be construed to prevent an attorney general of a State*
17 *from exercising the powers conferred on such attorney gen-*
18 *eral by the laws of that State to—*

19 (1) *conduct investigations;*

20 (2) *administer oaths or affirmations; or*

21 (3) *compel the attendance of witnesses or the*
22 *production of documentary and other evidence.*

23 (e) *VENUE; SERVICE OF PROCESS.—*

24 (1) *VENUE.—Any action brought under sub-*
25 *section (a) may be brought in—*

1 (A) *the district court of the United States*
 2 *that meets applicable requirements relating to*
 3 *venue under section 1391 of title 28, United*
 4 *States Code; or*

5 (B) *another court of competent jurisdiction.*

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

9 (A) *is an inhabitant; or*

10 (B) *may be found.*

11 **SEC. 205. SUPPLEMENTAL ENFORCEMENT BY INDIVIDUALS.**

12 (a) *IN GENERAL.—Any person aggrieved by a viola-*
 13 *tion of the provisions of this subtitle by a business entity*
 14 *may bring a civil action in a court of appropriate jurisdic-*
 15 *tion to recover for personal injuries sustained as a result*
 16 *of the violation.*

17 (b) *AUTHORITY TO BRING CIVIL ACTION; JURISDIC-*
 18 *TION.—As provided in subsection (c), any person may com-*
 19 *mence a civil action on his own behalf against any business*
 20 *entity who is alleged to have violated the provisions of this*
 21 *subtitle.*

22 (c) *REMEDIES IN A CITIZEN SUIT.—*

23 (1) *DAMAGES.—Any individual harmed by a*
 24 *failure of a business entity to comply with the provi-*
 25 *sions of this subtitle, shall be able to collect damages*

1 of not more than \$10,000 per violation per day while
2 such violations persist, up to a maximum of
3 \$20,000,000 per violation.

4 (2) *PUNITIVE DAMAGES.*—A business entity may
5 be liable for punitive damages if the business entity
6 intentionally or willfully violates the provisions of
7 this subtitle.

8 (3) *EQUITABLE RELIEF.*—A business entity that
9 violates the provisions of this subtitle may be enjoined
10 to comply with the provisions of those sections.

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

15 (e) *NONENFORCEABILITY OF CERTAIN PROVISIONS*
16 *WAIVING RIGHTS AND REMEDIES OR REQUIRING ARBITRA-*
17 *TION OF DISPUTES.*—

18 (1) *WAIVER OF RIGHTS AND REMEDIES.*—The
19 rights and remedies provided for in this section may
20 not be waived by any agreement, policy form, or con-
21 dition of employment including by a predispute arbi-
22 tration agreement.

23 (2) *PREDISPUTE ARBITRATION AGREEMENTS.*—
24 No predispute arbitration agreement shall be valid or

1 enforceable, if the agreement requires arbitration of a
2 dispute arising under this section.

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

6 (1) *the degree of culpability of the business enti-*
7 *ty;*

8 (2) *any prior violations of this subtitle by the*
9 *business entity;*

10 (3) *the ability of the business entity to pay a*
11 *civil penalty;*

12 (4) *the effect on the ability of the business entity*
13 *to continue to do business;*

14 (5) *the number of individuals whose sensitive*
15 *personally identifiable information was compromised*
16 *by the breach;*

17 (6) *the relative cost of compliance with this sub-*
18 *title; and*

19 (7) *such other matters as justice may require.*

20 ***Subtitle B—Security Breach***
21 ***Notification***

22 ***SEC. 211. NOTICE TO INDIVIDUALS.***

23 (a) *IN GENERAL.*—*Any agency, or business entity en-*
24 *gaged in interstate commerce other than a service provider,*
25 *that uses, accesses, transmits, stores, disposes of or collects*

1 *sensitive personally identifiable information that experi-*
2 *ences a security breach of such information, shall, following*
3 *the discovery of such security breach of such information,*
4 *notify any resident of the United States whose sensitive per-*
5 *sonally identifiable information has been, or is reasonably*
6 *believed to have been, accessed, or acquired.*

7 (b) *OBLIGATION OF OWNER OR LICENSEE.—*

8 (1) *NOTICE TO OWNER OR LICENSEE.—Any*
9 *agency, or business entity engaged in interstate com-*
10 *merce, that uses, accesses, transmits, stores, disposes*
11 *of, or collects sensitive personally identifiable infor-*
12 *mation that the agency or business entity does not*
13 *own or license shall notify the owner or licensee of the*
14 *information following the discovery of a security*
15 *breach involving such information.*

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

1 (3) *BUSINESS ENTITY RELIEVED FROM GIVING*
2 *NOTICE.*—*A business entity obligated to give notice*
3 *under subsection (a) shall be relieved of such obliga-*
4 *tion if an owner or licensee of the sensitive personally*
5 *identifiable information subject to the security breach,*
6 *or other designated third party, provides such notifi-*
7 *cation.*

8 (4) *SERVICE PROVIDERS.*—*If a service provider*
9 *becomes aware of a security breach containing sen-*
10 *sitive personally identifiable information that is*
11 *owned or possessed by another business entity that*
12 *connects to or uses a system or network provided by*
13 *the service provider for the purpose of transmitting,*
14 *routing, or providing intermediate or transient stor-*
15 *age of such data, the service provider shall be required*
16 *to notify the business entity who initiated such con-*
17 *nection, transmission, routing, or storage of the secu-*
18 *rity breach if the business entity can be reasonably*
19 *identified. Upon receiving such notification from a*
20 *service provider, the business entity shall be required*
21 *to provide the notification required under subsection*
22 *(a).*

23 (c) *TIMELINESS OF NOTIFICATION.*—

24 (1) *IN GENERAL.*—*All notifications required*
25 *under this section shall be made without unreasonable*

1 *delay following the discovery by the agency or busi-*
2 *ness entity of a security breach.*

3 (2) *REASONABLE DELAY.*—*Reasonable delay*
4 *under this subsection may include any time necessary*
5 *to determine the scope of the security breach, conduct*
6 *the risk assessment described in section 212(b)(1), and*
7 *provide notice to law enforcement when required.*

8 (3) *BURDEN OF PRODUCTION.*—*The agency,*
9 *business entity, owner, or licensee required to provide*
10 *notice under this subtitle shall, upon the request of the*
11 *Attorney General, the Federal Trade Commission, or*
12 *the attorney general of a State or any State or local*
13 *law enforcement agency authorized by the attorney*
14 *general of the State or by State statute to prosecute*
15 *violations of consumer protection law, provide records*
16 *or other evidence of the notifications required under*
17 *this subtitle, including to the extent applicable, the*
18 *reasons for any delay of notification.*

19 (d) *DELAY OF NOTIFICATION AUTHORIZED FOR LAW*
20 *ENFORCEMENT OR NATIONAL SECURITY PURPOSES.*—

21 (1) *IN GENERAL.*—*If a Federal law enforcement*
22 *agency or member of the intelligence community de-*
23 *termines that the notification required under this sec-*
24 *tion would impede any lawfully authorized criminal*
25 *investigation or authorized investigative, protective,*

1 *or intelligence activities that are carried out by or on*
2 *behalf of any element of the intelligence community*
3 *and conducted in accordance with the United States*
4 *laws, authorities, and regulations governing such in-*
5 *telligence activities, such notification shall be delayed*
6 *upon written notice from such Federal law enforce-*
7 *ment agency or member of the intelligence community*
8 *to the agency or business entity that experienced the*
9 *breach. The notification shall specify in writing the*
10 *period of delay required.*

11 (2) *EXTENDED DELAY OF NOTIFICATION.*—*If the*
12 *notification required under subsection (a) is delayed*
13 *pursuant to paragraph (1), an agency or business en-*
14 *tity shall give notice 30 days after the day such law*
15 *enforcement delay was invoked unless a Federal law*
16 *enforcement or member of the intelligence community*
17 *provides written notification that further delay is*
18 *necessary.*

19 (3) *LAW ENFORCEMENT IMMUNITY.*—*No non-con-*
20 *stitutional cause of action shall lie in any court*
21 *against an agency for acts relating to the delay of no-*
22 *tification for law enforcement or intelligence purposes*
23 *under this subtitle.*

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

2 (a) *EXEMPTION FOR NATIONAL SECURITY AND LAW*
3 *ENFORCEMENT.*—

4 (1) *IN GENERAL.*—*Section 211 shall not apply to*
5 *an agency or business entity if—*

6 (A) *the United States Secret Service or the*
7 *Federal Bureau of Investigation determines that*
8 *notification of the security breach could be ex-*
9 *pected to reveal sensitive sources and methods or*
10 *similarly impede the ability of the Government*
11 *to conduct law enforcement investigations; or*

12 (B) *the Federal Bureau of Investigation de-*
13 *termines that notification of the security breach*
14 *could be expected to cause damage to national se-*
15 *curity.*

16 (2) *IMMUNITY.*—*No non-constitutional cause of*
17 *action shall lie in any court against any Federal*
18 *agency for acts relating to the exemption from notifi-*
19 *cation under this subtitle.*

20 (b) *SAFE HARBOR.*—

21 (1) *IN GENERAL.*—*An agency or business entity*
22 *shall be exempt from the notice requirements under*
23 *section 211, if—*

24 (A) *a risk assessment conducted by the*
25 *agency or business entity, in consultation with*
26 *the Federal Trade Commission, concludes that*

1 *there is no significant risk that a security breach*
2 *has resulted in, or will result in harm to the in-*
3 *dividuals whose sensitive personally identifiable*
4 *information was subject to the security breach;*
5 *and*

6 *(B) the Federal Trade Commission or des-*
7 *ignated entity does not indicate within 7 busi-*
8 *ness days from the receipt of written notification*
9 *from an agency or business entity pursuant to*
10 *subsection 212 (b)(2), that the agency or business*
11 *entity should not be exempt from the notice re-*
12 *quirements of section 211.*

13 *(2) RISK ASSESSMENT REQUIREMENTS.—*

14 *(A) CONDUCTING A RISK ASSESSMENT.—*

15 *Upon discovery of a security breach of an agency*
16 *or business entity, the agency or business entity*
17 *shall conduct a risk assessment to determine if*
18 *there is a significant risk that the security*
19 *breach resulted in, or will result in, harm to the*
20 *individuals whose sensitive personally identifi-*
21 *able information was subject to the security*
22 *breach.*

23 *(i) PRESUMPTION OF NO SIGNIFICANT*

24 *RISK.—It is presumed that there is no sig-*
25 *nificant risk that the security breach has re-*

1 sulted in, or will result in, harm to the in-
2 dividuals whose sensitive personally identi-
3 fiable data was subject to the security
4 breach, if the sensitive personally identifi-
5 able information has been rendered unus-
6 able, unreadable, or indecipherable through
7 a security technology or methodology (if the
8 technology or methodology is generally ac-
9 cepted by experts in the information secu-
10 rity field). Any such presumption may be
11 rebutted by facts demonstrating that the se-
12 curity technologies or methodologies in a
13 specific case, have been or are reasonably
14 likely to be compromised.

15 (ii) *PRESUMPTION OF SIGNIFICANT*
16 *RISK.*—It is presumed that there is a sig-
17 nificant risk that the security breach has re-
18 sulted in, or will result in, harm to individ-
19 uals whose sensitive personally identifiable
20 information was subject to the security
21 breach if the agency or business entity
22 failed to render such sensitive personally
23 identifiable information indecipherable
24 through a security technology or method-
25 ology (if the technology or methodology is

1 *generally accepted by experts in the infor-*
2 *mation security field).*

3 (iii) *METHODOLOGIES OR TECH-*
4 *NOLOGIES.—*

5 (I) *REQUIRED RULEMAKING.—Not*
6 *later than 1 year after the date of the*
7 *enactment of this Act, and biannually*
8 *thereafter, the Federal Trade Commis-*
9 *sion, after consultation with the Na-*
10 *tional Institute of Standards and*
11 *Technology, shall issue rules (pursuant*
12 *to section 553 of title 5, United States*
13 *Code) or guidance to identify security*
14 *methodologies or technologies, such as*
15 *encryption, which render sensitive per-*
16 *sonally identifiable information unus-*
17 *able, unreadable, or indecipherable,*
18 *that shall, if applied to such sensitive*
19 *personally identifiable information, es-*
20 *tablish a presumption that no signifi-*
21 *cant risk of harm exists to individuals*
22 *whose sensitive personally identifiable*
23 *information was subject to a security*
24 *breach. Any such presumption may be*
25 *rebutted by facts demonstrating that*

1 *any such methodology or technology in*
2 *a specific case has been or is reason-*
3 *ably likely to be compromised.*

4 (II) *REQUIRED CONSULTATION.*—

5 *In issuing rules or guidance under*
6 *subclause (II), the Commission shall*
7 *also consult with relevant industries,*
8 *consumer organizations, and data se-*
9 *curity and identity theft prevention ex-*
10 *erts and established standards setting*
11 *bodies.*

12 (iv) *FTC GUIDANCE.*—*Not later than 1*

13 *year after the date of the enactment of this*
14 *Act, the Federal Trade Commission, after*
15 *consultation with the National Institute of*
16 *Standards and Technology, shall issue guid-*
17 *ance regarding the application of the ex-*
18 *emption in clause (i).*

19 (B) *WRITTEN NOTIFICATION.*—*Without un-*

20 *reasonable delay, but not later than 7 days after*
21 *the discovery of a security breach, unless ex-*
22 *tended by the United States Secret Service or the*
23 *Federal Bureau of Investigation, the agency or*
24 *business entity must notify the Federal Trade*

1 *Commission and designated entity, in writing,*
2 *of—*

3 *(i) the results of the risk assessment;*

4 *and*

5 *(ii) its decision to invoke the risk as-*
6 *essment exemption.*

7 *(C) VIOLATIONS.—It shall be a violation of*
8 *this section to—*

9 *(i) fail to conduct a risk assessment in*
10 *a reasonable manner, or according to stand-*
11 *ards generally accepted by experts in the*
12 *field of information security; or*

13 *(ii) submit results of a risk assessment*
14 *that—*

15 *(I) conceal violations of law, inef-*
16 *iciency, or administrative error;*

17 *(II) prevent embarrassment to a*
18 *business entity, organization, or agen-*
19 *cy;*

20 *(III) restrain competition;*

21 *(IV) contain fraudulent or delib-*
22 *erately misleading information; or*

23 *(V) delay notification under sec-*
24 *tion 211 for any other reason, except*
25 *where the agency or business entity*

1 *reasonably believes that the risk assess-*
2 *ment exception may apply.*

3 (c) *FINANCIAL FRAUD PREVENTION EXEMPTION.—*

4 (1) *IN GENERAL.—A business entity shall be ex-*
5 *empt from the notice requirements of this subtitle if*
6 *the business entity utilizes or participates in a secu-*
7 *rity program that—*

8 (A) *effectively blocks the use of the sensitive*
9 *personally identifiable information to initiate*
10 *unauthorized financial transactions before they*
11 *are charged to the account of the individual; and*

12 (B) *provides for notice to affected individ-*
13 *uals after a security breach that has resulted in*
14 *fraud or unauthorized transactions.*

15 (2) *LIMITATION.—Paragraph (1) shall not apply*
16 *to a business entity if the information subject to the*
17 *security breach includes an individual's first and last*
18 *name, or any other type of sensitive personally identi-*
19 *fiable information, other than a credit card or credit*
20 *card security code identified in section 3, unless that*
21 *information is only a credit card number or a credit*
22 *card security code.*

23 (d) *LIMITATIONS.—Notwithstanding any other obliga-*
24 *tion under this subtitle, this subtitle does not apply to the*
25 *following—*

1 (1) *FINANCIAL INSTITUTIONS.*—*A financial in-*
2 *stitution subject to the data security requirements and*
3 *standards under 501(b) of the Gramm-Leach-Bliley*
4 *Act (15 U.S.C. 6801 et seq.), and subject to the juris-*
5 *isdiction of an agency or authority described in section*
6 *505(a) of the Gramm-Leach-Bliley Act (15 U.S.C.*
7 *6805(a)), if the Federal functional regulator (as de-*
8 *fined by section 509 of the Gramm-Leach-Bliley Act*
9 *(15 U.S.C. 6809)) with jurisdiction over that finan-*
10 *cial institution has issued a regulation under title V*
11 *of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et*
12 *seq.) that requires financial institutions within its ju-*
13 *risdiction to provide notification to individuals fol-*
14 *lowing a breach of security.*

15 (2) *HIPAA REGULATED ENTITIES EXEMPTION.*—

16 (A) *IN GENERAL.*—*A business entity shall*
17 *be exempt from the notice requirement under sec-*
18 *tion 211 if the business entity is one of the fol-*
19 *lowing:*

20 (i) *COVERED ENTITIES.*—*A business*
21 *entity subject to the Health Insurance Port-*
22 *ability and Accountability Act of 1996 (42*
23 *U.S.C. 1301 et seq.), including the data*
24 *breach notification requirements and imple-*
25 *menting regulations of that Act.*

1 (ii) *BUSINESS ENTITIES.*—A business
2 entity that—

3 (I) is acting as a business asso-
4 ciate, as that term is defined under the
5 Health Insurance Portability and Ac-
6 countability Act of 1996 (42 U.S.C.
7 1301 et seq.) and is in compliance with
8 the requirements imposed under that
9 Act and implementing regulations pro-
10 mulgated under that Act; and

11 (II) is subject to, and currently in
12 compliance with, the data breach noti-
13 fication requirements under section
14 13402 or 13407 of the American Rein-
15 vestment and Recovery Act of 2009 (42
16 U.S.C. 17932 and 17937) and imple-
17 menting regulations promulgated
18 under such sections.

19 (B) *LIMITATION.*—Paragraph (1) shall not
20 apply to a business entity if the information
21 subject to the security breach includes an indi-
22 vidual's first and last name, or any other type
23 of sensitive personally identifiable information
24 other than a health insurance policy or sub-
25 scriber identification number or information re-

1 *garding an individual’s medical history, mental*
2 *or physical medical condition, or medical treat-*
3 *ment or diagnosis by a health care professional*
4 *as identified in section 3 unless that information*
5 *is only a health insurance policy or subscriber*
6 *identification number or information regarding*
7 *an individual’s medical history, mental or phys-*
8 *ical medical condition, or medical treatment or*
9 *diagnosis by a health care professional.*

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

11 *To comply with section 211, an agency or business en-*
12 *tity shall provide the following forms of notice:*

13 (1) *INDIVIDUAL WRITTEN NOTICE.—Written no-*
14 *tice to individuals by 1 of the following means:*

15 (A) *Individual written notification to the*
16 *last known home mailing address of the indi-*
17 *vidual in the records of the agency or business*
18 *entity.*

19 (B) *E-mail notice, unless the individual has*
20 *expressly opted not to receive such notices of se-*
21 *curity breaches or the notice is inconsistent with*
22 *the provisions permitting electronic transmission*
23 *of notices under section 101 of the Electronic*
24 *Signatures in Global and National Commerce*
25 *Act (15 U.S.C. 7001).*

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

3 (3) *PUBLIC NOTICE.*—

4 (A) *ELECTRONIC NOTICE.*—*Prominent no-*
5 *tice via all reasonable means of electronic contact*
6 *between the individual and the agency or busi-*
7 *ness entity, including any website, networked de-*
8 *vices, or other interface through which the agency*
9 *or business entity regularly interacts with the*
10 *consumer, if the number of individuals whose*
11 *sensitive personally identifiable information was*
12 *or is reasonably believed to have been accessed or*
13 *acquired by an unauthorized person exceeds*
14 *5,000.*

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

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

22 (a) *IN GENERAL.*—*Regardless of the method by which*
23 *individual notice is provided to individuals under section*
24 *213(1), such notice shall include—*

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 acquired
4 by an unauthorized person, and how the agency or
5 business entity came into possession of the sensitive
6 personally identifiable information at issue;

7 (2) a toll-free number—

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

11 (B) from which the individual may learn
12 what types of sensitive personally identifiable in-
13 formation the agency or business entity main-
14 tained about that individual;

15 (3) the toll-free contact telephone numbers,
16 websites, and addresses for the major credit reporting
17 agencies;

18 (4) the telephone numbers and websites for the
19 relevant Federal agencies that provide information re-
20 garding identity theft prevention and protection;

21 (5) notice that the individual is entitled to re-
22 ceive, at no cost to such individual, consumer credit
23 reports on a quarterly basis for a period of 2 years,
24 credit monitoring or any other service that enables
25 consumers to detect the misuse of sensitive personally

1 *identifiable information for a period of 2 years, and*
2 *instructions to the individual on requesting such re-*
3 *ports or service from the agency or business entity;*

4 (6) *notice that the individual is entitled to re-*
5 *ceive a security freeze and that the agency or business*
6 *entity will be liable for any costs associated with the*
7 *security freeze for 2 years and the necessary instruc-*
8 *tions for requesting a security freeze; and*

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

13 (b) *TELEPHONE NOTICE.—Telephone notice described*
14 *in section 213(2) shall include, to the extent possible—*

15 (1) *notification that a security breach has oc-*
16 *curred and that the individual’s sensitive personally*
17 *identifiable information may have been compromised;*

18 (2) *a description of the categories of sensitive*
19 *personally identifiable information that were, or are*
20 *reasonably believed to have been, accessed or acquired*
21 *by an unauthorized person;*

22 (3) *a toll-free number and website—*

23 (A) *that the individual may use to contact*
24 *the agency or business entity, or the authorized*
25 *agent of the agency or business entity; and*

1 (B) from which the individual may learn
2 what types of sensitive personally identifiable in-
3 formation the agency or business entity main-
4 tained about that individual and remedies avail-
5 able to that individual; and

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

10 (c) *PUBLIC NOTICE*.—Public notice described in sec-
11 tion 213(3) shall include—

12 (1) electronic notice, which includes—

13 (A) notification that a security breach has
14 occurred and that the individual’s sensitive per-
15 sonally identifiable information may have been
16 compromised;

17 (B) a description of the categories of sen-
18 sitive personally identifiable information that
19 were, or are reasonably believed to have been,
20 accessed or acquired by an unauthorized person;
21 and

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

23 (i) that the individual may use to con-
24 tact the agency or business entity, or the

1 *authorized agent of the agency or business*
2 *entity; and*

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

9 (2) *media notice, which includes—*

10 (A) *a description of the categories of sen-*
11 *sitive personally identifiable information that*
12 *was, or is reasonably believed to have been,*
13 *accessed or acquired by an unauthorized person;*

14 (B) *a toll-free number—*

15 (i) *that the individual may use to con-*
16 *tact the agency or business entity, or the*
17 *authorized agent of the agency or business*
18 *entity; and*

19 (ii) *from which the individual may*
20 *learn what types of sensitive personally*
21 *identifiable information the agency or busi-*
22 *ness entity maintained about that indi-*
23 *vidual and remedies available to that indi-*
24 *vidual;*

1 (C) the toll-free contact telephone numbers,
2 websites, and addresses for the major credit re-
3 porting agencies;

4 (D) the telephone numbers and websites for
5 the relevant Federal agencies that provide infor-
6 mation regarding identity theft prevention and
7 protection;

8 (E) notice that the affected individuals are
9 entitled to receive, at no cost to such individuals,
10 consumer credit reports on a quarterly basis for
11 a period of 2 years, credit monitoring, or any
12 other service that enables consumers to detect the
13 misuse of sensitive personally identifiable infor-
14 mation for a period of 2 years;

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

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

23 (d) *ADDITIONAL CONTENT.*—Notwithstanding section
24 221, a State may require that a notice under subsection

1 (a) shall also include information regarding victim protec-
2 tion assistance provided for by that State.

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

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

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

17 (1) consumer credit reports from not fewer than
18 1 of the major credit reporting agencies beginning not
19 later than 60 days following the request of the indi-
20 vidual and continuing on a quarterly basis for a pe-
21 riod of 2 years thereafter; and

22 (2) a credit monitoring or other service that en-
23 ables consumers to detect the misuse of their personal
24 information, beginning not later than 60 days fol-

1 *lowing the request of the individual and continuing*
2 *for a period of 2 years.*

3 *(b) SECURITY FREEZE.—*

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

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

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

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

24 *(3) DURATION OF SECURITY FREEZE.—Except as*
25 *provided in paragraph (4), any security freeze au-*

1 *thorized pursuant to the provisions of this section*
2 *shall remain in effect until the consumer requests se-*
3 *curity freeze to be removed.*

4 (4) *DISCLOSURE OF CREDIT REPORT TO THIRD*
5 *PARTY.—*

6 (A) *IN GENERAL.—If a consumer that has*
7 *requested a security freeze under this subsection*
8 *wishes to authorize the disclosure of the credit re-*
9 *port of the consumer to a third party, or for a*
10 *specified period of time, while such security*
11 *freeze is in effect, the consumer shall contact the*
12 *credit rating agency and provide—*

13 (i) *proper identification;*

14 (ii) *the unique personal identification*
15 *number or password described in paragraph*
16 *(2)(B); and*

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

21 (B) *REQUIREMENT.—Not later than 3 busi-*
22 *ness days after receipt of a request under sub-*
23 *paragraph (A), a credit rating agency shall lift*
24 *the security freeze.*

25 (5) *PROCEDURES.—*

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

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

10 (6) *REQUESTS BY THIRD PARTY.*—If a third
11 party requests access to a credit report of a consumer
12 that has been frozen under this subsection and the
13 consumer has not authorized the disclosure of the
14 credit report of the consumer to the third party, the
15 third party may deem such credit application as in-
16 complete.

17 (7) *DETERMINATION BY CREDIT RATING AGEN-*
18 *CY.*—

19 (A) *IN GENERAL.*—A credit rating agency
20 may refuse to implement or may remove a secu-
21 rity freeze under this subsection if the agency de-
22 termines, in good faith, that—

23 (i) the request for a security freeze was
24 made as part of a fraud that the consumer
25 participated in, had knowledge of, or that

1 *can be demonstrated by circumstantial evi-*
2 *dence; or*

3 *(ii) the consumer credit report was fro-*
4 *zen due to a material misrepresentation of*
5 *fact by the consumer.*

6 *(B) NOTICE.—If a credit rating agency*
7 *makes a determination under subparagraph (A)*
8 *to not implement, or to remove, a security freeze*
9 *under this subsection, the credit rating agency*
10 *shall notify the consumer in writing of such de-*
11 *termination—*

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

16 *(ii) in the case of a removal of a secu-*
17 *rity freeze, prior to removing the freeze on*
18 *the credit report of the consumer.*

19 *(8) RULE OF CONSTRUCTION.—Nothing in this*
20 *section shall be construed to prohibit disclosure of a*
21 *credit report of a consumer to—*

22 *(A) a person, or the person's subsidiary, af-*
23 *filiate, agent or assignee with which the con-*
24 *sumer has or, prior to assignment, had an ac-*
25 *count, contract or debtor-creditor relationship for*

1 *the purpose of reviewing the account or collecting*
2 *the financial obligation owing for the account,*
3 *contract or debt;*

4 *(B) a subsidiary, affiliate, agent, assignee*
5 *or prospective assignee of a person to whom ac-*
6 *cess has been granted under paragraph (4) for*
7 *the purpose of facilitating the extension of credit*
8 *or other permissible use;*

9 *(C) any person acting pursuant to a court*
10 *order, warrant or subpoena;*

11 *(D) any person for the purpose of using*
12 *such credit information to prescreen as provided*
13 *by the Fair Credit Reporting Act (15 U.S.C.*
14 *1681 et seq.);*

15 *(E) any person for the sole purpose of pro-*
16 *viding a credit file monitoring subscription serv-*
17 *ice to which the consumer has subscribed;*

18 *(F) a credit rating agency for the sole pur-*
19 *pose of providing a consumer with a copy of the*
20 *credit report of the consumer upon the request of*
21 *the consumer; or*

22 *(G) a Federal, State or local governmental*
23 *entity, including a law enforcement agency, or*
24 *court, or their agents or assignees pursuant to*
25 *their statutory or regulatory duties. For purposes*

1 of this subsection, “reviewing the account” in-
2 cludes activities related to account maintenance,
3 monitoring, credit line increases and account
4 upgrades and enhancements; and

5 (H) any person for the sole purpose of pro-
6 viding a remedy requested by an individual
7 under this section.

8 (9) *EXCEPTIONS.*—The following persons shall
9 not be required to place a security freeze under this
10 subsection, but shall be subject to any security freeze
11 placed on a credit report by another credit rating
12 agency:

13 (A) A check services or fraud prevention
14 services company that reports on incidents of
15 fraud or issues authorizations for the purpose of
16 approving or processing negotiable instruments,
17 electronic fund transfers or similar methods of
18 payment.

19 (B) A deposit account information service
20 company that issues reports regarding account
21 closures due to fraud, substantial overdrafts,
22 automated teller machine abuse, or similar infor-
23 mation regarding a consumer to inquiring banks
24 or other financial institutions for use only in re-

1 *viewing a consumer request for a deposit account*
2 *at the inquiring bank or financial institution.*

3 *(C) A credit rating agency that—*

4 *(i) acts only to resell credit informa-*
5 *tion by assembling and merging informa-*
6 *tion contained in a database of 1 or more*
7 *credit reporting agencies; and*

8 *(ii) does not maintain a permanent*
9 *database of credit information from which*
10 *new credit reports are produced.*

11 *(10) FEES.—*

12 *(A) IN GENERAL.—A credit rating agency*
13 *may charge reasonable fees for each security*
14 *freeze, removal of such freeze or temporary lift of*
15 *such freeze for a period of time, and a temporary*
16 *lift of such freeze for a specific party.*

17 *(B) REQUIREMENT.—Any fees charged*
18 *under subparagraph (A) shall be borne by the*
19 *agency or business entity providing notice under*
20 *section 214 for 2 years following the establish-*
21 *ment of the security freeze under this subsection.*

22 *(c) COSTS RESULTING FROM A SECURITY BREACH.—*

23 *(1) IN GENERAL.—A business entity or agency*
24 *that experiences a security breach and is required to*
25 *provide notice under this subtitle shall pay, upon re-*

1 *quest, to any individual whose sensitive personally*
2 *identifiable information has been, or is reasonably be-*
3 *lieved to have been, accessed or acquired as a result*
4 *of such security breach, any costs or damages in-*
5 *curring by the individual as a result of such security*
6 *breach, including costs associated with identity theft*
7 *suffered as a result of such security breach.*

8 (2) *COMPLIANCE.—A business entity or agency*
9 *shall be deemed in compliance with this subsection if*
10 *the business entity or agency—*

11 (A) *provides insurance to any individual*
12 *whose sensitive personally identifiable informa-*
13 *tion has been, or is reasonably believed to have*
14 *been, accessed or acquired as a result of a secu-*
15 *rity breach and such insurance is sufficient to*
16 *compensate the consumer for not less than*
17 *\$25,000 of costs or damages; or*

18 (B) *pays, without unreasonable delay, any*
19 *actual costs or damages incurred by an indi-*
20 *vidual as a result of the security breach.*

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

22 *If an agency or business entity is required to provide*
23 *notification to more than 5,000 individuals under section*
24 *211(a), the agency or business entity shall also notify all*
25 *consumer reporting agencies that compile and maintain*

1 *files on consumers on a nationwide basis (as defined in sec-*
2 *tion 603(p) of the Fair Credit Reporting Act (15 U.S.C.*
3 *1681a(p)) of the timing and distribution of the notices.*
4 *Such notice shall be given to the consumer credit reporting*
5 *agencies without unreasonable delay and, if it will not*
6 *delay notice to the affected individuals, prior to the dis-*
7 *tribution of notices to the affected individuals.*

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

9 (a) *DESIGNATION OF A GOVERNMENT ENTITY TO RE-*
10 *CEIVE NOTICE.—*

11 (1) *IN GENERAL.—Not later than 60 days after*
12 *the date of enactment of this Act, the Secretary of*
13 *Homeland Security, in consultation with the Attorney*
14 *General, shall designate a Federal Government entity*
15 *to receive the information required to be submitted*
16 *under this subtitle, and any other reports and infor-*
17 *mation about information security incidents, threats,*
18 *and vulnerabilities.*

19 (2) *RESPONSIBILITIES OF THE DESIGNATED EN-*
20 *TITY.—The designated entity shall—*

21 (A) *be responsible for promptly providing*
22 *the information it receives to the United States*
23 *Secret Service and the Federal Bureau of Inves-*
24 *tigation, and to the Federal Trade Commission*
25 *for civil law enforcement purposes; and*

1 (B) provide the information described in
2 subparagraph (A) as appropriate to other Fed-
3 eral agencies for law enforcement, national secu-
4 rity, or data security purposes.

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

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

12 (2) the security breach involves a database,
13 networked or integrated databases, or other data sys-
14 tem containing the sensitive personally identifiable
15 information of more than 500,000 individuals nation-
16 wide;

17 (3) the security breach involves databases owned
18 by the Federal Government; or

19 (4) the security breach involves primarily sen-
20 sitive personally identifiable information of individ-
21 uals known to the agency or business entity to be em-
22 ployees and contractors of the Federal Government in-
23 volved in national security or law enforcement.

24 (c) FTC REVIEW OF THRESHOLDS.—

1 (1) *REVIEW.*—Not later than 1 year after the
2 date of enactment of this Act, the Federal Trade Com-
3 mission, in consultation with the Attorney General
4 and the Secretary of Homeland Security, shall pro-
5 mulgate regulations regarding the reports required
6 under subsection (a).

7 (2) *RULEMAKING.*—The Federal Trade Commis-
8 sion, in consultation with the Attorney General and
9 the Secretary of Homeland Security, after notice and
10 the opportunity for public comment, and in a manner
11 consistent with this section, shall promulgate regula-
12 tions, as necessary, under section 553 of title 5,
13 United States Code, to adjust the thresholds for notice
14 to law enforcement and national security authorities
15 under subsection (a) and to facilitate the purposes of
16 this section.

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

19 (1) Notice under subsection (a) shall be delivered
20 as promptly as possible, but not later than 10 days
21 after discovery of the security breach.

22 (2) Notice under section 211 shall be delivered to
23 individuals not later than 48 hours after the Federal
24 Bureau of Investigation or the Secret Service receives

1 *notice of a security breach from an agency or business*
2 *entity.*

3 **SEC. 218. FEDERAL ENFORCEMENT.**

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

5 *(1) IN GENERAL.—The Attorney General may*
6 *bring a civil action in the appropriate United States*
7 *district court against any business entity that engages*
8 *in conduct constituting a violation of this subtitle*
9 *and, upon proof of such conduct by a preponderance*
10 *of the evidence, such business entity shall be subject*
11 *to a civil penalty of not more than \$500 per day per*
12 *individual whose sensitive personally identifiable in-*
13 *formation was, or is reasonably believed to have been,*
14 *accessed or acquired by an unauthorized person, up*
15 *to a maximum of \$20,000,000 per violation, unless*
16 *such conduct is found to be willful or intentional.*

17 *(2) PRESUMPTION.—A violation of section*
18 *212(b)(2)(C) shall be presumed to be willful or inten-*
19 *tional conduct.*

20 *(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-*
21 *ERAL.—*

22 *(1) IN GENERAL.—If it appears that a business*
23 *entity has engaged, or is engaged, in any act or prac-*
24 *tice constituting a violation of this subtitle, the Attor-*

1 *ney General may petition an appropriate district*
2 *court of the United States for an order—*

3 *(A) enjoining such act or practice; or*

4 *(B) enforcing compliance with this subtitle.*

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

9 *(c) CIVIL ACTIONS BY THE FEDERAL TRADE COMMIS-*
10 *SION.—*

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

21 *(2) UNFAIR OR DECEPTIVE ACTS OR PRAC-*
22 *TICES.—For the purpose of the exercise by the Federal*
23 *Trade Commission of its functions and powers under*
24 *the Federal Trade Commission Act, a violation of any*
25 *requirement or prohibition imposed under this title*

1 *shall constitute an unfair or deceptive act or practice*
2 *in commerce in violation of a regulation under sec-*
3 *tion 18(a)(1)(B) of the Federal Trade Commission*
4 *Act (15 U.S.C. 57a(a)(I)(B)) regarding unfair or de-*
5 *ceptive acts or practices and shall be subject to en-*
6 *forcement by the Federal Trade Commission under*
7 *that Act with respect to any business entity, irrespec-*
8 *tive of whether that business entity is engaged in com-*
9 *merce or meets any other jurisdictional tests in the*
10 *Federal Trade Commission.*

11 *(d) CONSIDERATIONS.—In determining the amount of*
12 *a civil penalty under this subsection, the court shall take*
13 *into account—*

14 *(1) the degree of culpability of the business enti-*
15 *ty;*

16 *(2) any prior violations of this subtitle by the*
17 *business entity;*

18 *(3) the ability of the business entity to pay a*
19 *civil penalty;*

20 *(4) the effect on the ability of the business entity*
21 *to continue to do business;*

22 *(5) the number of individuals whose sensitive*
23 *personally identifiable information was compromised*
24 *by the breach;*

1 (6) *the relative cost of compliance with this sub-*
2 *title; and*

3 (7) *such other matters as justice may require.*

4 (e) *COORDINATION OF ENFORCEMENT.—*

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

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

13 (3) *COORDINATION AGREEMENT.—*

14 (A) *IN GENERAL.—In order to avoid con-*
15 *licts and promote consistency regarding the en-*
16 *forcement and litigation of matters under this*
17 *Act, not later than 180 days after the enactment*
18 *of this Act, the Attorney General and the Com-*
19 *mission shall enter into an agreement for coordi-*
20 *nation regarding the enforcement of this Act.*

21 (B) *REQUIREMENT.—The coordination*
22 *agreement entered into under subparagraph (A)*
23 *shall include provisions to ensure that parallel*
24 *investigations and proceedings under this section*
25 *are conducted in a manner that avoids conflicts*

1 *and does not impede the ability of the Attorney*
2 *General to prosecute violations of Federal crimi-*
3 *nal laws.*

4 (4) *COORDINATION WITH THE FCC.—If an en-*
5 *forcement action under this Act relates to customer*
6 *proprietary network information, the Federal Trade*
7 *Commission shall coordinate the enforcement action*
8 *with the Federal Communications Commission.*

9 (f) *RULEMAKING.—The Federal Trade Commission*
10 *may, in consultation with the Attorney General, issue such*
11 *other regulations as it determines to be necessary to carry*
12 *out this subtitle. All regulations promulgated under this Act*
13 *shall be issued in accordance with section 553 of title 5,*
14 *United States Code. Where regulations relate to customer*
15 *proprietary network information, the promulgation of such*
16 *regulations will be coordinated with the Federal Commu-*
17 *nications Commission.*

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

22 (h) *FRAUD ALERT.—Section 605A(b)(1) of the Fair*
23 *Credit Reporting Act (15 U.S.C. 1681c–1(b)(1)) is amended*
24 *by inserting “, or evidence that the consumer has received*

1 *notice that the consumer’s financial information has or*
2 *may have been compromised,” after “identity theft report”.*

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

4 (a) *IN GENERAL.*—

5 (1) *CIVIL ACTIONS.*—

6 (A) *IN GENERAL.*—*In any case in which the*
7 *attorney general of a State or any State or local*
8 *law enforcement agency authorized by the State*
9 *attorney general or by State statute to prosecute*
10 *violations of consumer protection law, has reason*
11 *to believe that an interest of the residents of that*
12 *State has been or is threatened or adversely af-*
13 *ected by the engagement of a business entity in*
14 *a practice that is prohibited under this subtitle,*
15 *the State or the State or local law enforcement*
16 *agency on behalf of the residents of the agency’s*
17 *jurisdiction, may bring a civil action on behalf*
18 *of the residents of the State or jurisdiction in a*
19 *district court of the United States of appropriate*
20 *jurisdiction or any other court of competent ju-*
21 *risdiction, including a State court, to—*

22 (i) *enjoin that practice;*

23 (ii) *enforce compliance with this sub-*
24 *title; or*

1 (iii) obtain civil penalties of not more
2 than \$500 per day per individual whose
3 sensitive personally identifiable information
4 was, or is reasonably believed to have been,
5 accessed or acquired by an unauthorized
6 person, up to a maximum of \$20,000,000
7 per violation, unless such conduct is found
8 to be willful or intentional.

9 (B) *PRESUMPTION.*—A violation of section
10 212(b)(2)(C) shall be presumed to be willful or
11 intentional.

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

15 (A) the degree of culpability of the business
16 entity;

17 (B) any prior violations of this subtitle by
18 the business entity;

19 (C) the ability of the business entity to pay
20 a civil penalty;

21 (D) the effect on the ability of the business
22 entity to continue to do business;

23 (E) the number of individuals whose sen-
24 sitive personally identifiable information was
25 compromised by the breach;

1 (F) *the relative cost of compliance with this*
2 *subtitle; and*

3 (G) *such other matters as justice may re-*
4 *quire.*

5 (3) *NOTICE.—*

6 (A) *IN GENERAL.—Before filing an action*
7 *under paragraph (1), the attorney general of the*
8 *State involved shall provide to the Attorney Gen-*
9 *eral of the United States—*

10 (i) *written notice of the action; and*

11 (ii) *a copy of the complaint for the ac-*
12 *tion.*

13 (B) *EXEMPTION.—*

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

21 (ii) *NOTIFICATION.—In an action de-*
22 *scribed in clause (i), the attorney general of*
23 *a State shall provide notice and a copy of*
24 *the complaint to the Attorney General at*

1 *the time the State attorney general files the*
2 *action.*

3 (b) *FEDERAL PROCEEDINGS.*—*Upon receiving notice*
4 *under subsection (a)(2), the Attorney General shall have the*
5 *right to—*

6 (1) *move to stay the action, pending the final*
7 *disposition of a pending Federal proceeding or action;*

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

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

14 (4) *file petitions for appeal.*

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

23 (d) *CONSTRUCTION.*—*For purposes of bringing any*
24 *civil action under subsection (a), nothing in this subtitle*
25 *regarding notification shall be construed to prevent an at-*

1 *torney general of a State from exercising the powers con-*
 2 *ferred on such attorney general by the laws of that State*
 3 *to—*

4 (1) *conduct investigations;*

5 (2) *administer oaths or affirmations; or*

6 (3) *compel the attendance of witnesses or the*
 7 *production of documentary and other evidence.*

8 (e) *VENUE; SERVICE OF PROCESS.—*

9 (1) *VENUE.—Any action brought under sub-*
 10 *section (a) may be brought in—*

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

15 (B) *another court of competent jurisdiction.*

16 (2) *SERVICE OF PROCESS.—In an action brought*
 17 *under subsection (a), process may be served in any*
 18 *district in which the defendant—*

19 (A) *is an inhabitant; or*

20 (B) *may be found.*

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

22 (a) *IN GENERAL.—Any person aggrieved by a viola-*
 23 *tion of the provisions of section 211, 213, 214, 215, or 216*
 24 *by a business entity may bring a civil action in a court*

1 *of appropriate jurisdiction to recover for personal injuries*
2 *sustained as a result of the violation.*

3 (b) *AUTHORITY TO BRING CIVIL ACTION; JURISDIC-*
4 *TION.—As provided in subsection (c), an individual may*
5 *commence a civil action on his own behalf against any busi-*
6 *ness entity who is alleged to have violated the provisions*
7 *of this subtitle.*

8 (c) *REMEDIES IN A CITIZEN SUIT.—*

9 (1) *DAMAGES.—Any individual harmed by a*
10 *failure of a business entity to comply with the provi-*
11 *sions of section 211, 213, 214, 215, or 216, shall be*
12 *able to collect damages of not more than \$500 per day*
13 *per individual whose sensitive personally identifiable*
14 *information was, or is reasonably believed to have*
15 *been, accessed or acquired by an unauthorized person,*
16 *up to a maximum of \$20,000,000 per violation*

17 (2) *PUNITIVE DAMAGES.—A business entity may*
18 *be liable for punitive damages if it—*

19 (A) *intentionally or willfully violates the*
20 *provisions of section 211, 213, 214, 215, or 216;*

21 *or*

22 (B) *failed to comply with the requirements*
23 *of subsections (a) through (d) of section 202.*

24 (3) *EQUITABLE RELIEF.—A business entity that*
25 *violates the provisions of section 211, 213, 214, 215,*

1 *or 216 may be enjoined to provide required remedies*
2 *under section 215 by a court of competent jurisdic-*
3 *tion.*

4 *(d) OTHER RIGHTS AND REMEDIES.—The rights and*
5 *remedies available under this subsection are cumulative and*
6 *shall not affect any other rights and remedies available*
7 *under law.*

8 *(e) NONENFORCEABILITY OF CERTAIN PROVISIONS*
9 *WAIVING RIGHTS AND REMEDIES OR REQUIRING ARBITRA-*
10 *TION OF DISPUTES.—*

11 *(1) WAIVER OF RIGHTS AND REMEDIES.—The*
12 *rights and remedies provided for in this section may*
13 *not be waived by any agreement, policy form, or con-*
14 *dition of employment including by a predispute arbi-*
15 *tration agreement.*

16 *(2) PREDISPUTE ARBITRATION AGREEMENTS.—*
17 *No predispute arbitration agreement shall be valid or*
18 *enforceable, if the agreement requires arbitration of a*
19 *dispute arising under this section.*

20 *(f) CONSIDERATIONS.—In determining the amount of*
21 *a civil penalty under this subsection, the court shall take*
22 *into account—*

23 *(1) the degree of culpability of the business enti-*
24 *ty;*

1 (2) *any prior violations of this subtitle by the*
2 *business entity;*

3 (3) *the ability of the business entity to pay a*
4 *civil penalty;*

5 (4) *the effect on the ability of the business entity*
6 *to continue to do business;*

7 (5) *the number of individuals whose sensitive*
8 *personally identifiable information was compromised*
9 *by the breach;*

10 (6) *the relative cost of compliance with this sub-*
11 *title; and*

12 (7) *such other matters as justice may require.*

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

14 (a) *IN GENERAL.*—*The provisions of this subtitle shall*
15 *supersede any other provision of Federal law or any provi-*
16 *sion of law of any State relating to notification by a busi-*
17 *ness entity engaged in interstate commerce or an agency*
18 *of a security breach, except as provided in this subsection.*

19 (b) *LIMITATIONS.*—

20 (1) *STATE COMMON LAW.*—*Nothing in this sub-*
21 *title shall be construed to exempt any entity from li-*
22 *ability under common law, including through the op-*
23 *eration of ordinary preemption principles, and in-*
24 *cluding liability through state trespass, contract, or*

1 *tort law, for damages caused by the failure to notify*
2 *an individual following a security breach.*

3 (2) *GRAMM-LEACH-BLILEY ACT.*—*Nothing in*
4 *this Act shall supersede the data security require-*
5 *ments of the Gramm-Leach-Bliley Act (15 U.S.C.*
6 *6801 et seq.), or implementing regulations based on*
7 *that Act.*

8 (3) *HEALTH PRIVACY.*—

9 (A) *To the extent that a business entity acts*
10 *as a covered entity or a business associate under*
11 *the Health Information Technology for Economic*
12 *and Clinical Health Act (42 U.S.C. 17932), and*
13 *has the obligation to provide breach notification*
14 *under that Act or its implementing regulations,*
15 *the requirements of this Act shall not apply.*

16 (B) *To the extent that a business entity acts*
17 *as a vendor of personal health records, a third*
18 *party service provider, or other entity subject to*
19 *the Health Information Technology for Economi-*
20 *cal and Clinical Health Act (42 U.S.C. 17937),*
21 *and has the obligation to provide breach notifica-*
22 *tion under that Act or its implementing regula-*
23 *tions, the requirements of this Act shall not*
24 *apply.*

1 **SEC. 222. AUTHORIZATION OF APPROPRIATIONS.**

2 *There are authorized to be appropriated such sums as*
3 *may be necessary to cover the costs incurred by the United*
4 *States Secret Service to carry out investigations and risk*
5 *assessments of security breaches as required under this sub-*
6 *title.*

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

8 *The United States Secret Service and the Federal Bu-*
9 *reau of Investigation shall report to Congress not later than*
10 *18 months after the date of enactment of this Act, and upon*
11 *the request by Congress thereafter, on—*

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

18 *(2) the number and nature of security breaches*
19 *subject to the national security and law enforcement*
20 *exemptions under section 212(a), provided that such*
21 *report may not disclose the contents of any risk as-*
22 *essment provided to the United States Secret Service*
23 *and the Federal Bureau of Investigation pursuant to*
24 *this subtitle.*

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

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

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

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

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

13 *(b) POST-BREACH TECHNICAL NOTIFICATION.—In any*
14 *instance where an agency or business entity is required to*
15 *notify the designated entity under section 217, the agency*
16 *or business entity shall also provide the designated entity*
17 *with technical information concerning the nature of the se-*
18 *curity breach, including—*

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

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

1 (3) *any other technical information concerning*
2 *the nature of the security breach deemed appropriate*
3 *for collection by the designated entity in furtherance*
4 *of this subtitle.*

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

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

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

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

24 (3) *may not be shared with any third party, in-*
25 *cluding other parties certified for access to the infor-*

1 *mation clearinghouse, without the express written*
2 *consent of the designated entity.*

3 *(e) RULEMAKING.—In consultation with the private*
4 *sector, appropriate representatives of State and local gov-*
5 *ernments, and other appropriate Federal agencies, the des-*
6 *ignated entity may issue such regulations as it determines*
7 *to be necessary to carry out this subtitle. All regulations*
8 *promulgated under this Act shall be issued in accordance*
9 *with section 553 of title 5, United States Code.*

10 **SEC. 231. PROTECTIONS FOR CLEARINGHOUSE PARTICI-**
11 **PANTS.**

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

18 *(b) ANONYMOUS DATA RELEASE.—To the extent fea-*
19 *sible, the designated entity shall ensure that all information*
20 *stored in the technical information clearinghouse and*
21 *accessed by certified parties is presented in a form that*
22 *minimizes the potential for such information to be traced*
23 *to a particular network, company, or security breach inci-*
24 *dent.*

1 (c) *PROTECTION FROM PUBLIC DISCLOSURE.—Except*
2 *as otherwise provided in this subtitle—*

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

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

13 (A) *does not prohibit the sharing of such in-*
14 *formation, as the designated entity determines to*
15 *be appropriate, in order to mitigate cybersecurity*
16 *threats or further the official functions of a*
17 *government agency; and*

18 (B) *does not authorized such information to*
19 *be withheld from a committee of Congress au-*
20 *thorized to request the information.*

21 (d) *PROTECTION OF CLASSIFIED INFORMATION.—*
22 *Nothing in this subtitle permits the unauthorized disclosure*
23 *of classified information.*

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

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

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

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

9 *(a) IN GENERAL.—In considering contract awards to-*
10 *taling more than \$500,000 and entered into after the date*
11 *of enactment of this Act with data brokers, the Adminis-*
12 *trator of the General Services Administration shall evalu-*
13 *ate—*

14 *(1) the data privacy and security program of a*
15 *data broker to ensure the privacy and security of data*
16 *containing sensitive personally identifiable informa-*
17 *tion, including whether such program adequately ad-*
18 *dresses privacy and security threats created by mali-*
19 *cious software or code, or the use of peer-to-peer file*
20 *sharing software;*

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

23 *(3) the extent to which the databases and systems*
24 *containing sensitive personally identifiable informa-*
25 *tion of a data broker have been compromised by secu-*
26 *rity breaches; and*

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

4 (b) *COMPLIANCE SAFE HARBOR.—The data privacy*
5 *and security program of a data broker shall be deemed suffi-*
6 *cient for the purposes of subsection (a), if the data broker*
7 *complies with or provides protection equal to industry*
8 *standards, as identified by the Federal Trade Commission,*
9 *that are applicable to the type of sensitive personally identi-*
10 *fiable information involved in the ordinary course of busi-*
11 *ness of such data broker.*

12 (c) *PENALTIES.—In awarding contracts with data*
13 *brokers for products or services related to access, use, com-*
14 *pilation, distribution, processing, analyzing, or evaluating*
15 *sensitive personally identifiable information, the Adminis-*
16 *trator of the General Services Administration shall—*

17 (1) *include monetary or other penalties—*

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

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

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

1 *sponsibilities related to sensitive personally identifi-*
2 *able information to—*

3 *(A) exercise appropriate due diligence in se-*
4 *lecting those service providers for responsibilities*
5 *related to sensitive personally identifiable infor-*
6 *mation;*

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

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

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

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

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

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

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

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

6 “(9) *procedures for evaluating and auditing the*
7 *information security practices of contractors or third*
8 *party business entities supporting the information*
9 *systems or operations of the agency involving sen-*
10 *sitive personally identifiable information (as that*
11 *term is defined in section 3 of the Personal Data Pro-*
12 *tection and Breach Accountability Act of 2011) and*
13 *ensuring remedial action to address any significant*
14 *deficiencies.”.*

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

19 (a) *IN GENERAL.*—*Section 208(b)(1) of the E-Govern-*
20 *ment Act of 2002 (44 U.S.C. 3501 note) is amended—*

21 (1) *in subparagraph (A)(i), by striking “or”;*

22 (2) *in subparagraph (A)(ii), by striking the pe-*
23 *riod and inserting “; or”; and*

24 (3) *by inserting after clause (ii) the following:*

1 “(iii) purchasing or subscribing for a
2 fee to sensitive personally identifiable infor-
3 mation from a data broker (as such terms
4 are defined in section 3 of the Personal
5 Data Protection and Breach Accountability
6 Act of 2011).”.

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

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

20 (A) such database;

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

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

24 (2) adopts regulations that specify—

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

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

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

10 (D) standards limiting the retention and re-
11 disclosure of sensitive personally identifiable in-
12 formation obtained from such databases;

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

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

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

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

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

5 (3) incorporates into the contract or other agree-
6 ment totaling more than \$500,000, provisions—

7 (A) providing for penalties—

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

10 (ii) if the entity knows or has reason
11 to know that the sensitive personally identi-
12 fiable information being provided to the
13 Federal department or agency is inaccurate,
14 and provides such inaccurate information;
15 and

16 (B) requiring a data broker that engages
17 service providers not subject to subtitle A of title
18 II for responsibilities related to sensitive person-
19 ally identifiable information to—

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

24 (ii) take reasonable steps to select and
25 retain service providers that are capable of

1 *maintaining appropriate safeguards for the*
2 *security, privacy, and integrity of the sen-*
3 *sitive personally identifiable information at*
4 *issue; and*

5 *(iii) require such service providers, by*
6 *contract, to implement and maintain ap-*
7 *propriate measures designed to meet the ob-*
8 *jectives and requirements in title II.*

9 *(c) LIMITATION ON PENALTIES.—The penalties under*
10 *subsection (b)(3)(A) shall not apply to a data broker pro-*
11 *viding information that is accurately and completely re-*
12 *corded from a public record source.*

13 *(d) STUDY OF GOVERNMENT USE.—*

14 *(1) SCOPE OF STUDY.—Not later than 180 days*
15 *after the date of enactment of this Act, the Comp-*
16 *troller General of the United States shall conduct a*
17 *study and audit and prepare a report on Federal*
18 *agency actions to address the recommendations in the*
19 *Government Accountability Office’s April 2006 report*
20 *on agency adherence to key privacy principles in*
21 *using data brokers or commercial databases con-*
22 *taining sensitive personally identifiable information.*

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

1 **SEC. 304. FBI REPORT ON REPORTED BREACHES AND COM-**
2 **PLIANCE.**

3 (a) *IN GENERAL.*—Not later than 1 year after the date
4 of enactment of this Act, and each year thereafter, the Fed-
5 eral Bureau of Investigation, in coordination with the Se-
6 cret Service, shall submit to the Committee on the Judiciary
7 of the Senate and the Committee on the Judiciary of the
8 House of Representatives a report regarding any reported
9 breaches at agencies or business entities during the pre-
10 ceding year.

11 (b) *REPORT CONTENT.*—Such reporting shall in-
12 clude—

13 (1) *the total instances of breaches of security in*
14 *the previous year;*

15 (2) *the percentage of breaches described in sub-*
16 *section (a) that occurred at an agency or business en-*
17 *tity that did not comply with the personal data pri-*
18 *vacv and security program under section 202; and*

19 (3) *recommendations, if any, for modifying or*
20 *amending this Act to increase its effectiveness.*

21 **SEC. 305. DEPARTMENT OF JUSTICE REPORT ON ENFORCE-**
22 **MENT ACTIONS.**

23 *Section 529 of title 28, United States Code, is amended*
24 *by adding at the end the following:*

25 “(c) *Not later than 1 year after the date of enactment*
26 *of the Personal Data Protection and Breach Accountability*

1 *Act of 2011, and every fiscal year thereafter, the Attorney*
2 *General shall submit to Congress a report on Federal en-*
3 *forcement actions, State attorneys general enforcement ac-*
4 *tions, and private enforcement actions, undertaken pursu-*
5 *ant to the Personal Data Protection and Breach Account-*
6 *ability Act of 2011 that shall include a description of the*
7 *best practices for enforcement of such Act as well as rec-*
8 *ommendations, if any, for modifying or amending this Act*
9 *to increase the effectiveness of such enforcement actions.”.*

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

11 *(a) IN GENERAL.—Not later than 1 year after the date*
12 *of enactment of this Act, and each year thereafter, the des-*
13 *ignated entity, in coordination with the Attorney General*
14 *and the Federal Trade Commission, shall submit to the*
15 *Committee on the Judiciary of the Senate and the Com-*
16 *mittee on the Judiciary of the House of Representatives a*
17 *report regarding the effectiveness of post-breach notification*
18 *practices by agencies and business entities.*

19 *(b) REPORT CONTENT.—The report required under*
20 *subsection (a) shall include—*

21 *(1) in each instance of a breach of security, the*
22 *amount of time between the instance of the breach*
23 *and the discovery of the breach by the affected busi-*
24 *ness entity;*

1 (2) *in each instance of a breach of security, the*
2 *amount of time between the discovery of the breach by*
3 *the affected business entity and the notification to the*
4 *FBI and Secret Service; and*

5 (3) *in each instance of a breach of security, the*
6 *amount of time between the discovery of the breach by*
7 *the affected business entity and the notification to in-*
8 *dividuals whose sensitive personally identifiable infor-*
9 *mation was compromised.*

10 ***TITLE IV—COMPLIANCE WITH***
11 ***STATUTORY PAY-AS-YOU-GO ACT***

12 ***SEC. 401. BUDGET COMPLIANCE.***

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

Calendar No. 182

112TH CONGRESS
1ST Session
S. 1535

A BILL

To protect consumers by mitigating the vulnerability of personally identifiable information to theft through a security breach, providing notice and remedies to consumers in the wake of such a breach, holding companies accountable for preventable breaches, facilitating the sharing of post-breach technical information between companies, and enhancing criminal and civil penalties and other protections against the unauthorized collection or use of personally identifiable information.

SEPTEMBER 22, 2011

Reported with an amendment