

**Calendar No. 252**109<sup>TH</sup> CONGRESS  
1<sup>ST</sup> SESSION**S. 1326**

To require agencies and persons in possession of computerized data containing sensitive personal information, to disclose security breaches where such breach poses a significant risk of identity theft.

---

**IN THE SENATE OF THE UNITED STATES**

JUNE 28, 2005

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

OCTOBER 20, 2005

Reported by Mr. SPECTER, without amendment

---

**A BILL**

To require agencies and persons in possession of computerized data containing sensitive personal information, to disclose security breaches where such breach poses a significant risk of identity theft.

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”.

1 **SEC. 2. DEFINITIONS.**

2 In this Act, the following definitions shall apply:

3 (1) AGENCY.—The term “agency”—

4 (A) has the meaning given such term in  
5 section 551(1) of title 5, United States Code;  
6 and

7 (B) includes any authority of a State or  
8 political subdivision.

9 (2) BREACH OF SECURITY OF THE SYSTEM.—

10 The term “breach of security of the system”—

11 (A) means the compromise of the security  
12 of computerized data containing sensitive per-  
13 sonal information that establishes a reasonable  
14 basis to conclude that a significant risk of iden-  
15 tity theft to an individual exists; and

16 (B) does not include the compromise of the  
17 security of computerized data, if the agency or  
18 person concludes, after conducting a reasonable  
19 investigation, that there is not a significant risk  
20 of identity theft to an individual, including a  
21 situation in which—

22 (i) sensitive personal information is  
23 acquired in good faith by an employee or  
24 agent of the agency or person and the in-  
25 formation is not subject to further unau-  
26 thorized disclosure;

1 (ii) an investigation by an appropriate  
 2 law enforcement agency, government agen-  
 3 cy, or official determines that there is not  
 4 a significant risk of identity theft; or

5 (iii) the agency or person maintains or  
 6 participates in a security program reason-  
 7 ably designed to block unauthorized trans-  
 8 actions before they are charged to an indi-  
 9 vidual's account and the security program  
 10 does not indicate that the compromise of  
 11 sensitive personal information has resulted  
 12 in fraud or unauthorized transactions.

13 (3) PERSON.—The term “person” has the  
 14 meaning given such term in section 551(2) of title  
 15 5, United States Code.

16 (4) SENSITIVE PERSONAL INFORMATION.—The  
 17 term “sensitive personal information”—

18 (A) means—

19 (i) an individual's first and last name;

20 (ii) the individual's address or tele-  
 21 phone number; and

22 (iii) the individual's social security  
 23 number, the individual's driver's license  
 24 number or equivalent State identification  
 25 number, or the individual's financial ac-

1 count number, credit or debit card number,  
2 in combination with any required security  
3 code, access code, or password that would  
4 permit access to an individual's financial  
5 account, if the data element under this  
6 clause is not encrypted or redacted and is  
7 linked to the information described in  
8 clauses (i) and (ii); and

9 (B) does not include—

10 (i) any list, description, or other  
11 grouping of individuals (and publicly avail-  
12 able information pertaining to them) that  
13 is derived without using any sensitive per-  
14 sonal information; or

15 (ii) publicly available information that  
16 is lawfully made available to the general  
17 public from Federal, State or local govern-  
18 ment records.

19 (5) REDACTED.—The term “redacted” means  
20 truncated so that not more than the last 4 digits of  
21 the social security number, driver's license number,  
22 State identification card number, or account number  
23 are accessible as part of the data.

24 (6) IDENTITY THEFT.—The term “identity  
25 theft” means a fraud committed using the identifica-

1 tion of another person with the intent to commit, or  
2 to aid or abet any unlawful activity that constitutes  
3 a violation of Federal law, or that constitutes a fel-  
4 ony under any applicable State or local law and that  
5 results in economic loss to the individual.

6 (7) PERSONAL INFORMATION.—The term “per-  
7 sonal information” means personally identifiable in-  
8 formation about a specific individual.

9 (8) FUNCTIONAL REGULATOR.—The term  
10 “functional regulator” means—

11 (A) the Office of the Comptroller of the  
12 Currency with respect to national banks, and  
13 Federal branches, Federal agencies of foreign  
14 banks, and any subsidiaries of such entities (ex-  
15 cept brokers, dealers, persons providing insur-  
16 ance, investment companies, and investment ad-  
17 visers);

18 (B) the Board of Governors of the Federal  
19 Reserve System with respect to member banks  
20 of the Federal Reserve System (other than na-  
21 tional banks), branches and agencies of foreign  
22 banks (other than Federal branches, Federal  
23 agencies, and insured State branches of foreign  
24 banks), commercial lending companies owned or  
25 controlled by foreign banks, organizations oper-

1           ating under section 25 or 25A of the Federal  
2           Reserve Act (12 U.S.C. 601 and 611), bank  
3           and financial holding companies, and any  
4           nonbank subsidiaries or affiliates of such enti-  
5           ties (except brokers, dealers, persons providing  
6           insurance, investment companies, and invest-  
7           ment advisers);

8           (C) the Board of Directors of the Federal  
9           Deposit Insurance Corporation with respect to  
10          banks insured by the Federal Deposit Insurance  
11          Corporation (other than members of the Fed-  
12          eral Reserve System), insured State branches of  
13          foreign banks, and any subsidiaries of such en-  
14          ties (except brokers, dealers, persons providing  
15          insurance, investment companies, and invest-  
16          ment advisers);

17          (D) the Director of the Office of Thrift  
18          Supervision with respect to savings association  
19          the deposits of which are insured by the Fed-  
20          eral Deposit Insurance Corporation, savings  
21          and loan holding companies, and any subsidi-  
22          aries of such entities (except brokers, dealers,  
23          persons providing insurance, investment compa-  
24          nies, and investment advisers);

1           (E) the National Credit Union Administra-  
2           tion Board with respect to any Federal credit  
3           union and any subsidiaries of such an entity;

4           (F) the Secretary of Transportation with  
5           respect to any air carrier or foreign air carrier  
6           subject to part A of subtitle VII of title 49,  
7           United States Code;

8           (G) the Secretary of Agriculture with re-  
9           spect to any activities subject to the Packers  
10          and Stockyards Act, 1921 (7 U.S.C. 181 et  
11          seq.) (except as provided in section 406 of that  
12          Act (7 U.S.C. 226 and 227));

13          (H) the Farm Credit Administration with  
14          respect to any Federal land bank, Federal land  
15          bank association, Federal intermediate credit  
16          bank, or production credit association;

17          (I) the Securities and Exchange Commis-  
18          sion with respect to any broker or dealer, in-  
19          vestment company or investment adviser;

20          (J) the applicable State insurance author-  
21          ity of the State in which the person is domiciled  
22          with respect to any person engaged in providing  
23          insurance;

1           (K) the Federal Communications Commis-  
2 sion with respect to any entity subject to the ju-  
3 risdiction of the Commission; and

4           (L) the Federal Trade Commission with  
5 respect to any other financial institution or  
6 other person that is not subject to the jurisdic-  
7 tion of any agency or authority under subpara-  
8 graphs (A) through (K).

9 **SEC. 3. DATABASE SECURITY.**

10       (a) IN GENERAL.—Any agency or person that owns  
11 or licenses computerized data containing sensitive personal  
12 information shall implement and maintain reasonable se-  
13 curity and notification procedures and practices appro-  
14 priate to the size and nature of the agency or person and  
15 the nature of the information to protect the sensitive per-  
16 sonal information from unauthorized access, destruction,  
17 use, modification or disclosure.

18       (b) DISCLOSURE OF SECURITY BREACH.—

19           (1) NOTIFICATION OF INDIVIDUAL.—

20               (A) IN GENERAL.—If an agency or person  
21 that owns or licenses computerized data con-  
22 taining sensitive personal information, deter-  
23 mines, after discovery and a reasonable inves-  
24 tigation, or notification under paragraph (2),  
25 that a significant risk of identity theft exists as

1 a result of a breach of security of the system  
2 of such agency or person containing such data,  
3 the agency or person shall notify any individual  
4 whose sensitive personal information was com-  
5 promised if such individual is known to be a  
6 resident of the United States.

7 (B) DELAY OF NOTIFICATION.—If a Fed-  
8 eral law enforcement agency of either appro-  
9 priate domestic or foreign jurisdiction deter-  
10 mines that the notification required under this  
11 subsection would impede a criminal or civil in-  
12 vestigation, such notification may be delayed  
13 until such Federal law enforcement agency de-  
14 termines that the notification will no longer  
15 compromise such investigation.

16 (2) NOTIFICATION OF OWNER OR LICENSOR.—  
17 Any agency or person in possession of computerized  
18 data containing sensitive personal information that  
19 the agency or person does not own or license shall  
20 notify the entity from whom it received the informa-  
21 tion if the security of the sensitive personal informa-  
22 tion was compromised and such compromise has re-  
23 sulted in a significant risk of identity theft to an in-  
24 dividual.

1           (3) TIMELINESS OF NOTIFICATION.—All notifi-  
2           cations required under paragraph (1) or (2) shall be  
3           made as expediently as possible and without unrea-  
4           sonable delay following—

5                   (A) the discovery and reasonable investiga-  
6                   tion by the agency or person of a breach of se-  
7                   curity of the system; and

8                   (B) any measures the agency or person  
9                   takes that are necessary to determine the scope  
10                  of the breach, prevent further breaches, deter-  
11                  mine whether there is a reasonable basis to con-  
12                  clude that a significant risk of identity theft to  
13                  an individual exists, restore the reasonable in-  
14                  tegrity of the data system, and comply with ap-  
15                  plicable requirements of securities laws and reg-  
16                  ulations.

17           (4) METHODS OF NOTICE.—An agency or per-  
18           son shall be in compliance with this subsection if it  
19           provides the resident, owner, or licensee, as appro-  
20           priate, with—

21                   (A) written notification to a mailing ad-  
22                   dress for the subject individual;

23                   (B) telephonic notification to a telephone  
24                   number for the subject individual;

1 (C) e-mail notice to an e-mail address for  
2 the subject individual; or

3 (D) conspicuous posting of the notice on  
4 the Internet site of the agency or person, if the  
5 agency or person maintains an Internet site, or  
6 notification to major media, if—

7 (i) the agency or person demonstrates  
8 that the cost of providing direct notice  
9 under paragraphs (A) through (C) of this  
10 subsection would exceed \$250,000;

11 (ii) the affected class of subject indi-  
12 viduals to be notified exceeds 500,000; or

13 (iii) the agency or person does not  
14 have sufficient contact information for  
15 those to be notified.

16 (5) CONTENTS OF NOTICE.—Notice under this  
17 subsection shall—

18 (A) be given in a clear and conspicuous  
19 manner;

20 (B) describe the breach of security of the  
21 system in general terms and the type of sen-  
22 sitive personal information involved; and

23 (C) include a toll-free telephone number or  
24 website that individuals can utilize for further  
25 information and assistance.

1           (6) DUTY TO COORDINATE WITH CONSUMER  
2 REPORTING AGENCIES.—Before any agency or per-  
3 son provides notice to more than 1,000 individuals  
4 at any time, or provides notice pursuant to para-  
5 graph (4)(D), that sensitive personal information on  
6 the individuals was, or may reasonably be expected  
7 to have been, the subject of a breach of security of  
8 the system, the agency or person shall, without un-  
9 reasonable delay—

10                   (A) notify all nationwide consumer report-  
11 ing agencies (as defined in section 603(p) of the  
12 Fair Credit Reporting Act (15 U.S.C.  
13 1681a(p))) of the timing, content, and distribu-  
14 tion of the notice, including—

15                           (i) the number of individuals to whom  
16 the notice will be given; or

17                           (ii) the type of notice provided under  
18 paragraph (4)(D); and

19                   (B) conform the notice to individuals to be  
20 delivered by such agency or person to accu-  
21 rately reflect, to the extent given in such no-  
22 tice—

23                           (i) the method of contact reasonably  
24 specified by each nationwide consumer re-  
25 porting agency that such individuals are to

1 use with respect to the particular notice;  
2 and

3 (ii) the responsibilities of a nationwide  
4 consumer reporting agency under the Fair  
5 Credit Reporting Act (15 U.S.C. 1681 et  
6 seq.) and any other applicable law.

7 (7) SAFE HARBOR.—Notwithstanding any other  
8 obligation under this subsection, an agency or per-  
9 son that maintains notification procedures as part of  
10 an information security policy for the treatment of  
11 sensitive personal information and is otherwise con-  
12 sistent with the requirements of paragraphs (3) and  
13 (6) shall be in compliance with this subsection if the  
14 agency or person notifies subject persons in accord-  
15 ance with its policies in the event of a breach of se-  
16 curity of the system.

17 (8) RELATION TO OTHER PROVISIONS.—Noth-  
18 ing in this Act shall be construed to modify, limit or  
19 supersede the operation of either the Fair Credit Re-  
20 porting Act, the Gramm-Leach-Bliley Act, or any  
21 other applicable provision of Federal law.

22 (c) CIVIL REMEDIES.—

23 (1) PENALTIES.—

24 (A) IN GENERAL.—Except as provided  
25 under subparagraph (B), any agency or person

1 that fails to give notice in accordance with  
2 paragraph (1) through (4) of subsection (b)  
3 shall be subject to—

4 (i) a fine in an amount not to exceed  
5 \$250,000 per breach of security of the sys-  
6 tem; or

7 (ii) in the case of a violation of sub-  
8 section (a), such actual damages as may be  
9 proven.

10 (B) EXEMPTION.—An agency or person  
11 shall not be subject to a fine under this para-  
12 graph if the breach of security of the system—

13 (i) was not a result of the negligence  
14 of such agency or person; and

15 (ii) was the result of fraud committed  
16 by a third party.

17 (2) EQUITABLE RELIEF.—Any person that vio-  
18 lates, proposes to violate, or has violated this section  
19 may be enjoined from further violations by a court  
20 of competent jurisdiction.

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

25 (d) ENFORCEMENT.—

1           (1) IN GENERAL.—The functional regulator is  
2           authorized to enforce compliance with this section,  
3           including the assessment of fines under subsection  
4           (c)(1).

5           (2) CIVIL ACTIONS.—No private right of action  
6           or class action shall be brought under this Act. No  
7           person other than the attorney general of a State  
8           may bring a civil action under the law of any State  
9           if such action is premised in whole or in part upon  
10          the defendant violating any provision of this Act.

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

12          (a) IN GENERAL.—

13           (1) CIVIL ACTIONS.—In any case in which the  
14           attorney general of a State has reason to believe  
15           that an interest of the residents of that State has  
16           been or is threatened or adversely affected by the  
17           engagement of any person in a practice that is pro-  
18           hibited under this Act, the State, as *parens patriae*,  
19           may bring a civil action on behalf of the residents  
20           of the State in a United States district court of ap-  
21           propriate jurisdiction to—

22                   (A) enjoin that practice;

23                   (B) enforce compliance with this Act; or

24                   (C) obtain damage, restitution, or other  
25           compensation on behalf of residents of the

1 State under the conditions and up to the mone-  
2 tary limits set forth in section 3(c)(1).

3 (2) NOTICE.—

4 (A) IN GENERAL.—Before filing an action  
5 under paragraph (1), the attorney general of  
6 the State shall provide the Attorney General of  
7 the United States and the functional regu-  
8 lator—

9 (i) written notice of the action; and

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

12 (B) EXEMPTION.—

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

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

1 (C) UNITED STATES ATTORNEY GENERAL  
2 PRIORITY.—After having been notified, as pro-  
3 vided in subparagraph (A), the Attorney Gen-  
4 eral shall have the right—

5 (i) to file a civil action, subject to  
6 monetary limits equal to those set forth in  
7 section 3(e)(1);

8 (ii) to intervene in the action;

9 (iii) upon so intervening, to be heard  
10 on all matters arising therein;

11 (iv) to remove the action to the appro-  
12 priate United States district court; and

13 (v) to file petitions for appeal.

14 (D) PREEMPTION.—

15 (i) ACTION BY DEPARTMENT OF JUST-  
16 TICE.—If the Attorney General institutes a  
17 civil action or intervenes in an action  
18 under this subsection, the functional regu-  
19 lator, a State attorney general, or an offi-  
20 cial or agency of a State may not bring an  
21 action under this section for any violation  
22 of this Act alleged in the complaint.

23 (ii) ACTION BY FUNCTIONAL REGU-  
24 LATOR.—If the functional regulator insti-  
25 tutes a civil action or intervenes under sec-

1           tion 3(d)(1) to enforce compliance with  
2           section 3, a State attorney general or offi-  
3           cial or agency of a State, may not bring an  
4           action under this section for any violation  
5           of this Act alleged in the complaint.

6           (b) LIMITATIONS ON STATE ACTIONS.—

7           (1) VIOLATION OF INJUNCTION REQUIRED.—A  
8           State may not bring an action against a person  
9           under subsection (a)(1)(C) unless—

10           (A) the person has been enjoined from  
11           committing the violation, in an action brought  
12           by the State under subsection (a)(1)(A); and

13           (B) the person has violated the injunction.

14           (2) LIMITATION ON DAMAGES RECOVERABLE.—

15           In an action under subsection (a)(1)(C), a State  
16           may not recover any damages incurred before the  
17           date of the violation of an injunction on which the  
18           action is based.

19           (c) CONSTRUCTION.—For purposes of a civil action  
20           under subsection (a), nothing in this Act shall be con-  
21           strued to prevent the attorney general of a State from ex-  
22           ercising the powers conferred on such attorney general by  
23           the laws of that State to—

24           (1) conduct investigations;

25           (2) administer oaths or affirmations; or

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

3           (d) VENUE; SERVICE OF PROCESS.—

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

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

15           The provisions of this Act shall supersede any law,  
16 rule, or regulation of any State or unit of local government  
17 that relates in any way to electronic information security  
18 standards or the notification of any resident of the United  
19 States of any breach of security pertaining to any collec-  
20 tion of personal information about such resident.

21 **SEC. 6. EFFECTIVE DATE.**

22           This Act shall take effect on the expiration of the  
23 date which is 180 days after the date of enactment of this  
24 Act.

**Calendar No. 252**

109<sup>TH</sup> CONGRESS  
1<sup>ST</sup> Session  
**S. 1326**

---

---

**A BILL**

To require agencies and persons in possession of computerized data containing sensitive personal information, to disclose security breaches where such breach poses a significant risk of identity theft.

---

---

OCTOBER 20, 2005

Reported without amendment