

109<sup>TH</sup> CONGRESS  
1<sup>ST</sup> SESSION

# S. 115

To require Federal agencies, and persons engaged in interstate commerce, in possession of electronic data containing personal information, to disclose any unauthorized acquisition of such information.

---

IN THE SENATE OF THE UNITED STATES

JANUARY 24, 2005

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 electronic data containing personal information, to disclose any unauthorized acquisition 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”.

6       **SEC. 2. DEFINITIONS.**

7       In this Act, the following definitions shall apply:

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

4           (2) BREACH OF SECURITY OF THE SYSTEM.—  
5 The term “breach of security of the system”—

6           (A) means the compromise of the security,  
7 confidentiality, or integrity of computerized  
8 data that results in, or there is a reasonable  
9 basis to conclude has resulted in, the unauthor-  
10 ized acquisition of and access to personal infor-  
11 mation maintained by the person or business;  
12 and

13           (B) does not include good faith acquisition  
14 of personal information by an employee or  
15 agent of the person or business for the purposes  
16 of the person or business, if the personal infor-  
17 mation is not used or subject to further unau-  
18 thorized disclosure.

19           (3) PERSON.—The term “person” has the same  
20 meaning given such term in section 551(2) of title  
21 5, United States Code.

22           (4) PERSONAL INFORMATION.—The term “per-  
23 sonal information” means an individual’s last name  
24 in combination with any 1 or more of the following

1 data elements, when either the name or the data ele-  
 2 ments are not encrypted:

3 (A) Social security number.

4 (B) Driver's license number or State iden-  
 5 tification number.

6 (C) Account number, credit or debit card  
 7 number, in combination with any required secu-  
 8 rity code, access code, or password that would  
 9 permit access to an individual's financial ac-  
 10 count.

11 (5) SUBSTITUTE NOTICE.—The term “sub-  
 12 stitute notice” means—

13 (A) e-mail notice, if the agency or person  
 14 has an e-mail address for the subject persons;

15 (B) conspicuous posting of the notice on  
 16 the Internet site of the agency or person, if the  
 17 agency or person maintains an Internet site; or

18 (C) notification to major media.

19 **SEC. 3. DATABASE SECURITY.**

20 (a) DISCLOSURE OF SECURITY BREACH.—

21 (1) IN GENERAL.—Any agency, or person en-  
 22 gaged in interstate commerce, that owns or licenses  
 23 electronic data containing personal information  
 24 shall, following the discovery of a breach of security  
 25 of the system containing such data, notify any resi-

1       dent of the United States whose unencrypted per-  
2       sonal information was, or is reasonably believed to  
3       have been, acquired by an unauthorized person.

4           (2) NOTIFICATION OF OWNER OR LICENSEE.—

5       Any agency, or person engaged in interstate com-  
6       merce, in possession of electronic data containing  
7       personal information that the agency does not own  
8       or license shall notify the owner or licensee of the in-  
9       formation if the personal information was, or is rea-  
10      sonably believed to have been, acquired by an unau-  
11      thorized person through a breach of security of the  
12      system containing such data.

13          (3) TIMELINESS OF NOTIFICATION.—Except as

14      provided in paragraph (4), all notifications required  
15      under paragraph (1) or (2) shall be made as expedi-  
16      ently as possible and without unreasonable delay fol-  
17      lowing—

18           (A) the discovery by the agency or person  
19           of a breach of security of the system; and

20           (B) any measures necessary to determine  
21           the scope of the breach, prevent further disclo-  
22           sures, and restore the reasonable integrity of  
23           the data system.

24          (4) DELAY OF NOTIFICATION AUTHORIZED FOR

25      LAW ENFORCEMENT PURPOSES.—If a law enforce-

1       ment agency determines that the notification re-  
2       quired under this subsection would impede a crimi-  
3       nal investigation, such notification may be delayed  
4       until such law enforcement agency determines that  
5       the notification will no longer compromise such in-  
6       vestigation.

7               (5) METHODS OF NOTICE.—An agency, or per-  
8       son engaged in interstate commerce, shall be in com-  
9       pliance with this subsection if it provides the resi-  
10      dent, owner, or licensee, as appropriate, with—

11                   (A) written notification;

12                   (B) e-mail notice, if the person or business  
13      has an e-mail address for the subject person; or

14                   (C) substitute notice, if—

15                           (i) the agency or person demonstrates  
16      that the cost of providing direct notice  
17      would exceed \$250,000;

18                           (ii) the affected class of subject per-  
19      sons to be notified exceeds 500,000; or

20                           (iii) the agency or person does not  
21      have sufficient contact information for  
22      those to be notified.

23               (6) ALTERNATIVE NOTIFICATION PROCEDURE-  
24      S.—Notwithstanding any other obligation  
25      under this subsection, an agency, or person engaged

1 in interstate commerce, shall be deemed to be in  
2 compliance with this subsection if the agency or per-  
3 son—

4 (A) maintains its own reasonable notifica-  
5 tion procedures as part of an information secu-  
6 rity policy for the treatment of personal infor-  
7 mation; and

8 (B) notifies subject persons in accordance  
9 with its information security policy in the event  
10 of a breach of security of the system.

11 (7) REASONABLE NOTIFICATION PROCE-  
12 DURES.—As used in paragraph (6), with respect to  
13 a breach of security of the system involving personal  
14 information described in section 2(4)(C), the term  
15 “reasonable notification procedures” means proce-  
16 dures that—

17 (A) use a security program reasonably de-  
18 signed to block unauthorized transactions be-  
19 fore they are charged to the customer’s ac-  
20 count;

21 (B) provide for notice to be given by the  
22 owner or licensee of the database, or another  
23 party acting on behalf of such owner or li-  
24 censee, after the security program indicates  
25 that the breach of security of the system has re-

1           sulted in fraud or unauthorized transactions,  
2           but does not necessarily require notice in other  
3           circumstances; and

4           (C) are subject to examination for compli-  
5           ance with the requirements of this Act by 1 or  
6           more Federal functional regulators (as defined  
7           in section 509 of the Gramm-Leach Bliley Act  
8           (15 U.S.C. 6809)), with respect to the oper-  
9           ation of the security program and the notifica-  
10          tion procedures.

11       (b) CIVIL REMEDIES.—

12           (1) PENALTIES.—Any agency, or person en-  
13           gaged in interstate commerce, that violates this sec-  
14           tion shall be subject to a fine of not more than  
15           \$5,000 per violation, to a maximum of \$25,000 per  
16           day while such violations persist.

17           (2) EQUITABLE RELIEF.—Any person engaged  
18           in interstate commerce that violates, proposes to vio-  
19           late, or has violated this section may be enjoined  
20           from further violations by a court of competent ju-  
21           risdiction.

22           (3) OTHER RIGHTS AND REMEDIES.—The  
23           rights and remedies available under this subsection  
24           are cumulative and shall not affect any other rights  
25           and remedies available under law.

1 (c) ENFORCEMENT.—The Federal Trade Commission  
2 is authorized to enforce compliance with this section, in-  
3 cluding the assessment of fines under subsection (b)(1).

4 **SEC. 4. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

5 (a) IN GENERAL.—

6 (1) CIVIL ACTIONS.—In any case in which the  
7 attorney general of a State has reason to believe  
8 that an interest of the residents of that State has  
9 been or is threatened or adversely affected by the  
10 engagement of any person in a practice that is pro-  
11 hibited under this Act, the State, as *parens patriae*,  
12 may bring a civil action on behalf of the residents  
13 of the State in a district court of the United States  
14 of appropriate jurisdiction to—

15 (A) enjoin that practice;

16 (B) enforce compliance with this Act;

17 (C) obtain damage, restitution, or other  
18 compensation on behalf of residents of the  
19 State; or

20 (D) obtain such other relief as the court  
21 may consider to be appropriate.

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—

- 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 subsection, if the State attorney  
11 general determines that it is not feasible to  
12 provide the notice described in such sub-  
13 paragraph before the filing of the action.

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

20 (b) CONSTRUCTION.—For purposes of bringing any  
21 civil action under subsection (a), nothing in this Act shall  
22 be construed to prevent an attorney general of a State  
23 from exercising the powers conferred on such attorney  
24 general by the laws of 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 (c) VENUE; SERVICE OF PROCESS.—

5 (1) VENUE.—Any action brought under sub-  
6 section (a) may be brought in the district court of  
7 the United States that meets applicable require-  
8 ments relating to venue under section 1391 of title  
9 28, United States Code.

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

13 (A) is an inhabitant; or

14 (B) may be found.

15 **SEC. 5. EFFECT ON STATE LAW.**

16 The provisions of this Act shall supersede any incon-  
17 sistent provisions of law of any State or unit of local gov-  
18 ernment relating to the notification of any resident of the  
19 United States of any breach of security of an electronic  
20 database containing such resident's personal information  
21 (as defined in this Act), except as provided under sections  
22 1798.82 and 1798.29 of the California Civil Code.

1 **SEC. 6. EFFECTIVE DATE.**

2       This Act shall take effect on the expiration of the  
3 date which is 6 months after the date of enactment of  
4 this Act.

○