

112TH CONGRESS
1ST 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

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”.

6 **SEC. 2. NOTICE TO INDIVIDUALS.**

7 (a) IN GENERAL.—Any agency, or business entity en-
8 gaged in interstate commerce, that uses, accesses, trans-

1 mits, stores, disposes of or collects sensitive personally
2 identifiable information shall, following the discovery of a
3 security breach of such information notify any resident of
4 the United States whose sensitive personally identifiable
5 information has been, or is reasonably believed to have
6 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, dis-
11 poses of, or collects sensitive personally identifiable
12 information that the agency or business entity does
13 not own or license shall notify the owner or licensee
14 of the information following the discovery of a secu-
15 rity breach involving such information.

16 (2) NOTICE BY OWNER, LICENSEE OR OTHER
17 DESIGNATED THIRD PARTY.—Nothing in this Act
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 person-
5 ally identifiable information subject to the security
6 breach, or other designated third party, provides
7 such notification.

8 (c) TIMELINESS OF NOTIFICATION.—

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

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

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

1 (d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW
2 ENFORCEMENT PURPOSES.—

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

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

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

22 **SEC. 3. EXEMPTIONS.**

23 (a) EXEMPTION FOR NATIONAL SECURITY AND LAW
24 ENFORCEMENT.—

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

6 (A) cause damage to the national security;

7 or

8 (B) hinder a law enforcement investigation
9 or the ability of the agency to conduct law en-
10 forcement investigations.

11 (2) LIMITS ON CERTIFICATIONS.—An agency or
12 business entity may not execute a certification under
13 paragraph (1) to—

14 (A) conceal violations of law, inefficiency,
15 or administrative error;

16 (B) prevent embarrassment to a business
17 entity, organization, or agency; or

18 (C) restrain competition.

19 (3) NOTICE.—In every case in which an agency
20 or business entity issues a certification under para-
21 graph (1), the certification, accompanied by a de-
22 scription of the factual basis for the certification,
23 shall be immediately provided to the United States
24 Secret Service.

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

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

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

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

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

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 may request additional information
5 from the agency or business entity regarding
6 the basis for the claimed exemption, if such ad-
7 ditional information is necessary to determine
8 whether the exemption is merited.

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

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

21 (b) SAFE HARBOR.—

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

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

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

12 (i) the results of the risk assessment;

13 and

14 (ii) its decision to invoke the risk as-
15 sessment exemption; and

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

21 (2) PRESUMPTIONS.—There shall be a pre-
22 sumption that no significant risk of harm to the in-
23 dividual whose sensitive personally identifiable infor-
24 mation was subject to a security breach if such in-
25 formation—

1 (A) was encrypted; or

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

8 (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

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

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

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

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

23 (A) the information subject to the security
24 breach includes sensitive personally identifiable

1 information, other than a credit card number or
2 credit card security code, of any type; or

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

7 **SEC. 4. METHODS OF NOTICE.**

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

10 (1) INDIVIDUAL NOTICE.—

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

14 (B) telephone notice to the individual per-
15 sonally; or

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

22 (2) MEDIA NOTICE.—Notice to major media
23 outlets serving a State or jurisdiction, if the number
24 of residents of such State whose sensitive personally
25 identifiable information was, or is reasonably be-

1 lieved to have been, acquired by an unauthorized
2 person exceeds 5,000.

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

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

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

11 (2) a toll-free number—

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

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

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

21 (b) ADDITIONAL CONTENT.—Notwithstanding sec-
22 tion 10, a State may require that a notice under sub-
23 section (a) shall also include information regarding victim
24 protection assistance provided for by that State.

1 **SEC. 6. COORDINATION OF NOTIFICATION WITH CREDIT**
2 **REPORTING AGENCIES.**

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

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

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

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

22 (2) the security breach involves a database,
23 networked or integrated databases, or other data
24 system containing the sensitive personally identifi-
25 able information of more than 1,000,000 individuals
26 nationwide;

1 (3) the security breach involves databases
2 owned by the Federal Government; or

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

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

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

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

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

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

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

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

10 **SEC. 8. ENFORCEMENT.**

11 (a) CIVIL ACTIONS BY THE ATTORNEY GENERAL.—
12 The Attorney General may bring a civil action in the ap-
13 propriate United States district court against any business
14 entity that engages in conduct constituting a violation of
15 this Act and, upon proof of such conduct by a preponder-
16 ance of the evidence, such business entity shall be subject
17 to a civil penalty of not more than \$1,000 per day per
18 individual whose sensitive personally identifiable informa-
19 tion was, or is reasonably believed to have been, accessed
20 or acquired by an unauthorized person, up to a maximum
21 of \$1,000,000 per violation, unless such conduct is found
22 to be willful or intentional.

23 (b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-
24 ERAL.—

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

6 (A) enjoining such act or practice; or

7 (B) enforcing compliance with this Act.

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

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

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

22 **SEC. 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 consumer protection law, has reason to believe that
4 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 is pro-
7 hibited under this Act, the State or the State or
8 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 ju-
11 risdiction in a district court of the United States of
12 appropriate jurisdiction or any other court of com-
13 petent 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 \$1,000 per day per individual whose sensitive
18 personally identifiable information was, or is
19 reasonably believed to have been, accessed or
20 acquired by an unauthorized person, up to a
21 maximum of \$1,000,000 per violation, unless
22 such conduct is found to be willful or inten-
23 tional.

24 (2) NOTICE.—

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

5 (i) written notice of the action; and

6 (ii) a copy of the complaint for the ac-
7 tion.

8 (B) EXEMPTION.—

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

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

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

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

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

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

10 (4) file petitions for appeal.

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

19 (d) RULE OF CONSTRUCTION.—For purposes of
20 bringing any civil action under subsection (a), nothing in
21 this Act regarding notification shall be construed to pre-
22 vent an attorney general of a State from exercising the
23 powers conferred on such attorney general by the laws of
24 that State to—

25 (1) conduct investigations;

1 (2) administer oaths or affirmations; or

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

4 (e) VENUE; SERVICE OF PROCESS.—

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

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

11 (B) another court of competent jurisdic-
12 tion.

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

16 (A) is an inhabitant; or

17 (B) may be found.

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

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

22 The provisions of this Act shall supersede any other
23 provision of Federal law or any provision of law of any
24 State relating to notification by a business entity engaged

1 in interstate commerce or an agency of a security breach,
2 except as provided in section 5(b).

3 **SEC. 11. AUTHORIZATION OF APPROPRIATIONS.**

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

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

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

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

20 (2) the number and nature of security breaches
21 subject to the national security and law enforcement
22 exemptions under section 3(a) of this Act.

23 (b) REPORT.—Any report submitted under sub-
24 section (a) shall not disclose the contents of any risk as-

1 assessment provided to the United States Secret Service
2 under this Act.

3 **SEC. 13. DEFINITIONS.**

4 In this Act, the following definitions shall apply:

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

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

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

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

19 (A) means the protection of data in elec-
20 tronic form, in storage or in transit, using an
21 encryption technology that has been adopted by
22 an established standards setting body which
23 renders such data indecipherable in the absence
24 of associated cryptographic keys necessary to
25 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 (5) PERSONALLY IDENTIFIABLE INFORMA-
5 TION.—The term “personally identifiable informa-
6 tion” means any information, or compilation of in-
7 formation, in electronic or digital form serving as a
8 means of identification, as defined by section
9 1028(d)(7) of title 18, United State Code.

10 (6) SECURITY BREACH.—

11 (A) IN GENERAL.—The term “security
12 breach” means compromise of the security, con-
13 fidentiality, or integrity of computerized data
14 through misrepresentation or actions that result
15 in, or there is a reasonable basis to conclude
16 has resulted in, acquisition of or access to sen-
17 sitive personally identifiable information that is
18 unauthorized or in excess 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
24 or agent of a business entity or agency, if
25 the sensitive personally identifiable infor-

1 mation is not subject to further unauthor-
2 ized disclosure; or

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

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

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

14 (i) A non-truncated Social Security
15 number, driver’s license number, passport
16 number, or alien registration number.

17 (ii) Any 2 of the following:

18 (I) Home address or telephone
19 number.

20 (II) Mother’s maiden name, if
21 identified as such.

22 (III) Month, day, and year of
23 birth.

24 (iii) Unique biometric data such as a
25 finger print, voice print, a retina or iris

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

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

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

16 **SEC. 14. EFFECTIVE DATE.**

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

○