

Calendar No. 310

112TH CONGRESS
2^D SESSION

S. 1408

To require Federal agencies, and persons engaged in interstate commerce, in possession of data containing sensitive personally identifiable information, to disclose any breach of such information.

IN THE SENATE OF THE UNITED STATES

JULY 22, 2011

Mrs. FEINSTEIN introduced the following bill; which was read twice and referred to the Committee on the Judiciary

FEBRUARY 6, 2012

Reported by Mr. LEAHY, with an amendment

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

A BILL

To require Federal agencies, and persons engaged in interstate commerce, in possession of data containing sensitive personally identifiable information, to disclose any breach of such 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.**

4 ~~This Act may be cited as the “Data Breach Notifica-~~
5 ~~tion Act of 2011”.~~

1 **SEC. 2. NOTICE TO INDIVIDUALS.**

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

10 (b) OBLIGATION OF OWNER OR LICENSEE.—

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

19 (2) NOTICE BY OWNER, LICENSEE OR OTHER
20 DESIGNATED THIRD PARTY.—Nothing in this Act
21 shall prevent or abrogate an agreement between an
22 agency or business entity required to give notice
23 under this section and a designated third party, in-
24 cluding an owner or licensee of the sensitive person-
25 ally identifiable information subject to the security

1 breach, to provide the notifications required under
2 subsection (a).

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

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

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

15 ~~(2) REASONABLE DELAY.~~—Reasonable delay
16 under this subsection may include any time nec-
17 essary to determine the scope of the security breach,
18 prevent further disclosures, and restore the reason-
19 able integrity of the data system and provide notice
20 to law enforcement when required.

21 ~~(3) BURDEN OF PROOF.~~—The agency, business
22 entity, owner, or licensee required to provide notifi-
23 cation under this section shall have the burden of
24 demonstrating that all notifications were made as re-

1 required under this Act, including evidence dem-
2 onstrating the reasons for any delay.

3 ~~(d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW~~
4 ~~ENFORCEMENT PURPOSES.—~~

5 ~~(1) IN GENERAL.—~~If a Federal law enforce-
6 ment agency determines that the notification re-
7 quired under this section would impede a criminal
8 investigation, such notification shall be delayed upon
9 written notice from such Federal law enforcement
10 agency to the agency or business entity that experi-
11 enced the breach.

12 ~~(2) EXTENDED DELAY OF NOTIFICATION.—~~If
13 the notification required under subsection (a) is de-
14 layed pursuant to paragraph (1), an agency or busi-
15 ness entity shall give notice 30 days after the day
16 such law enforcement delay was invoked unless a
17 Federal law enforcement agency provides written no-
18 tification that further delay is necessary.

19 ~~(3) LAW ENFORCEMENT IMMUNITY.—~~No cause
20 of action shall lie in any court against any law en-
21 forcement agency for acts relating to the delay of
22 notification for law enforcement purposes under this
23 Act.

1 **SEC. 3. EXEMPTIONS.**

2 (a) ~~EXEMPTION FOR NATIONAL SECURITY AND LAW~~
3 ~~ENFORCEMENT.—~~

4 (1) ~~IN GENERAL.—~~Section 2 shall not apply to
5 an agency or business entity if the agency or busi-
6 ness entity certifies, in writing, that notification of
7 the security breach as required by section 2 reason-
8 ably could be expected to—

9 (A) ~~cause damage to the national security;~~

10 or

11 (B) ~~hinder a law enforcement investigation~~
12 ~~or the ability of the agency to conduct law en-~~
13 ~~forcement investigations.~~

14 (2) ~~LIMITS ON CERTIFICATIONS.—~~An agency or
15 business entity may not execute a certification under
16 paragraph (1) to—

17 (A) ~~conceal violations of law, inefficiency,~~
18 ~~or administrative error;~~

19 (B) ~~prevent embarrassment to a business~~
20 ~~entity, organization, or agency; or~~

21 (C) ~~restrain competition.~~

22 (3) ~~NOTICE.—~~In every case in which an agency
23 or business entity issues a certification under para-
24 graph (1), the certification, accompanied by a de-
25 scription of the factual basis for the certification,

1 shall be immediately provided to the United States
2 Secret Service.

3 (4) SECRET SERVICE REVIEW OF CERTIFI-
4 CATIONS.—

5 (A) IN GENERAL.—The United States Se-
6 cret Service may review a certification provided
7 by an agency under paragraph (3), and shall re-
8 view a certification provided by a business enti-
9 ty under paragraph (3), to determine whether
10 an exemption under paragraph (1) is merited.
11 Such review shall be completed not later than
12 10 business days after the date of receipt of the
13 certification, except as provided in paragraph
14 (5)(C).

15 (B) NOTICE.—Upon completing a review
16 under subparagraph (A) the United States Se-
17 cret Service shall immediately notify the agency
18 or business entity, in writing, of its determina-
19 tion of whether an exemption under paragraph
20 (1) is merited.

21 (C) EXEMPTION.—The exemption under
22 paragraph (1) shall not apply if the United
23 States Secret Service determines under this
24 paragraph that the exemption is not merited.

1 (5) ~~ADDITIONAL AUTHORITY OF THE SECRET~~
2 ~~SERVICE.—~~

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

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

15 (C) ~~TIMING.—~~If the United States Secret
16 Service requests additional information under
17 subparagraph (A), the United States Secret
18 Service shall notify the agency or business enti-
19 ty not later than 10 business days after the
20 date of receipt of the additional information
21 whether an exemption under paragraph (1) is
22 merited.

23 (b) ~~SAFE HARBOR.—~~

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

4 (A) a risk assessment concludes that there
5 is no significant risk that a security breach has
6 resulted in, or will result in, harm to the indi-
7 vidual whose sensitive personally identifiable in-
8 formation was subject to the security breach;

9 (B) without unreasonable delay, but not
10 later than 45 days after the discovery of a secu-
11 rity breach (unless extended by the United
12 States Secret Service); the agency or business
13 entity notifies the United States Secret Service,
14 in writing, of—

15 (i) the results of the risk assessment;

16 and

17 (ii) its decision to invoke the risk as-
18 sessment exemption; and

19 (C) the United States Secret Service does
20 not indicate, in writing, and not later than 10
21 business days after the date of receipt of the
22 decision described in subparagraph (B)(ii), that
23 notice should be given.

24 (2) ~~PRESUMPTIONS.~~—There shall be a pre-
25 sumption that no significant risk of harm to the in-

1 dividual whose sensitive personally identifiable infor-
 2 mation was subject to a security breach if such in-
 3 formation—

4 (A) was encrypted; or

5 (B) was rendered indecipherable through
 6 the use of best practices or methods, such as
 7 redaction, access controls, or other such mecha-
 8 nisms, that are widely accepted as an effective
 9 industry practice, or an effective industry
 10 standard.

11 (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

12 (1) IN GENERAL.—A business entity will be ex-
 13 empt from the notice requirement under section 2 if
 14 the business entity utilizes or participates in a secu-
 15 rity program that—

16 (A) is designed to block the use of the sen-
 17 sitive personally identifiable information to ini-
 18 tiate unauthorized financial transactions before
 19 they are charged to the account of the indi-
 20 vidual; and

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

24 (2) LIMITATION.—The exemption by this sub-
 25 section does not apply if—

1 (A) the information subject to the security
2 breach includes sensitive personally identifiable
3 information, other than a credit card number or
4 credit card security code, of any type; or

5 (B) the information subject to the security
6 breach includes both the individual's credit card
7 number and the individual's first and last
8 name.

9 **SEC. 4. METHODS OF NOTICE.**

10 An agency, or business entity shall be in compliance
11 with section 2 if it provides both:

12 (1) **INDIVIDUAL NOTICE.**—

13 (A) Written notification to the last known
14 home mailing address of the individual in the
15 records of the agency or business entity;

16 (B) telephone notice to the individual per-
17 sonally; or

18 (C) e-mail notice, if the individual has con-
19 sented to receive such notice and the notice is
20 consistent with the provisions permitting elec-
21 tronic transmission of notices under section 101
22 of the Electronic Signatures in Global and Na-
23 tional Commerce Act (15 U.S.C. 7001).

24 (2) **MEDIA NOTICE.**—Notice to major media
25 outlets serving a State or jurisdiction, if the number

1 of residents of such State whose sensitive personally
2 identifiable information was, or is reasonably be-
3 lieved to have been, acquired by an unauthorized
4 person exceeds 5,000.

5 **SEC. 5. CONTENT OF NOTIFICATION.**

6 (a) **IN GENERAL.**—Regardless of the method by
7 which notice is provided to individuals under section 4,
8 such notice shall include, to the extent possible—

9 (1) a description of the categories of sensitive
10 personally identifiable information that was, or is
11 reasonably believed to have been, acquired by an un-
12 authorized person;

13 (2) a toll-free number—

14 (A) that the individual may use to contact
15 the agency or business entity, or the agent of
16 the agency or business entity; and

17 (B) from which the individual may learn
18 what types of sensitive personally identifiable
19 information the agency or business entity main-
20 tained about that individual; and

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

23 (b) **ADDITIONAL CONTENT.**—Notwithstanding sec-
24 tion 10, a State may require that a notice under sub-

1 section (a) shall also include information regarding victim
2 protection assistance provided for by that State.

3 **SEC. 6. COORDINATION OF NOTIFICATION WITH CREDIT**
4 **REPORTING AGENCIES.**

5 If an agency or business entity is required to provide
6 notification to more than 5,000 individuals under section
7 2(a), the agency or business entity shall also notify all con-
8 sumer reporting agencies that compile and maintain files
9 on consumers on a nationwide basis (as defined in section
10 603(p) of the Fair Credit Reporting Act (15 U.S.C.
11 1681a(p))) of the timing and distribution of the notices.
12 Such notice shall be given to the consumer credit reporting
13 agencies without unreasonable delay and, if it will not
14 delay notice to the affected individuals, prior to the dis-
15 tribution of notices to the affected individuals.

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

17 (a) SECRET SERVICE.—Any business entity or agen-
18 cy shall notify the United States Secret Service of the fact
19 that a security breach has occurred if—

20 (1) the number of individuals whose sensitive
21 personally identifying information was, or is reason-
22 ably believed to have been acquired by an unauthor-
23 ized person exceeds 10,000;

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

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

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

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

12 (b) NOTICE TO OTHER LAW ENFORCEMENT AGEN-
13 CIES.—The United States Secret Service shall be respon-
14 sible for notifying—

15 (1) the Federal Bureau of Investigation, if the
16 security breach involves espionage, foreign counter-
17 intelligence, information protected against unauthor-
18 ized disclosure for reasons of national defense or for-
19 eign relations, or Restricted Data (as that term is
20 defined in section 11y of the Atomic Energy Act of
21 1954 (42 U.S.C. 2014(y))), except for offenses af-
22 fecting the duties of the United States Secret Serv-
23 ice under section 3056(a) of title 18, United States
24 Code;

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

3 (3) the attorney general of each State affected
4 by the security breach.

5 (e) **TIMING OF NOTICES.**—The notices required
6 under this section shall be delivered as follows:

7 (1) Notice under subsection (a) shall be deliv-
8 ered as promptly as possible, but not later than 14
9 days after discovery of the events requiring notice.

10 (2) Notice under subsection (b) shall be deliv-
11 ered not later than 14 days after the United States
12 Secret Service receives notice of a security breach
13 from an agency or business entity.

14 **SEC. 8. ENFORCEMENT.**

15 (a) **CIVIL ACTIONS BY THE ATTORNEY GENERAL.**—

16 The Attorney General may bring a civil action in the ap-
17 propriate United States district court against any business
18 entity that engages in conduct constituting a violation of
19 this Act and, upon proof of such conduct by a preponder-
20 ance of the evidence, such business entity shall be subject
21 to a civil penalty of not more than \$1,000 per day per
22 individual whose sensitive personally identifiable informa-
23 tion was, or is reasonably believed to have been, accessed
24 or acquired by an unauthorized person, up to a maximum

1 of \$1,000,000 per violation, unless such conduct is found
2 to be willful or intentional.

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

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

10 (A) enjoining such act or practice; or

11 (B) enforcing compliance with this Act.

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

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

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

1 **SEC. 9. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

2 (a) IN GENERAL.—

3 (1) CIVIL ACTIONS.—In any case in which the
4 attorney general of a State or any State or local law
5 enforcement agency authorized by the State attorney
6 general or by State statute to prosecute violations of
7 consumer protection law, has reason to believe that
8 an interest of the residents of that State has been
9 or is threatened or adversely affected by the engage-
10 ment of a business entity in a practice that is pro-
11 hibited under this Act, the State or the State or
12 local law enforcement agency on behalf of the resi-
13 dents of the agency's jurisdiction, may bring a civil
14 action on behalf of the residents of the State or ju-
15 risdiction in a district court of the United States of
16 appropriate jurisdiction or any other court of com-
17 petent jurisdiction, including a State court, to—

18 (A) enjoin that practice;

19 (B) enforce compliance with this Act; or

20 (C) obtain civil penalties of not more than
21 \$1,000 per day per individual whose sensitive
22 personally identifiable information was, or is
23 reasonably believed to have been, accessed or
24 acquired by an unauthorized person, up to a
25 maximum of \$1,000,000 per violation, unless

1 such conduct is found to be willful or inten-
2 tional.

3 (2) NOTICE.—

4 (A) IN GENERAL.—Before filing an action
5 under paragraph (1), the attorney general of
6 the State involved shall provide to the Attorney
7 General of the United States—

8 (i) written notice of the action; and

9 (ii) a copy of the complaint for the ac-
10 tion.

11 (B) EXEMPTION.—

12 (i) IN GENERAL.—Subparagraph (A)
13 shall not apply with respect to the filing of
14 an action by an attorney general of a State
15 under this Act, if the State attorney gen-
16 eral determines that it is not feasible to
17 provide the notice described in such sub-
18 paragraph before the filing of the action.

19 (ii) NOTIFICATION.—In an action de-
20 scribed in clause (i), the attorney general
21 of a State shall provide notice and a copy
22 of the complaint to the Attorney General
23 at the time the State attorney general files
24 the action.

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

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

7 (2) initiate an action in the appropriate United
8 States district court under section 8 and move to
9 consolidate all pending actions, including State ac-
10 tions, in such court;

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

13 (4) file petitions for appeal.

14 (c) PENDING PROCEEDINGS.—If the Attorney Gen-
15 eral has instituted a proceeding or action for a violation
16 of this Act or any regulations thereunder, no attorney gen-
17 eral of a State may, during the pendency of such pro-
18 ceeding or action, bring an action under this Act against
19 any defendant named in such criminal proceeding or civil
20 action for any violation that is alleged in that proceeding
21 or action.

22 (d) RULE OF CONSTRUCTION.—For purposes of
23 bringing any civil action under subsection (a), nothing in
24 this Act regarding notification shall be construed to pre-
25 vent an attorney general of a State from exercising the

1 powers conferred on such attorney general by the laws of
2 that State to—

- 3 (1) conduct investigations;
- 4 (2) administer oaths or affirmations; or
- 5 (3) compel the attendance of witnesses or the
6 production of documentary and other evidence.

7 (e) VENUE; SERVICE OF PROCESS.—

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

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

14 (B) another court of competent jurisdic-
15 tion.

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

19 (A) is an inhabitant; or

20 (B) may be found.

21 (f) NO PRIVATE CAUSE OF ACTION.—Nothing in this
22 Act establishes a private cause of action against a business
23 entity for violation of any provision of this Act.

1 **SEC. 10. EFFECT ON FEDERAL AND STATE LAW.**

2 The provisions of this Act shall supersede any other
3 provision of Federal law or any provision of law of any
4 State relating to notification by a business entity engaged
5 in interstate commerce or an agency of a security breach,
6 except as provided in section 5(b).

7 **SEC. 11. AUTHORIZATION OF APPROPRIATIONS.**

8 There are authorized to be appropriated such sums
9 as may be necessary to cover the costs incurred by the
10 United States Secret Service to carry out investigations
11 and risk assessments of security breaches as required
12 under this Act.

13 **SEC. 12. REPORTING ON RISK ASSESSMENT EXEMPTIONS.**

14 (a) IN GENERAL.—The United States Secret Service
15 shall report to Congress not later than 18 months after
16 the date of enactment of this Act, and upon the request
17 by Congress thereafter, on—

18 (1) the number and nature of the security
19 breaches described in the notices filed by those busi-
20 ness entities invoking the risk assessment exemption
21 under section 3(b) of this Act and the response of
22 the United States Secret Service to such notices;
23 and

24 (2) the number and nature of security breaches
25 subject to the national security and law enforcement
26 exemptions under section 3(a) of this Act.

1 (b) REPORT.—Any report submitted under sub-
 2 section (a) shall not disclose the contents of any risk as-
 3 sessment provided to the United States Secret Service
 4 under this Act.

5 **SEC. 13. DEFINITIONS.**

6 In this Act, the following definitions shall apply:

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

10 (2) AFFILIATE.—The term “affiliate” means
 11 persons related by common ownership or by cor-
 12 porate control.

13 (3) BUSINESS ENTITY.—The term “business
 14 entity” means any organization, corporation, trust,
 15 partnership, sole proprietorship, unincorporated as-
 16 sociation, venture established to make a profit, or
 17 nonprofit, and any contractor, subcontractor, affil-
 18 iate, or licensee thereof engaged in interstate com-
 19 merce.

20 (4) ENCRYPTED.—The term “encrypted”—

21 (A) means the protection of data in elec-
 22 tronic form, in storage or in transit, using an
 23 encryption technology that has been adopted by
 24 an established standards setting body which
 25 renders such data indecipherable in the absence

1 of associated cryptographic keys necessary to
 2 enable decryption of such data; and

3 (B) includes appropriate management and
 4 safeguards of such cryptographic keys so as to
 5 protect the integrity of the encryption.

6 (5) PERSONALLY IDENTIFIABLE INFORMA-
 7 TION.—The term “personally identifiable informa-
 8 tion” means any information, or compilation of in-
 9 formation, in electronic or digital form serving as a
 10 means of identification, as defined by section
 11 1028(d)(7) of title 18, United State Code.

12 (6) 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 that result
 17 in, or there is a reasonable basis to conclude
 18 has resulted in, acquisition of or access to sen-
 19 sitive personally identifiable information that is
 20 unauthorized or in excess of authorization.

21 (B) EXCLUSION.—The term “security
 22 breach” does not include—

23 (i) a good faith acquisition of sensitive
 24 personally identifiable information by a
 25 business entity or agency, or an employee

1 or agent of a business entity or agency, if
 2 the sensitive personally identifiable infor-
 3 mation is not subject to further unauthor-
 4 ized disclosure; or

5 (ii) the release of a public record not
 6 otherwise subject to confidentiality or non-
 7 disclosure requirements.

8 (7) 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 non-truncated 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 or telephone
 21 number.

22 (II) Mother’s maiden name, if
 23 identified as such.

24 (III) Month, day, and year of
 25 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 that is required for an individual to
10 obtain money, goods, services or any other
11 thing of value; or

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.

18 **SEC. 14. EFFECTIVE DATE.**

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

22 **SECTION 1. SHORT TITLE.**

23 *This Act may be cited as the Data Breach Notification*
24 *Act of 2011.*

1 **SEC. 2. NOTICE TO INDIVIDUALS.**

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

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

11 (1) *NOTICE TO OWNER OR LICENSEE.*—Any
12 agency, or business entity engaged in interstate com-
13 merce, that uses, accesses, transmits, stores, disposes
14 of, or collects sensitive personally identifiable infor-
15 mation that the agency or business entity does not
16 own or license shall notify the owner or licensee of the
17 information following the discovery of a security
18 breach involving such information.

19 (2) *NOTICE BY OWNER, LICENSEE OR OTHER*
20 *DESIGNATED THIRD PARTY.*—Nothing in this Act
21 shall prevent or abrogate an agreement between an
22 agency or business entity required to give notice
23 under this section and a designated third party, in-
24 cluding an owner or licensee of the sensitive person-
25 ally identifiable information subject to the security

1 breach, to provide the notifications required under
2 subsection (a).

3 (3) *BUSINESS ENTITY RELIEVED FROM GIVING*
4 *NOTICE.*—A business entity obligated to give notice
5 under subsection (a) shall be relieved of such obliga-
6 tion if an owner or licensee of the sensitive personally
7 identifiable information subject to the security breach,
8 or other designated third party, provides such notifi-
9 cation.

10 (c) *TIMELINESS OF NOTIFICATION.*—

11 (1) *IN GENERAL.*—All notifications required
12 under this section shall be made without unreasonable
13 delay following the discovery by the agency or busi-
14 ness entity of a security breach.

15 (2) *REASONABLE DELAY.*—

16 (A) *IN GENERAL.*—Reasonable delay under
17 this subsection may include any time necessary
18 to determine the scope of the security breach, pre-
19 vent further disclosures, conduct the risk assess-
20 ment described in section 3(b)(1), and restore the
21 reasonable integrity of the data system and pro-
22 vide notice to law enforcement when required.

23 (B) *EXCEPTION.*—

24 (i) *IN GENERAL.*—Except as provided
25 in section 3, delay of notification shall not

1 *exceed 60 days following the discovery of the*
2 *security breach, unless—*

3 *(I) the business entity or agency*
4 *requests an extension of time from the*
5 *Federal Trade Commission; and*

6 *(II) the Federal Trade Commis-*
7 *sion determines that the additional*
8 *time requested under subclause (II) is*
9 *reasonably necessary.*

10 *(ii) ADDITIONAL TIME.—If a request*
11 *for delay is approved under clause (i), the*
12 *agency or business entity that requested the*
13 *delay may delay the time period for notifi-*
14 *cation for an additional period of 30 days.*
15 *Successive requests for delay are not prohib-*
16 *ited.*

17 *(3) BURDEN OF PROOF.—The agency, business*
18 *entity, owner, or licensee required to provide notifica-*
19 *tion under this section shall have the burden of dem-*
20 *onstrating that all notifications were made as re-*
21 *quired under this Act, including evidence dem-*
22 *onstrating the reasons for any delay.*

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

1 (1) *IN GENERAL.*—*If the United States Secret*
2 *Service or the Federal Bureau of Investigation deter-*
3 *mines that a notification required under this section*
4 *would impede a criminal investigation, or national*
5 *security activity, such notification shall be delayed*
6 *upon written notice from the United States Secret*
7 *Service or the Federal Bureau of Investigation to the*
8 *agency or business entity that experienced the security*
9 *breach. The notification from the United States Secret*
10 *Service or the Federal Bureau of Investigation shall*
11 *specify in writing the period of delay requested for*
12 *law enforcement or national security purposes.*

13 (2) *EXTENDED DELAY OF NOTIFICATION.*—

14 (A) *IN GENERAL.*—*If the notification re-*
15 *quired under subsection (a) is delayed pursuant*
16 *to paragraph (1), an agency or business entity*
17 *shall give notice 30 days after the day such law*
18 *enforcement delay was invoked unless a Federal*
19 *law enforcement or intelligence agency provides*
20 *written notification that further delay is nec-*
21 *essary.*

22 (B) *WRITTEN JUSTIFICATION REQUIRE-*
23 *MENTS.*—

24 (i) *UNITED STATES SECRET SERV-*
25 *ICE.*—*If the United States Secret Service*

1 *instructs the agency or business entity to*
2 *delay notification under this section longer*
3 *than 30 days, the United States Secret*
4 *Service shall submit written justification*
5 *for such delay to the Secretary of Homeland*
6 *Security before such delay takes place.*

7 *(ii) FEDERAL BUREAU OF INVESTIGA-*
8 *TION.—If the Federal Bureau of Investiga-*
9 *tion instructs the agency or business entity*
10 *to delay notification under this section*
11 *longer than 30 days, the Federal Bureau of*
12 *Investigation shall submit written justifica-*
13 *tion for such delay to the Attorney General*
14 *before such delay takes place.*

15 (3) *LAW ENFORCEMENT IMMUNITY.—No cause of*
16 *action shall lie in any court against any agency for*
17 *acts relating to the delay of notification for law en-*
18 *forcement or national security purposes under this*
19 *Act.*

20 **SEC. 3. EXEMPTIONS.**

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

23 (1) *IN GENERAL.—Section 2 shall not apply to*
24 *an agency or business entity if—*

1 (A) *the United States Secret Service or the*
2 *Federal Bureau of Investigation determines that*
3 *notification of the security breach could be ex-*
4 *pected to reveal sensitive sources and methods or*
5 *similarly impede the ability of the Government*
6 *to conduct law enforcement or intelligence inves-*
7 *tigations; or*

8 (B) *the Federal Bureau of Investigation de-*
9 *termines that notification of the security breach*
10 *could be expected to cause damage to the na-*
11 *tional security.*

12 (2) *WRITTEN JUSTIFICATION REQUIREMENTS.—*

13 (A) *UNITED STATES SECRET SERVICE.—If*
14 *the United States Secret Service invokes the ex-*
15 *emption in this section, the United States Secret*
16 *Service shall submit written justification for*
17 *such exemption to the Secretary of Homeland Se-*
18 *curity before such exemption is invoked.*

19 (B) *FEDERAL BUREAU OF INVESTIGA-*
20 *TION.—If the Federal Bureau of Investigation*
21 *invokes the exemption in this section, the Federal*
22 *Bureau of Investigation shall submit written jus-*
23 *tification for such exemption to the Attorney*
24 *General before such exemption is invoked.*

1 (3) *IMMUNITY.*—No cause of action shall lie in
2 any court against any Federal agency for acts relat-
3 ing to the exemption from notification for law en-
4 forcement or national security purposes under this
5 title.

6 (b) *SAFE HARBOR.*—

7 (1) *IN GENERAL.*—An agency or business entity
8 shall be exempt from the notice requirements under
9 section 2, if—

10 (A) a risk assessment concludes that there is
11 no significant risk that a security breach has re-
12 sulted in, or will result in, identity theft, eco-
13 nomic loss or harm, or physical harm to the in-
14 dividuals whose sensitive personally identifiable
15 information was subject to the security breach;

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

22 (i) the results of the risk assessment;

23 and

24 (ii) its decision to invoke the risk as-
25 sessment exemption; and

1 (C) the Federal Trade Commission does not
2 indicate, in writing, and not later than 10 busi-
3 ness days after the date of receipt of the decision
4 described in subparagraph (B)(ii), that notice
5 should be given.

6 (2) *PRESUMPTIONS.*—There shall be a presump-
7 tion that no significant risk of harm to the individual
8 whose sensitive personally identifiable information
9 was subject to a security breach if such information—

10 (A) was encrypted; or

11 (B) was otherwise rendered unusable,
12 unreadable, or indecipherable through the use of
13 data security technology that is generally accept-
14 ed by experts in the field of information security
15 as an effective information security practice.

16 (c) *FINANCIAL FRAUD PREVENTION EXEMPTION.*—

17 (1) *IN GENERAL.*—A business entity will be ex-
18 empt from the notice requirement under section 2 if
19 the business entity utilizes or participates in a secu-
20 rity program that—

21 (A) effectively blocks the use of the sensitive
22 personally identifiable information to initiate
23 unauthorized financial transactions before they
24 are charged to the account of the individual; and

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

4 (2) *LIMITATION.*—*The exemption by this sub-*
 5 *section does not apply if—*

6 (A) the information subject to the security
 7 breach includes sensitive personally identifiable
 8 information, other than a credit card number or
 9 credit card security code, of any type; or

10 (B) the information subject to the security
 11 breach includes both the individual’s credit card
 12 number and the individual’s first and last name.

13 (d) *LIMITATIONS.*—

14 (1) *DEFINITIONS.*—*In this subsection—*

15 (A) the term “covered financial institution”
 16 means a financial institution that is subject to—

17 (i) the data security requirements of
 18 the Gramm-Leach-Bliley Act (15 U.S.C.
 19 6801 et seq.);

20 (ii) any implementing regulations
 21 issued under that Act; and

22 (iii) the jurisdiction of a Federal func-
 23 tional regulator under that Act; and

24 (B) the terms “Federal functional regu-
 25 lator” and “financial institution” have the

1 *meaning given those terms in section 509 of the*
 2 *Gramm-Leach-Bliley Act (15 U.S.C. 6809).*

3 (2) *FINANCIAL INSTITUTIONS REGULATED BY*
 4 *FEDERAL FUNCTIONAL REGULATORS.—Nothing in*
 5 *this Act shall apply to a covered financial institution*
 6 *if the Federal functional regulator with jurisdiction*
 7 *over the covered financial institution has issued a*
 8 *regulation under title V of the Gramm-Leach-Bliley*
 9 *Act (15 U.S.C. 6801 et seq.) that—*

10 (A) *requires financial institutions within*
 11 *its jurisdiction to provide notification to indi-*
 12 *viduals following a breach of security; and*

13 (B) *provides protections substantially simi-*
 14 *lar to, or greater than, those required under this*
 15 *Act.*

16 **SEC. 4. METHODS OF NOTICE.**

17 *An agency or business entity shall be in compliance*
 18 *with section 2 if it provides both:*

19 (1) *INDIVIDUAL NOTICE.—*

20 (A) *Written notification to the last known*
 21 *home mailing address of the individual in the*
 22 *records of the agency or business entity;*

23 (B) *telephone notice to the individual per-*
 24 *sonally; or*

1 (C) e-mail notice, if the individual has con-
 2 sented to receive such notice and the notice is
 3 consistent with the provisions permitting elec-
 4 tronic transmission of notices under section 101
 5 of the *Electronic Signatures in Global and Na-*
 6 *tional Commerce Act (15 U.S.C. 7001).*

7 (2) *MEDIA NOTICE.*—Notice to major media out-
 8 lets serving a State or jurisdiction, if the number of
 9 residents of such State whose sensitive personally
 10 identifiable information was, or is reasonably believed
 11 to have been, acquired by an unauthorized person ex-
 12 ceeds 5,000.

13 **SEC. 5. CONTENT OF NOTIFICATION.**

14 (a) *IN GENERAL.*—Regardless of the method by which
 15 notice is provided to individuals under section 4, such no-
 16 tice shall include, to the extent possible—

17 (1) a description of the categories of sensitive
 18 personally identifiable information that was, or is
 19 reasonably believed to have been, acquired by an un-
 20 authorized person;

21 (2) a toll-free number—

22 (A) that the individual may use to contact
 23 the agency or business entity, or the agent of the
 24 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
5 (3) the toll-free contact telephone numbers and
6 addresses for the major credit reporting agencies.

7 (b) *ADDITIONAL CONTENT.*—Notwithstanding section
8 11, a State may require that a notice under subsection (a)
9 shall also include information regarding victim protection
10 assistance provided for by that State.

11 **SEC. 6. COORDINATION OF NOTIFICATION WITH CREDIT**
12 **REPORTING AGENCIES.**

13 If an agency or business entity is required to provide
14 notification to more than 5,000 individuals under section
15 2(a), the agency or business entity shall also notify all con-
16 sumer reporting agencies that compile and maintain files
17 on consumers on a nationwide basis (as defined in section
18 603(p) of the Fair Credit Reporting Act (15 U.S.C.
19 1681a(p)) of the timing and distribution of the notices.
20 Such notice shall be given to the consumer credit reporting
21 agencies without unreasonable delay and, if it will not
22 delay notice to the affected individuals, prior to the dis-
23 tribution of notices to the affected individuals.

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

2 (a) *DESIGNATION OF GOVERNMENT ENTITY TO RE-*
3 *CEIVE NOTICE.—*

4 (1) *IN GENERAL.—Not later than 60 days after*
5 *the date of enactment of this Act, the Secretary of the*
6 *Department of Homeland Security shall designate a*
7 *Federal Government entity to receive the notices re-*
8 *quired under this section.*

9 (2) *RESPONSIBILITIES OF THE DESIGNATED EN-*
10 *TITY.—The designated entity shall promptly provide*
11 *the notices and other information it receives under*
12 *this section to—*

13 (A) *the United States Secret Service;*

14 (B) *the Federal Bureau of Investigation;*

15 (C) *the Federal Trade Commission;*

16 (D) *the United States Postal Inspection*
17 *Service, if the security breach involves mail*
18 *fraud;*

19 (E) *the attorney general of each State af-*
20 *ected by the security breach; and*

21 (F) *as appropriate, to other Federal agen-*
22 *cies for law enforcement, national security, or*
23 *data security purposes.*

24 (b) *NOTICE.—Any business entity or agency shall no-*
25 *tify the designated entity of the fact that a security breach*
26 *has occurred if—*

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

5 (2) *the security breach involves a database,*
6 *networked or integrated databases, or other data sys-*
7 *tem containing the sensitive personally identifiable*
8 *information of more than 1,000,000 individuals na-*
9 *tionwide;*

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

12 (4) *the security breach involves primarily sen-*
13 *sitive personally identifiable information of individ-*
14 *uals known to the agency or business entity to be em-*
15 *ployees or contractors of the Federal Government in-*
16 *volved in national security or law enforcement.*

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

19 (1) *Notice under subsection (b) shall be delivered*
20 *as promptly as possible, but must occur not more*
21 *than 72 hours before notification of an individual*
22 *pursuant to section 2, or within 10 days after dis-*
23 *covery of the events requiring notice, whichever occurs*
24 *first.*

1 (2) *Notice under subsection (a)(2) shall be deliv-*
2 *ered as promptly as possible after the designated enti-*
3 *ty receives notice of a security breach from an agency*
4 *or business entity.*

5 **SEC. 8. ENFORCEMENT.**

6 (a) *CIVIL ACTIONS BY THE ATTORNEY GENERAL.—The*
7 *Attorney General may bring a civil action in the appro-*
8 *priate United States district court against any business en-*
9 *tity that engages in conduct constituting a violation of this*
10 *Act and, upon proof of such conduct by a preponderance*
11 *of the evidence, such business entity shall be subject to a*
12 *civil penalty of not more than \$11,000 per day per security*
13 *breach.*

14 (b) *PENALTY LIMITATIONS.—*

15 (1) *IN GENERAL.—Notwithstanding any other*
16 *provision of law, the total amount of the civil penalty*
17 *assessed against a business entity for conduct involv-*
18 *ing the same or related acts or omissions that results*
19 *in a violation of this Act may not exceed \$1,000,000,*
20 *unless the violation was willful or intentional.*

21 (2) *WILLFUL OR INTENTIONAL VIOLATION.—If a*
22 *violation of this Act is found to be willful or inten-*
23 *tional, an additional civil penalty up to a maximum*
24 *of \$1,000,000 may be imposed.*

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

3 (1) *IN GENERAL.—If it appears that a business*
4 *entity has engaged, or is engaged, in any act or prac-*
5 *tice constituting a violation of this Act, the Attorney*
6 *General may petition an appropriate district court of*
7 *the United States for an order—*

8 (A) *enjoining such act or practice; or*

9 (B) *enforcing compliance with this Act.*

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

13 (d) *OTHER RIGHTS AND REMEDIES.—The rights and*
14 *remedies available under this Act are cumulative and shall*
15 *not affect any other rights and remedies available under*
16 *law.*

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

22 **SEC. 9. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

23 (a) *IN GENERAL.—*

24 (1) *CIVIL ACTIONS.—In any case in which the*
25 *attorney general of a State or any State or local law*

1 enforcement agency authorized by the State attorney
2 general or by State statute to prosecute violations of
3 State consumer protection law, has reason to believe
4 that an interest of the residents of that State has been
5 or is threatened or adversely affected by the engage-
6 ment of a business entity in a practice that con-
7 stitutes a violation of this Act, the State or the State
8 or local law enforcement agency on behalf of the resi-
9 dents of the agency's jurisdiction, may bring a civil
10 action on behalf of the residents of the State or juris-
11 diction in a district court of the United States of ap-
12 propriate jurisdiction or any other court of competent
13 jurisdiction, including a State court, to—

14 (A) enjoin that practice;

15 (B) enforce compliance with this Act; or

16 (C) obtain civil penalties of not more than
17 \$11,000 per day per security breach.

18 (2) *OVERALL MAXIMUM PENALTY FOR ACTIONS*
19 *BROUGHT BY STATE ATTORNEYS GENERAL.—*

20 (A) *IN GENERAL.—If more than 1 civil ac-*
21 *tion is brought against a business entity under*
22 *this section and the civil actions all arose out of*
23 *the same security breach—*

24 (i) *the business entity may file a mo-*
25 *tion, in any United States district court for*

1 *the district in which not less than 1 of the*
2 *civil actions brought under this section is*
3 *pending, to consolidate the civil actions in*
4 *such United States district court;*

5 *(ii) the United States district court in*
6 *which a motion is filed under clause (i)*
7 *shall order that the civil actions be consoli-*
8 *dated before such court; and*

9 *(iii) any civil action subsequently*
10 *brought against the business entity under*
11 *this section that arises out of the same secu-*
12 *rity breach at issue in the consolidated ac-*
13 *tions shall be consolidated with the consoli-*
14 *dated actions.*

15 *(B) TRANSFER OF VENUE.—If a United*
16 *States district court issues an order described in*
17 *subparagraph (A)(ii), such court may, at any-*
18 *time after the order is issued, consider whether*
19 *the consolidated actions should be transferred to*
20 *another district for the convenience of the parties*
21 *and witnesses, in interest of justice.*

22 *(C) PENALTY LIMITATIONS.—*

23 *(i) IN GENERAL.—Notwithstanding*
24 *any other provision of law, the total*
25 *amount of the civil penalty assessed against*

1 *a business entity for conduct involving the*
2 *same or related acts or omissions that re-*
3 *sults in a violation of this Act may not ex-*
4 *ceed \$1,000,000, unless the violation was*
5 *willful or intentional.*

6 *(ii) WILLFUL OR INTENTIONAL VIOLA-*
7 *TION.—If a violation of this Act is found to*
8 *be willful or intentional, an additional civil*
9 *penalty up to a maximum of \$1,000,000*
10 *may be imposed.*

11 (3) NOTICE.—

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

16 (i) *written notice of the action; and*

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

19 (B) EXEMPTION.—

20 (i) IN GENERAL.—*Subparagraph (A)*
21 *shall not apply with respect to the filing of*
22 *an action by an attorney general of a State*
23 *under this Act, if the State attorney general*
24 *determines that it is not feasible to provide*

1 the notice described in such subparagraph
2 before the filing of the action.

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

9 (b) *FEDERAL PROCEEDINGS.*—Upon receiving notice
10 under subsection (a)(3), the Attorney General shall have the
11 right to—

12 (1) move to stay the action, pending the final
13 disposition of a pending Federal proceeding or action;

14 (2) initiate an action in the appropriate United
15 States district court under section 8 and move to con-
16 solidate all pending actions, including State actions,
17 in such court;

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

20 (4) file petitions for appeal.

21 (c) *PENDING PROCEEDINGS.*—If the Attorney General
22 has initiated a criminal proceeding or civil action for a
23 violation of this Act, no attorney general of a State or any
24 State or local law enforcement agency authorized by the
25 State attorney general or by State statute to prosecute vio-

1 *lations of State consumer protection law may bring an ac-*
 2 *tion for a violation of a provision of this Act against a*
 3 *defendant named in the Federal criminal proceeding or*
 4 *civil action.*

5 *(d) RULE OF CONSTRUCTION.—For purposes of bring-*
 6 *ing any civil action under subsection (a), nothing in this*
 7 *Act regarding notification shall be construed to prevent an*
 8 *attorney general of a State from exercising the powers con-*
 9 *ferred on such attorney general by the laws of that State*
 10 *to—*

11 *(1) conduct investigations;*

12 *(2) administer oaths or affirmations; or*

13 *(3) compel the attendance of witnesses or the*
 14 *production of documentary and other evidence.*

15 *(e) VENUE; SERVICE OF PROCESS.—*

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

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

22 *(B) another court of competent jurisdiction.*

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

1 (A) is an inhabitant; or

2 (B) may be found.

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

6 **SEC. 10. CONCEALMENT OF SECURITY BREACH INVOLVING**
7 ***SENSITIVE PERSONALLY IDENTIFIABLE IN-***
8 ***FORMATION.***

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

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

14 “(a) *IN GENERAL.*—Any person who, having knowl-
15 *edge* of a security breach and of the fact that notice of such
16 *security breach* is required under the *Data Breach Notifica-*
17 *tion Act* of 2011, intentionally and willfully conceals the
18 *fact* of such security breach, shall, in the event that such
19 *security breach* results in economic harm to any individual
20 *in the amount* of \$1,000 or more, be fined under this title,
21 *imprisoned* for not more than 5 years, or both.

22 “(b) *PERSON DEFINED.*—For purposes of subsection
23 (a), the term ‘person’ has the same meaning as in section
24 1030(a)(12) of title 18, United States Code.

1 “(c) *NOTICE REQUIREMENT.*—Any persons seeking an
 2 exemption under section 3(b) of the Data Breach Notifica-
 3 tion Act of 2011 shall be immune from prosecution under
 4 this section if the Federal Trade Commission does not indi-
 5 cate, in writing, that notice be given under such Act.

6 “(d) *ENFORCEMENT AUTHORITY.*—

7 “(1) *IN GENERAL.*—The United States Secret
 8 Service and the Federal Bureau of Investigation shall
 9 have the authority to investigate offenses under this
 10 section.

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

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

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

17 **SEC. 11. EFFECT ON FEDERAL AND STATE LAW.**

18 “(a) *IN GENERAL.*—The provisions of this Act shall su-
 19 percede any other provision of Federal law or any provision
 20 of law of any State relating to notification by a business
 21 entity engaged in interstate commerce or an agency of a
 22 security breach, except as provided in section 5(b).

23 “(b) *LIMITATIONS.*—

1 (1) *GRAMM-LEACH-BLILEY ACT.*—*Nothing in*
2 *this Act shall supersede the data security require-*
3 *ments of the Gramm-Leach-Bliley Act (15 U.S.C.*
4 *6801 et seq.), or implementing regulations issued*
5 *under that Act.*

6 (2) *HEALTH PRIVACY.*—

7 (A) *To the extent that a business entity acts*
8 *as a covered entity or a business associate under*
9 *the Health Information Technology for Economic*
10 *and Clinical Health Act (42 U.S.C. 17932), and*
11 *has the obligation to provide breach notification*
12 *under that Act or its implementing regulations,*
13 *the requirements of this Act shall not apply;*

14 (B) *To the extent that a business entity acts*
15 *as a vendor of personal health records, a third*
16 *party service provider, or other entity subject to*
17 *the Health Information Technology for Economi-*
18 *cal and Clinical Health Act (42 U.S.C. 17937),*
19 *and has the obligation to provide breach notifica-*
20 *tion under that Act or its implementing regula-*
21 *tions, the requirements of this Act shall not*
22 *apply.*

23 **SEC. 12. AUTHORIZATION OF APPROPRIATIONS.**

24 *There are authorized to be appropriated such sums as*
25 *may be necessary to cover the costs incurred by agencies*

1 *to carry out investigations, risk assessments, and civil ac-*
2 *tions relating to security breaches under this Act.*

3 **SEC. 13. REPORTING ON EXEMPTIONS.**

4 *(a) FTC REPORTS.—*

5 *(1) IN GENERAL.—Not later than 18 months*
6 *after the date of enactment of this Act, and upon the*
7 *request by Congress thereafter, the Federal Trade*
8 *Commission shall submit to Congress a report on the*
9 *number and nature of the security breaches described*
10 *in the notices filed by those business entities invoking*
11 *the risk assessment exemption under section 3(b) of*
12 *this Act and the response of the Federal Trade Com-*
13 *mission to such notices.*

14 *(2) PROHIBITED DISCLOSURE.—Any report sub-*
15 *mitted under paragraph (1) shall not disclose the con-*
16 *tents of any risk assessment provided to the Federal*
17 *Trade Commission under this Act.*

18 *(b) LAW ENFORCEMENT REPORTS.—Not later than 18*
19 *months after the date of enactment of this Act, and upon*
20 *request by Congress thereafter, the United States Secret*
21 *Service and Federal Bureau of Investigation shall submit*
22 *to Congress a report on the number and nature of security*
23 *breaches subject to the national security and law enforce-*
24 *ment exemptions under section 3(a) of this Act.*

1 **SEC. 14. DEFINITIONS.**

2 *In this Act, the following definitions shall apply:*

3 (1) *AGENCY.*—*The term “agency” has the same*
4 *meaning given such term in section 551 of title 5,*
5 *United States Code.*

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

9 (3) *BUSINESS ENTITY.*—*The term “business enti-*
10 *ty” means any organization, corporation, trust, part-*
11 *nership, sole proprietorship, unincorporated associa-*
12 *tion, venture established to make a profit, or non-*
13 *profit, and any contractor, subcontractor, affiliate, or*
14 *licensee thereof engaged in interstate commerce.*

15 (4) *DESIGNATED ENTITY.*—*The term “designated*
16 *entity” means the Federal Government entity des-*
17 *ignated by the Secretary of Homeland Security under*
18 *section 7.*

19 (5) *ENCRYPTED.*—*The term “encrypted”—*

20 (A) *means the protection of data in elec-*
21 *tronic form, in storage or in transit, using an*
22 *encryption technology that is generally accepted*
23 *by experts in the field of information security*
24 *which renders such data indecipherable in the*
25 *absence of associated cryptographic keys nec-*
26 *essary to enable decryption of such data; and*

1 (B) includes appropriate management and
2 safeguards of such cryptographic keys so as to
3 protect the integrity of the encryption.

4 (6) *PERSONALLY IDENTIFIABLE INFORMATION.*—
5 The term “personally identifiable information” means
6 any information, or compilation of information, in
7 electronic or digital form serving as a means of iden-
8 tification, as defined by section 1028(d)(7) of title 18,
9 United State Code.

10 (7) *SECURITY BREACH.*—

11 (A) *IN GENERAL.*—The term “security
12 breach” means compromise of the security, con-
13 fidentiality, or integrity of, or the loss of, com-
14 puterized data that results in, or there is a rea-
15 sonable basis to conclude has resulted in, acquisi-
16 tion of or access to sensitive personally identifi-
17 able information that is unauthorized or in ex-
18 cess of authorization.

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

21 (i) a good faith acquisition of sensitive
22 personally identifiable information by a
23 business entity or agency, or an employee or
24 agent of a business entity or agency, if the
25 sensitive personally identifiable information

1 *is not subject to further unauthorized disclo-*
2 *sure;*

3 *(ii) any lawfully authorized investiga-*
4 *tive, protective, or intelligence activity of a*
5 *law enforcement or intelligence agency of*
6 *the United States, a State, or a political*
7 *subdivision of a State; or*

8 *(iii) the release of a public record not*
9 *otherwise subject to confidentiality or non-*
10 *disclosure requirements.*

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

16 *(A) an individual’s first and last name or*
17 *first initial and last name in combination with*
18 *any 1 of the following data elements:*

19 *(i) A non-truncated social security*
20 *number, driver’s license number, passport*
21 *number, or alien registration number.*

22 *(ii) Any 2 of the following:*

23 *(I) Home address or telephone*
24 *number.*

1 (II) *Mother's maiden name, if*
2 *identified as such.*

3 (III) *Month, day, and year of*
4 *birth.*

5 (iii) *Unique biometric data such as a*
6 *finger print, voice print, a retina or iris*
7 *image, or any other unique physical rep-*
8 *resentation.*

9 (iv) *A unique account identifier, elec-*
10 *tronic identification number, user name, or*
11 *routing code in combination with any asso-*
12 *ciated security code, access code, or pass-*
13 *word that is required for an individual to*
14 *obtain money, goods, services, or any other*
15 *thing of value; or*

16 (B) *a financial account number or credit or*
17 *debit card number in combination with any se-*
18 *curity code, access code, or password that is re-*
19 *quired for an individual to obtain credit, with-*
20 *draw funds, or engage in a financial trans-*
21 *action.*

22 **SEC. 15. EFFECTIVE DATE.**

23 *This Act shall take effect on the expiration of the date*
24 *which is 90 days after the date of enactment of this Act.*

Calendar No. 310

112TH CONGRESS
2^D SESSION

S. 1408

A BILL

To require Federal agencies, and persons engaged in interstate commerce, in possession of data containing sensitive personally identifiable information, to disclose any breach of such information.

FEBRUARY 6, 2012

Reported with an amendment