

110TH CONGRESS
1ST SESSION

S. 1202

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

APRIL 24, 2007

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

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 “Personal Data Protec-
5 tion Act of 2007”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

8 (1) AGENCY.—The term “agency”—

1 (A) has the meaning given that term in
2 section 551(1) of title 5, United States Code;
3 and

4 (B) includes any authority of a State or
5 political subdivision.

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

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

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

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

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

24 (ii) an investigation by an appropriate
25 law enforcement agency, government agen-

1 cy, or official determines that there is not
2 a significant risk of identity theft; or

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

11 (3) FUNCTIONAL REGULATOR.—The term
12 “functional regulator” means—

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

20 (B) the Board of Governors of the Federal
21 Reserve System with respect to member banks
22 of the Federal Reserve System (other than na-
23 tional banks), branches and agencies of foreign
24 banks (other than Federal branches, Federal
25 agencies, and insured State branches of foreign

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

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

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

1 persons providing insurance, investment compa-
2 nies, and investment advisers);

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

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

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

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

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

22 (J) the applicable State insurance author-
23 ity of the State in which the person is domiciled
24 with respect to any person engaged in providing
25 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 (4) IDENTITY THEFT.—The term “identity
10 theft” means a fraud committed using the sensitive
11 personal information of another individual with the
12 intent to commit, or to aid or abet any unlawful ac-
13 tivity that constitutes a violation of section 1028 of
14 title 18, United States Code, and that results in eco-
15 nomic loss to that individual.

16 (5) PERSON.—The term “person” has the
17 meaning given that term in section 551(2) of title 5,
18 United States Code.

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

22 (7) REDACTED.—The term “redacted” means
23 truncated so that not more than the last 4 digits of
24 the social security number, driver’s license number,

1 State identification card number, or account number
2 are accessible as part of the data.

3 (8) SENSITIVE PERSONAL INFORMATION.—

4 (A) IN GENERAL.—The term “sensitive
5 personal information” means an individual’s
6 first name (or first initial) and last name in
7 combination with any 1 or more of the following
8 data elements that relate to that individual
9 (when the data elements are not encrypted, re-
10 dacted, or secured by any other method ren-
11 dering that element unreadable or unusable):

12 (i) An individual’s social security
13 number.

14 (ii) An individual’s driver’s license
15 number or equivalent State identification
16 number.

17 (iii) An individual’s financial account
18 number, or credit or debit card number, in
19 combination with any required security
20 code, access code, or password that would
21 permit access to an individual’s financial
22 account.

23 (B) EXCLUSIONS.—The term “sensitive
24 personal information” does not include—

1 (i) any list, description, or other
 2 grouping of individuals (and publicly avail-
 3 able information pertaining to them) that
 4 is derived without using any sensitive per-
 5 sonal information; or

6 (ii) any information regardless of its
 7 source that is lawfully made available to
 8 the general public in Federal, State, or
 9 local government records.

10 **SEC. 3. DATABASE SECURITY.**

11 (a) IN GENERAL.—Any agency or person that owns
 12 or licenses computerized data containing sensitive personal
 13 information shall develop, implement, and maintain rea-
 14 sonable security and notification procedures and practices
 15 appropriate to the size and nature of the agency or person
 16 and the nature of the information to ensure the security
 17 and confidentiality of the personal information and protect
 18 it against any unauthorized access, destruction, use, modi-
 19 fication or disclosure.

20 (b) DISCLOSURE OF SECURITY BREACH.—

21 (1) NOTIFICATION OF INDIVIDUAL.—

22 (A) IN GENERAL.—If an agency or person
 23 that owns or licenses computerized data con-
 24 taining sensitive personal information, deter-
 25 mines, after discovery and a reasonable inves-

1 tigation, or notification under paragraph (2),
2 that a significant risk of identity theft exists as
3 a result of a breach of security of the system
4 of such agency or person containing such data,
5 the agency or person shall notify any individual
6 whose sensitive personal information was com-
7 promised.

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

17 (2) NOTIFICATION OF OWNER OR LICENSOR.—

18 (A) IN GENERAL.—Any agency or person
19 in possession of computerized data containing
20 sensitive personal information that the agency
21 or person does not own or license shall notify
22 and cooperate with the owner or licensor of the
23 information upon the discovery of a breach of
24 security of the system of such agency or person

1 as expediently as possible and without unrea-
2 sonable delay.

3 (B) AGREEMENTS TO NOTIFY INDIVIDUALS
4 PERMISSIBLE.—

5 (i) IN GENERAL.—Any agency or per-
6 son in possession of sensitive personal in-
7 formation on behalf of the owner or licen-
8 sor of such information may enter an
9 agreement with the owner or licensor re-
10 garding which person or entity will provide
11 any notice required under this subsection
12 to an individual whose sensitive personal
13 information was compromised.

14 (ii) SINGLE NOTICE.—This subsection
15 shall not be construed to require more
16 than a single notice to any individual for
17 each breach of security of the system relat-
18 ing to that individual.

19 (iii) NO AGREEMENT.—If an agency
20 or person in possession of sensitive per-
21 sonal information on behalf of the owner
22 or licensor of such information does not
23 have an agreement described in clause (i)
24 in effect on the date of a breach of security
25 of the system of that agency or person, the

1 agency or person that owns or licenses
2 computerized data containing sensitive per-
3 sonal information shall provide any notice
4 required under this subsection.

5 (3) TIMELINESS OF NOTIFICATION.—

6 (A) IN GENERAL.—All notifications re-
7 quired under paragraph (1) shall be made as
8 expediently as possible and without unreason-
9 able delay following—

10 (i) the discovery and reasonable inves-
11 tigation by the agency or person of a
12 breach of security of the system; and

13 (ii) measures the agency or person
14 takes that are necessary to determine the
15 scope of the breach, prevent further
16 breaches, determine whether there is a rea-
17 sonable basis to conclude that a significant
18 risk of identity theft to an individual ex-
19 ists, restore the reasonable integrity of the
20 data system, and comply with applicable
21 requirements of other laws and regulations.

22 (B) EXPEDITIOUS NOTICE.—Any measures
23 described in subparagraph (A)(ii) shall be un-
24 dertaken as expediently as possible and without
25 unreasonable delay. Such measures shall not be

1 undertaken for the purpose of causing delay of
2 notification.

3 (4) METHODS OF NOTICE.—An agency or per-
4 son required to give notice under paragraph (1) shall
5 be in compliance with this subsection if it provides—

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

8 (B) telephonic notification to a telephone
9 number for the subject individual;

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

12 (D) conspicuous posting of the notice on
13 the Internet site of the agency or person, if the
14 agency or person maintains an Internet site, or
15 notification to major media, if—

16 (i) the agency or person demonstrates
17 that the cost of providing direct notice
18 under subparagraphs (A) through (C) of
19 this subsection would exceed \$250,000;

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

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

1 (5) CONTENTS OF NOTICE.—Notice under this
2 subsection shall—

3 (A) be given in a clear and conspicuous
4 manner;

5 (B) describe the breach of security of the
6 system in general terms and the type of sen-
7 sitive personal information involved; and

8 (C) include a toll-free telephone number or
9 website that individuals can use for further in-
10 formation and assistance.

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

20 (A) notify any consumer reporting agency
21 that compiles and maintains files on consumers
22 on a nationwide basis (as that term is defined
23 in section 603(p) of the Fair Credit Reporting
24 Act (15 U.S.C. 1681a(p))) of the timing, con-
25 tent, and distribution of the notice, including—

1 (i) the number of individuals to whom
2 the notice will be given; or

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

5 (B) conform the notice to individuals to be
6 delivered by such agency or person to accu-
7 rately reflect, to the extent given in such no-
8 tice—

9 (i) the method of contact reasonably
10 specified by each consumer reporting agen-
11 cy that compiles and maintains files on
12 consumers on a nationwide basis that such
13 individuals are to use with respect to the
14 particular notice; and

15 (ii) the responsibilities of a consumer
16 reporting agency that compiles and main-
17 tains files on consumers on a nationwide
18 basis under the Fair Credit Reporting Act
19 (15 U.S.C. 1681 et seq.) and any other ap-
20 plicable law.

21 (7) SAFE HARBORS.—

22 (A) DATA SECURITY.—Notwithstanding
23 any other obligation under this section, a per-
24 son that is in compliance with data security re-
25 quirements under the laws, rules, regulations,

1 guidance, or guidelines established or enforced
2 by the functional regulator for that person shall
3 be deemed to be in compliance with subsection
4 (a).

5 (B) BREACH NOTIFICATION.—Notwith-
6 standing any other obligation under this sec-
7 tion, a person that is in compliance with breach
8 notification procedures under the laws, rules,
9 regulations, guidance, or guidelines established
10 or enforced by the functional regulator for that
11 person shall be deemed to be in compliance with
12 subsection (b).

13 (8) RELATION TO OTHER PROVISIONS.—Noth-
14 ing in this Act shall be construed to modify, limit or
15 supersede the operation of the Fair Credit Reporting
16 Act (15 U.S.C. 1681 et seq.), the Gramm-Leach-Bl-
17 ley Act (Public Law 106–102; 113 Stat. 1338), or
18 any other applicable provision of Federal law

19 (c) CIVIL REMEDIES.—

20 (1) PENALTIES.—

21 (A) IN GENERAL.—Except as provided
22 under subparagraph (B), any agency or person
23 that fails to give notice in accordance with
24 paragraph (1) through (4) of subsection (b)
25 shall be subject to—

1 (i) a fine in an amount not to exceed
2 \$250,000 per breach of security of the sys-
3 tem; or

4 (ii) in the case of a violation of sub-
5 section (a), such actual damages as may be
6 proven.

7 (B) AFFIRMATIVE DEFENSE.—An agency
8 or person shall have an affirmative defense to
9 a fine under this paragraph if the breach of se-
10 curity of the system—

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

13 (ii) was the result of a fraud or other
14 crime committed by a third party.

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

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

23 (d) ENFORCEMENT.—

24 (1) IN GENERAL.—The functional regulator is
25 authorized to enforce compliance with this section,

1 including the assessment of fines under subsection
 2 (c)(1).

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

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

10 (a) IN GENERAL.—

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

20 (A) enjoin that practice;

21 (B) enforce compliance with this Act; or

22 (C) obtain damage, restitution, or other
 23 compensation on behalf of residents of the
 24 State under the conditions and up to the mone-
 25 tary limits set forth in section 3(c)(1).

1 (2) NOTICE.—

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

7 (i) written notice of the action; and

8 (ii) a copy of the complaint for the ac-
9 tion.

10 (B) EXEMPTION.—

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

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

24 (C) UNITED STATES ATTORNEY GENERAL
25 PRIORITY.—After having been notified, as pro-

vided in subparagraph (A), the Attorney General shall have the right—

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

(ii) to intervene in the action; and

(iii) upon so intervening—

(I) to be heard on all matters arising therein;

(II) to remove the action to the appropriate United States district court; and

(III) to file petitions for appeal.

(D) PREEMPTION.—

(i) ACTION BY DEPARTMENT OF JUSTICE.—If the Attorney General institutes a civil action or intervenes in an action under this subsection, the functional regulator, a State attorney general, or an official or agency of a State may not bring an action under this section for any violation of this Act alleged in the complaint.

(ii) ACTION BY FUNCTIONAL REGULATOR.—If the functional regulator institutes 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.

○