

110TH CONGRESS
1ST SESSION

S. 239

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

JANUARY 10, 2007

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 “Notification of Risk
5 to Personal Data Act of 2007”.

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 necessity of 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 if the agency certifies, in writing, that no-
3 tification of the security breach as required by sec-
4 tion 2 reasonably could be expected to—

5 (A) cause damage to the national security;

6 or

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

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

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

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

17 (C) restrain competition.

18 (3) NOTICE.—In every case in which an agency
19 issues a certification under paragraph (1), the cer-
20 tification, accompanied by a description of the fac-
21 tual basis for the certification, shall be immediately
22 provided to the United States Secret Service.

23 (b) SAFE HARBOR.—An agency or business entity
24 will be exempt from the notice requirements under section
25 2, if—

1 (1) a risk assessment concludes that there is no
2 significant risk that the security breach has resulted
3 in, or will result in, harm to the individuals whose
4 sensitive personally identifiable information was sub-
5 ject to the security breach;

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

11 (A) the results of the risk assessment; and

12 (B) its decision to invoke the risk assess-
13 ment exemption; and

14 (3) the United States Secret Service does not
15 indicate, in writing, within 10 days from receipt of
16 the decision, that notice should be given.

17 (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

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

22 (A) is designed to block the use of the sen-
23 sitive personally identifiable information to ini-
24 tiate unauthorized financial transactions before

1 they are charged to the account of the indi-
2 vidual; and

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

6 (2) LIMITATION.—The exemption by this sub-
7 section does not apply if the information subject to
8 the security breach includes sensitive personally
9 identifiable information in addition to the sensitive
10 personally identifiable information identified in sec-
11 tion 13.

12 **SEC. 4. METHODS OF NOTICE.**

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

15 (1) INDIVIDUAL NOTICE.—

16 (A) Written notification to the last known
17 home mailing address of the individual in the
18 records of the agency or business entity;

19 (B) telephone notice to the individual per-
20 sonally; or

21 (C) e-mail notice, if the individual has con-
22 sented to receive such notice and the notice is
23 consistent with the provisions permitting elec-
24 tronic transmission of notices under section 101

1 of the Electronic Signatures in Global and Na-
2 tional Commerce Act (15 U.S.C. 7001).

3 (2) MEDIA NOTICE.—Notice to major media
4 outlets serving a State or jurisdiction, if the number
5 of residents of such State whose sensitive personally
6 identifiable information was, or is reasonably be-
7 lieved to have been, acquired by an unauthorized
8 person exceeds 5,000.

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

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

13 (1) a description of the categories of sensitive
14 personally identifiable information that was, or is
15 reasonably believed to have been, acquired by an un-
16 authorized person;

17 (2) a toll-free number—

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

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

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

3 (b) **ADDITIONAL CONTENT.**—Notwithstanding sec-
4 tion 10, a State may require that a notice under sub-
5 section (a) shall also include information regarding victim
6 protection assistance provided for by that State.

7 **SEC. 6. COORDINATION OF NOTIFICATION WITH CREDIT**
8 **REPORTING AGENCIES.**

9 If an agency or business entity is required to provide
10 notification to more than 1,000 individuals under section
11 2(a), the agency or business entity shall also notify, with-
12 out unreasonable delay, all consumer reporting agencies
13 that compile and maintain files on consumers on a nation-
14 wide basis (as defined in section 603(p) of the Fair Credit
15 Reporting Act (15 U.S.C. 1681a(p)) of the timing and dis-
16 tribution of the notices.

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

18 (a) **SECRET SERVICE.**—Any business entity or agen-
19 cy shall give notice of a security breach to the United
20 States Secret Service if—

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

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

6 (3) the security breach involves databases
7 owned by the Federal Government; or

8 (4) the security breach involves primarily sen-
9 sitive personally identifiable information of employ-
10 ees and contractors of the Federal Government in-
11 volved in national security or law enforcement.

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 (c) 14-DAY RULE.—The notices to Federal law en-
6 forcement and the attorney general of each State affected
7 by a security breach required under this section shall be
8 delivered as promptly as possible, but not later than 14
9 days after discovery of the events requiring notice.

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 \$50,000 per person.

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

24 (1) IN GENERAL.—If it appears that a business
25 entity has engaged, or is engaged, in any act or

1 practice constituting a violation of this Act, the At-
2 torney General may petition an appropriate district
3 court of the United States for an order—

4 (A) enjoining such act or practice; or

5 (B) enforcing compliance with this Act.

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

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

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

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

21 (a) IN GENERAL.—

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

1 consumer protection law, has reason to believe that
2 an interest of the residents of that State has been
3 or is threatened or adversely affected by the engage-
4 ment of a business entity in a practice that is pro-
5 hibited under this Act, the State or the State or
6 local law enforcement agency on behalf of the resi-
7 dents of the agency's jurisdiction, may bring a civil
8 action on behalf of the residents of the State or ju-
9 risdiction in a district court of the United States of
10 appropriate jurisdiction or any other court of com-
11 petent jurisdiction, including a State court, to—

12 (A) enjoin that practice;

13 (B) enforce compliance with this Act; or

14 (C) obtain civil penalties of not more than
15 \$1,000 per day per individual whose sensitive
16 personally identifiable information was, or is
17 reasonably believed to have been, accessed or
18 acquired by an unauthorized person, up to a
19 maximum of \$50,000 per day.

20 (2) NOTICE.—

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

25 (i) written notice of the action; and

1 (ii) a copy of the complaint for the ac-
2 tion.

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 Act, if the State attorney gen-
8 eral determines that it is not feasible to
9 provide the notice described in such sub-
10 paragraph before the filing of the action.

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

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

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

23 (2) initiate an action in the appropriate United
24 States district court under section 8 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 Act or any regulations thereunder, no attorney gen-
9 eral of a State may, during the pendency of such pro-
10 ceeding or action, bring an action under this Act against
11 any defendant named in such criminal proceeding or civil
12 action for any violation that is alleged in that proceeding
13 or action.

14 (d) RULE OF CONSTRUCTION.—For purposes of
15 bringing any civil action under subsection (a), nothing in
16 this Act regarding notification shall be construed to pre-
17 vent an attorney general of a State from exercising the
18 powers conferred on such attorney general by the laws of
19 that State 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 (f) NO PRIVATE CAUSE OF ACTION.—Nothing in this
15 Act establishes a private cause of action against a business
16 entity for violation of any provision of this Act.

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

18 The provisions of this Act shall supersede any other
19 provision of Federal law or any provision of law of any
20 State relating to notification of a security breach, except
21 as provided in section 5(b).

22 **SEC. 11. AUTHORIZATION OF APPROPRIATIONS.**

23 There are authorized to be appropriated such sums
24 as may be necessary to cover the costs incurred by the
25 United States Secret Service to carry out investigations

1 and risk assessments of security breaches as required
2 under this Act.

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

4 The United States Secret Service shall report to Con-
5 gress not later than 18 months after the date of enactment
6 of this Act, and upon the request by Congress thereafter,
7 on—

8 (1) the number and nature of the security
9 breaches described in the notices filed by those busi-
10 ness entities invoking the risk assessment exemption
11 under section 3(b) of this Act and the response of
12 the United States Secret Service to such notices;
13 and

14 (2) the number and nature of security breaches
15 subject to the national security and law enforcement
16 exemptions under section 3(a) of this Act.

17 **SEC. 13. DEFINITIONS.**

18 In this Act, the following definitions shall apply:

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

22 (2) AFFILIATE.—The term “affiliate” means
23 persons related by common ownership or by cor-
24 porate control.

1 (3) BUSINESS ENTITY.—The term “business
2 entity” means any organization, corporation, trust,
3 partnership, sole proprietorship, unincorporated as-
4 sociation, venture established to make a profit, or
5 nonprofit, and any contractor, subcontractor, affil-
6 iate, or licensee thereof engaged in interstate com-
7 merce.

8 (4) PERSONALLY IDENTIFIABLE INFORMA-
9 TION.—The term “personally identifiable informa-
10 tion” means any information, or compilation of in-
11 formation, in electronic or digital form serving as a
12 means of identification, as defined by section
13 1028(d)(7) of title 18, United State Code.

14 (5) SECURITY BREACH.—

15 (A) IN GENERAL.—The term “security
16 breach” means compromise of the security, con-
17 fidentiality, or integrity of computerized data
18 through misrepresentation or actions that result
19 in, or there is a reasonable basis to conclude
20 has resulted in, acquisition of or access to sen-
21 sitive personally identifiable information that is
22 unauthorized or in excess of authorization.

23 (B) EXCLUSION.—The term “security
24 breach” does not include—

1 (i) a good faith acquisition of sensitive
 2 personally identifiable information by a
 3 business entity or agency, or an employee
 4 or agent of a business entity or agency, if
 5 the sensitive personally identifiable infor-
 6 mation is not subject to further unauthor-
 7 ized disclosure; or

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

11 (6) SENSITIVE PERSONALLY IDENTIFIABLE IN-
 12 FORMATION.—The term “sensitive personally identi-
 13 fiable information” means any information or com-
 14 pilation 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
17 or debit card number in combination with any
18 security code, access code or password that is
19 required for an individual to obtain money,
20 goods, services or any other thing of value.

21 **SEC. 14. EFFECTIVE DATE.**

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

○