

Calendar No. 180

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

MAY 31, 2007

Reported under authority of the order of the Senate of May 25, 2007, 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 Representatives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the "Notification of Risk
3 to Personal Data Act of 2007".

4 **SEC. 2. NOTICE TO INDIVIDUALS.**

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

13 (b) OBLIGATION OF OWNER OR LICENSEE.—

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

22 (2) NOTICE BY OWNER, LICENSEE OR OTHER
23 DESIGNATED THIRD PARTY.—Nothing in this Act
24 shall prevent or abrogate an agreement between an
25 agency or business entity required to give notice
26 under this section and a designated third party, in-

1 eluding an owner or licensee of the sensitive personally
2 identifiable information subject to the security
3 breach, to provide the notifications required under
4 subsection (a).

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

11 **(e) TIMELINESS OF NOTIFICATION.**

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

16 **(2) REASONABLE DELAY.**—Reasonable delay
17 under this subsection may include any time necessary
18 to determine the scope of the security breach,
19 prevent further disclosures, and restore the reasonable
20 integrity of the data system and provide notice
21 to law enforcement when required.

22 **(3) BURDEN OF PROOF.**—The agency, business
23 entity, owner, or licensee required to provide notification
24 under this section shall have the burden of

1 demonstrating that all notifications were made as re-
2 quired under this Act, including evidence dem-
3 onstrating the necessity of any delay.

4 **(d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW**
5 **ENFORCEMENT PURPOSES.—**

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

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

20 **(3) LAW ENFORCEMENT IMMUNITY.**—No cause
21 of action shall lie in any court against any law en-
22 forcement agency for acts relating to the delay of
23 notification for law enforcement purposes under this
24 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 if the agency certifies, in writing, that no-
6 tification of the security breach as required by sec-
7 tion 2 reasonably could be expected to—

8 (A) cause damage to the national security;

9 or

10 (B) hinder a law enforcement investigation
11 or the ability of the agency to conduct law en-
12 forcement investigations.13 (2) LIMITS ON CERTIFICATIONS.—An agency
14 may not execute a certification under paragraph (1)
15 to—16 (A) conceal violations of law, inefficiency,
17 or administrative error;18 (B) prevent embarrassment to a business
19 entity, organization, or agency; or

20 (C) restrain competition.

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

1 (b) **SAFE HARBOR.**—An agency or business entity
2 will be exempt from the notice requirements under section
3 2, if—

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

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

14 (A) the results of the risk assessment; and
15 (B) its decision to invoke the risk assess-
16 ment exemption; and

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

20 (e) **FINANCIAL FRAUD PREVENTION EXEMPTION.**—

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

1 (A) is designed to block the use of the sen-
2 sitive personally identifiable information to ini-
3 tiate unauthorized financial transactions before
4 they are charged to the account of the indi-
5 vidual; and

(B) provides for notice to affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

15 SEC. 4. METHODS OF NOTICE.

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

18 (1) INDIVIDUAL NOTICE.—

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

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

24 (C) e-mail notice, if the individual has con-
25 sented to receive such notice and the notice is

1 consistent with the provisions permitting ele-
2 tronic transmission of notices under section 101
3 of the Electronic Signatures in Global and Na-
4 tional Commerce Act (15 U.S.C. 7001).

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

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

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

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

19 (2) a toll-free number—

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

23 (B) from which the individual may learn
24 what types of sensitive personally identifiable

1 information the agency or business entity main-
2 tained about that individual; and

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

5 ~~(b) ADDITIONAL CONTENT.—Notwithstanding~~ section 10; a State may require that a notice under sub-
6 section (a) shall also include information regarding victim
7 protection assistance provided for by that State.

9 **SEC. 6. COORDINATION OF NOTIFICATION WITH CREDIT**

10 **REPORTING AGENCIES.**

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

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

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

23 ~~(1) the number of individuals whose sensitive~~
24 ~~personally identifying information was, or is reason-~~

1 ably believed to have been acquired by an unauthorized
2 person exceeds 10,000;

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

8 (3) the security breach involves databases
9 owned by the Federal Government, or

10 (4) the security breach involves primarily sensitive
11 personally identifiable information of employees and
12 contractors of the Federal Government involved in
13 national security or law enforcement.

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

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

1 ice under section 3056(a) of title 18, United States
2 Code;

3 (2) the United States Postal Inspection Service,
4 if the security breach involves mail fraud; and
5 (3) the attorney general of each State affected
6 by the security breach.

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

12 **SEC. 8. ENFORCEMENT.**

13 (a) CIVIL ACTIONS BY THE ATTORNEY GENERAL.—
14 The Attorney General may bring a civil action in the ap-
15 propriate United States district court against any business
16 entity that engages in conduct constituting a violation of
17 this Act and, upon proof of such conduct by a preponder-
18 ance of the evidence, such business entity shall be subject
19 to a civil penalty of not more than \$1,000 per day per
20 individual whose sensitive personally identifiable informa-
21 tion was, or is reasonably believed to have been, accessed
22 or acquired by an unauthorized person, up to a maximum
23 of \$50,000 per person.

24 (b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-
25 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 \$50,000 per day.

22 (2) NOTICE.—

23 (A) IN GENERAL.—Before filing an action
24 under paragraph (1), the attorney general of

1 the State involved shall provide to the Attorney
2 General of the United States—

3 (i) written notice of the action; and
4 (ii) a copy of the complaint for the ac-
5 tion.

6 (B) EXEMPTION.—

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

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

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

7 (4) file petitions for appeal.

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

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

22 (1) conduct investigations;

23 (2) administer oaths or affirmations; or

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

1 (e) VENUE; SERVICE OF PROCESS.—

2 (1) VENUE.—Any action brought under sub-
3 section (a) may be brought in—4 (A) the district court of the United States
5 that meets applicable requirements relating to
6 venue under section 1391 of title 28, United
7 States Code; or

8 (B) another court of competent jurisdiction.

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

1 United States Secret Service to carry out investigations
2 and risk assessments of security breaches as required
3 under this Act.

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

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

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

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

18 **SEC. 13. DEFINITIONS.**

19 In this Act, the following definitions shall apply:

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

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

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 unauthorized
7 disclosure; or

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.

(II) Mother's maiden name, if

identified as such.

(III) Month, day, and year of

birth.

(iii) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation.

(iv) A unique account identifier, elec-

tronic identification number, user name, or routing code in combination with any associated security code, access code, or password that is required for an individual to obtain money, goods, services or any other thing of value; or

B) a financial account number or credit

or debit card number in combination with any security code, access code or password that is required for an individual to obtain money, 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.

1 **SECTION 1. SHORT TITLE.**

2 *This Act may be cited as the “Notification of Risk to
3 Personal Data Act of 2007”.*

4 **SEC. 2. NOTICE TO INDIVIDUALS.**

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

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

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

22 *(2) NOTICE BY OWNER, LICENSEE OR OTHER
23 DESIGNATED THIRD PARTY.—Nothing in this Act
24 shall prevent or abrogate an agreement between an
25 agency or business entity required to give notice
26 under this section and a designated third party, in-*

1 *cluding an owner or licensee of the sensitive personally*
2 *identifiable information subject to the security*
3 *breach, to provide the notifications required under*
4 *subsection (a).*

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

12 **(c) TIMELINESS OF NOTIFICATION.—**

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

17 **(2) REASONABLE DELAY.—***Reasonable delay*
18 *under this subsection may include any time necessary*
19 *to determine the scope of the security breach, prevent*
20 *further disclosures, and restore the reasonable integ-*
21 *rity of the data system and provide notice to law en-*
22 *forcement when required.*

23 **(3) BURDEN OF PROOF.—***The agency, business*
24 *entity, owner, or licensee required to provide notifica-*
25 *tion under this section shall have the burden of dem-*

1 *onstrating that all notifications were made as re-*
2 *quired under this Act, including evidence dem-*
3 *onstrating the reasons for any delay.*

4 *(d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW*
5 *ENFORCEMENT PURPOSES.—*

6 *(1) IN GENERAL.—If a Federal law enforcement*
7 *agency determines that the notification required*
8 *under this section would impede a criminal investiga-*
9 *tion, such notification shall be delayed upon written*
10 *notice from such Federal law enforcement agency to*
11 *the agency or business entity that experienced the*
12 *breach.*

13 *(2) EXTENDED DELAY OF NOTIFICATION.—If the*
14 *notification required under subsection (a) is delayed*
15 *pursuant to paragraph (1), an agency or business en-*
16 *tity shall give notice 30 days after the day such law*
17 *enforcement delay was invoked unless a Federal law*
18 *enforcement agency provides written notification that*
19 *further delay is necessary.*

20 *(3) LAW ENFORCEMENT IMMUNITY.—No cause of*
21 *action shall lie in any court against any law enforce-*
22 *ment agency for acts relating to the delay of notifica-*
23 *tion for law enforcement purposes under this 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 business
6 entity certifies, in writing, that notification of the se-
7 curity breach as required by section 2 reasonably
8 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 Secret*
6 *Service may review a certification provided by*
7 *an agency under paragraph (3), and shall re-*
8 *view a certification provided by a business entity*
9 *under paragraph (3), to determine whether an*
10 *exemption under paragraph (1) is merited. Such*
11 *review shall be completed not later than 10 busi-*
12 *ness days after the date of receipt of the certifi-*
13 *cation, except as provided in paragraph (5)(C).*

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

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

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

20 (b) *SAFE HARBOR.*—

24 (A) a risk assessment concludes that there is
25 no significant risk that a security breach has re-

1 *sulted in, or will result in, harm to the individual whose sensitive personally identifiable information was subject to the security breach;*

4 *(B) without unreasonable delay, but not later than 45 days after the discovery of a security breach (unless extended by the United States Secret Service), the agency or business entity notifies the United States Secret Service, in writing, of—*

10 *(i) the results of the risk assessment; and*

12 *(ii) its decision to invoke the risk assessment exemption; and*

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

19 *(2) PRESUMPTIONS.—There shall be a presumption that no significant risk of harm to the individual whose sensitive personally identifiable information was subject to a security breach if such information—*

23 *(A) was encrypted; or*

24 *(B) was rendered indecipherable through the use of best practices or methods, such as redac-*

1 *tion, access controls, or other such mechanisms,*
2 *that are widely accepted as an effective industry*
3 *practice, or an effective industry standard.*

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

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

9 *(A) is designed to block the use of the sen-*
10 *sitive personally identifiable information to ini-*
11 *tiate unauthorized financial transactions before*
12 *they are charged to the account of the individual;*
13 *and*

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

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

19 *(A) the information subject to the security*
20 *breach includes sensitive personally identifiable*
21 *information, other than a credit card number or*
22 *credit card security code, of any type; or*

23 *(B) the information subject to the security*
24 *breach includes both the individual's credit card*
25 *number and the individual's first and last name.*

1 **SEC. 4. METHODS OF NOTICE.**

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

4 *(1) INDIVIDUAL NOTICE.—*

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

8 *(B) telephone notice to the individual per-*
9 *sonally; or*

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

16 *(2) MEDIA NOTICE.—Notice to major media out-*
17 *lets serving a State or jurisdiction, if the number of*
18 *residents of such State whose sensitive personally*
19 *identifiable information was, or is reasonably believed*
20 *to have been, acquired by an unauthorized person ex-*
21 *ceeds 5,000.*

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

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

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

5 (2) a toll-free number—

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

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

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

15 (b) *ADDITIONAL CONTENT.*—Notwithstanding section
16 10, a State may require that a notice under subsection (a)
17 shall also include information regarding victim protection
18 assistance provided for by that State.

19 **SEC. 6. COORDINATION OF NOTIFICATION WITH CREDIT**
20 **REPORTING AGENCIES.**

21 If an agency or business entity is required to provide
22 notification to more than 5,000 individuals under section
23 2(a), the agency or business entity shall also notify all con-
24 sumer reporting agencies that compile and maintain files
25 on consumers on a nationwide basis (as defined in section

1 *603(p) of the Fair Credit Reporting Act (15 U.S.C.*
2 *1681a(p)) of the timing and distribution of the notices.*
3 *Such notice shall be given to the consumer credit reporting*
4 *agencies without unreasonable delay and, if it will not*
5 *delay notice to the affected individuals, prior to the dis-*
6 *tribution of notices to the affected individuals.*

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

8 (a) *SECRET SERVICE.—Any business entity or agency*
9 *shall notify the United States Secret Service of the fact that*
10 *a security breach has occurred if—*

11 (1) *the number of individuals whose sensitive*
12 *personally identifying information was, or is reason-*
13 *ably believed to have been acquired by an unauthor-*
14 *ized person exceeds 10,000;*

15 (2) *the security breach involves a database,*
16 *networked or integrated databases, or other data sys-*
17 *tem containing the sensitive personally identifiable*
18 *information of more than 1,000,000 individuals na-*
19 *tionwide;*

20 (3) *the security breach involves databases owned*
21 *by the Federal Government; or*

22 (4) *the security breach involves primarily sen-*
23 *sitive personally identifiable information of individ-*
24 *uals known to the agency or business entity to be em-*

1 *ployees and contractors of the Federal Government in-*
2 *olved in national security or law enforcement.*

3 *(b) NOTICE TO OTHER LAW ENFORCEMENT AGEN-*
4 *CIES.—The United States Secret Service shall be responsible*
5 *for notifying—*

6 *(1) the Federal Bureau of Investigation, if the se-*
7 *curity breach involves espionage, foreign counterintel-*
8 *ligence, information protected against unauthorized*
9 *disclosure for reasons of national defense or foreign*
10 *relations, or Restricted Data (as that term is defined*
11 *in section 11y of the Atomic Energy Act of 1954 (42*
12 *U.S.C. 2014(y)), except for offenses affecting the du-*
13 *ties of the United States Secret Service under section*
14 *3056(a) of title 18, United States Code;*

15 *(2) the United States Postal Inspection Service,*
16 *if the security breach involves mail fraud; and*
17 *(3) the attorney general of each State affected by*
18 *the security breach.*

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

21 *(1) Notice under subsection (a) shall be delivered*
22 *as promptly as possible, but not later than 14 days*
23 *after discovery of the events requiring notice.*

24 *(2) Notice under subsection (b) shall be delivered*
25 *not later than 14 days after the United States Secret*

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

3 **SEC. 8. ENFORCEMENT.**

4 *(a) CIVIL ACTIONS BY THE ATTORNEY GENERAL.—The*
5 *Attorney General may bring a civil action in the appro-*
6 *priate United States district court against any business en-*
7 *tity that engages in conduct constituting a violation of this*
8 *Act and, upon proof of such conduct by a preponderance*
9 *of the evidence, such business entity shall be subject to a*
10 *civil penalty of not more than \$1,000 per day per indi-*
11 *vidual whose sensitive personally identifiable information*
12 *was, or is reasonably believed to have been, accessed or ac-*
13 *quired by an unauthorized person, up to a maximum of*
14 *\$1,000,000 per violation, unless such conduct is found to*
15 *be willful or intentional.*

16 *(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-*
17 *ERAL.—*

18 *(1) IN GENERAL.—If it appears that a business*
19 *entity has engaged, or is engaged, in any act or prac-*
20 *tice constituting a violation of this Act, the Attorney*
21 *General may petition an appropriate district court of*
22 *the United States for an order—*
23 *(A) enjoining such act or practice; or*
24 *(B) enforcing compliance with this Act.*

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

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

13 SEC. 9. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

14 (a) *IN GENERAL.*—

1 *half of the residents of the State or jurisdiction in a*
2 *district court of the United States of appropriate ju-*
3 *risdiction or any other court of competent jurisdic-*
4 *tion, including a State court, to—*

5 *(A) enjoin that practice;*
6 *(B) enforce compliance with this Act; or*
7 *(C) obtain civil penalties of not more than*
8 *\$1,000 per day per individual whose sensitive*
9 *personally identifiable information was, or is*
10 *reasonably believed to have been, accessed or ac-*
11 *quired by an unauthorized person, up to a max-*
12 *imum of \$1,000,000 per violation, unless such*
13 *conduct is found to be willful or intentional.*

14 *(2) NOTICE.—*

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

19 *(i) written notice of the action; and*
20 *(ii) a copy of the complaint for the ac-*
21 *tion.*

22 *(B) EXEMPTION.—*

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

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

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

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

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

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

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

22 *(4) file petitions for appeal.*

23 *(c) PENDING PROCEEDINGS.—If the Attorney General*
24 *has instituted a proceeding or action for a violation of this*
25 *Act or any regulations thereunder, no attorney general of*

1 a State may, during the pendency of such proceeding or
2 action, bring an action under this Act against any defend-
3 ant named in such criminal proceeding or civil action for
4 any violation that is alleged in that proceeding or 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—

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. EFFECT ON FEDERAL AND STATE LAW.

7 *The provisions of this Act shall supersede any other*
8 *provision of Federal law or any provision of law of any*
9 *State relating to notification by a business entity engaged*
10 *in interstate commerce or an agency of a security breach,*
11 *except as provided in section 5(b).*

12 SEC. 11. AUTHORIZATION OF APPROPRIATIONS.

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

17 SEC. 12. REPORTING ON RISK ASSESSMENT EXEMPTIONS.

18 (a) *IN GENERAL.—The United States Secret Service*
19 *shall report to Congress not later than 18 months after the*
20 *date of enactment of this Act, and upon the request by Con-*
21 *gress thereafter, on—*

(1) the number and nature of the security breaches described in the notices filed by those business entities invoking the risk assessment exemption

1 *under section 3(b) of this Act and the response of the*
2 *United States Secret Service to such notices; and*

3 *(2) the number and nature of security breaches*
4 *subject to the national security and law enforcement*
5 *exemptions under section 3(a) of this Act.*

6 *(b) REPORT.—Any report submitted under subsection*
7 *(a) shall not disclose the contents of any risk assessment*
8 *provided to the United States Secret Service under this Act.*

9 **SEC. 13. DEFINITIONS.**

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

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

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

17 *(3) BUSINESS ENTITY.—The term “business enti-*
18 *ty” means any organization, corporation, trust, part-*
19 *nership, sole proprietorship, unincorporated associa-*
20 *tion, venture established to make a profit, or non-*
21 *profit, and any contractor, subcontractor, affiliate, or*
22 *licensee thereof engaged in interstate commerce.*

23 *(4) ENCRYPTED.—The term “encrypted”—*

24 *(A) means the protection of data in elec-*
25 *tronic form, in storage or in transit, using an*

1 *encryption technology that has been adopted by*
2 *an established standards setting body which ren-*
3 *ders such data indecipherable in the absence of*
4 *associated cryptographic keys necessary to enable*
5 *decryption of such data; and*

6 *(B) includes appropriate management and*
7 *safeguards of such cryptographic keys so as to*
8 *protect the integrity of the encryption.*

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

15 *(6) SECURITY BREACH.—*

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

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

(i) A non-truncated social security number, driver's license number, passport number, or alien registration number.

22 (ii) Any 2 of the following:

23 (I) Home address or telephone
24 number.

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

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

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*

22 SEC. 14. 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. 180

110th CONGRESS
1st SESSION
S. 239

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.

MAY 31, 2007

Reported with an amendment