

110TH CONGRESS
1ST SESSION

S. 1260

To protect information relating to consumers, to require notice of security breaches, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MAY 1, 2007

Mr. CARPER (for himself and Mr. BENNETT) introduced the following bill;
which was read twice and referred to the Committee on Banking, Housing,
and Urban Affairs

A BILL

To protect information relating to consumers, to require
notice of security breaches, and for other purposes.

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 “Data Security Act of
5 2007”.

6 **SEC. 2. DEFINITIONS.**

7 For purposes of this Act, the following definitions
8 shall apply:

1 (1) AFFILIATE.—The term “affiliate” means
2 any company that controls, is controlled by, or is
3 under common control with another company.

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

7 (3) BREACH OF DATA SECURITY.—

8 (A) IN GENERAL.—The term “breach of
9 data security” means the unauthorized acqui-
10 sition of sensitive account information or sen-
11 sitive personal information.

12 (B) EXCEPTION FOR DATA THAT IS NOT IN
13 USABLE FORM.—

14 (i) IN GENERAL.—The term “breach
15 of data security” does not include the un-
16 authorized acquisition of sensitive account
17 information or sensitive personal informa-
18 tion that is maintained or communicated in
19 a manner that is not usable—

20 (I) to commit identity theft; or

21 (II) to make fraudulent trans-
22 actions on financial accounts.

23 (ii) RULE OF CONSTRUCTION.—For
24 purposes of this subparagraph, information
25 that is maintained or communicated in a

1 manner that is not usable includes any in-
2 formation that is maintained or commu-
3 nicated in an encrypted, redacted, altered,
4 edited, or coded form.

5 (4) COMMISSION.—The term “Commission”
6 means the Federal Trade Commission.

7 (5) CONSUMER.—The term “consumer” means
8 an individual.

9 (6) CONSUMER REPORTING AGENCY THAT COM-
10 PILES AND MAINTAINS FILES ON CONSUMERS ON A
11 NATIONWIDE BASIS.—The term “consumer reporting
12 agency that compiles and maintains files on con-
13 sumers on a nationwide basis” has the same mean-
14 ing as in section 603(p) of the Fair Credit Report-
15 ing Act (15 U.S.C. 1681a(p)).

16 (7) COVERED ENTITY.—

17 (A) IN GENERAL.—The term “covered en-
18 tity” means any—

19 (i) entity, the business of which is en-
20 gaging in financial activities, as described
21 in section 4(k) of the Bank Holding Com-
22 pany Act of 1956 (12 U.S.C. 1843(k));

23 (ii) financial institution, including any
24 institution described in section 313.3(k) of

1 title 16, Code of Federal Regulations, as in
 2 effect on the date of enactment of this Act;

3 (iii) entity that maintains or otherwise
 4 possesses information that is subject to
 5 section 628 of the Fair Credit Reporting
 6 Act (15 U.S.C. 1681w); or

7 (iv) other individual, partnership, cor-
 8 poration, trust, estate, cooperative, associa-
 9 tion, or entity that maintains or commu-
 10 nicates sensitive account information or
 11 sensitive personal information.

12 (B) EXCEPTION.—The term “covered enti-
 13 ty” does not include any agency or any other
 14 unit of Federal, State, or local government or
 15 any subdivision of such unit.

16 (8) FINANCIAL INSTITUTION.—The term “fi-
 17 nancial institution” has the same meaning as in sec-
 18 tion 509 of the Gramm-Leach-Bliley Act (15 U.S.C.
 19 6809).

20 (9) SENSITIVE ACCOUNT INFORMATION.—The
 21 term “sensitive account information” means a finan-
 22 cial account number relating to a consumer, includ-
 23 ing a credit card number or debit card number, in
 24 combination with any security code, access code,

password, or other personal identification information required to access the financial account.

(10) SENSITIVE PERSONAL INFORMATION.—

(A) IN GENERAL.—The term “sensitive personal information” means the first and last name, address, or telephone number of a consumer, in combination with any of the following relating to such consumer:

(i) Social security account number.

(ii) Driver’s license number or equivalent State identification number.

(iii) Taxpayer identification number.

(B) EXCEPTION.—The term “sensitive personal information” does not include publicly available information that is lawfully made available to the general public from—

(i) Federal, State, or local government records; or

(ii) widely distributed media.

(11) SUBSTANTIAL HARM OR INCONVENIENCE.—

(A) IN GENERAL.—The term “substantial harm or inconvenience” means—

(i) material financial loss to, or civil or criminal penalties imposed on, a con-

sumer, due to the unauthorized use of sensitive account information or sensitive personal information relating to such consumer; or

(ii) the need for a consumer to expend significant time and effort to correct erroneous information relating to the consumer, including information maintained by a consumer reporting agency, financial institution, or government entity, in order to avoid material financial loss, increased costs, or civil or criminal penalties, due to the unauthorized use of sensitive account information or sensitive personal information relating to such consumer.

(B) EXCEPTION.—The term “substantial harm or inconvenience” does not include—

(i) changing a financial account number or closing a financial account; or

(ii) harm or inconvenience that does not result from identity theft or account fraud.

SEC. 3. PROTECTION OF INFORMATION AND SECURITY
BREACH NOTIFICATION.

(a) SECURITY PROCEDURES REQUIRED.—

1 (1) IN GENERAL.—Each covered entity shall
2 implement, maintain, and enforce reasonable policies
3 and procedures to protect the confidentiality and se-
4 curity of sensitive account information and sensitive
5 personal information which is maintained or is being
6 communicated by or on behalf of a covered entity,
7 from the unauthorized use of such information that
8 is reasonably likely to result in substantial harm or
9 inconvenience to the consumer to whom such infor-
10 mation relates.

11 (2) LIMITATION.—Any policy or procedure im-
12 plemented or maintained under paragraph (1) shall
13 be appropriate to the—

14 (A) size and complexity of a covered entity;

15 (B) nature and scope of the activities of
16 such entity; and

17 (C) sensitivity of the consumer information
18 to be protected.

19 (b) INVESTIGATION REQUIRED.—

20 (1) IN GENERAL.—If a covered entity deter-
21 mines that a breach of data security has or may
22 have occurred in relation to sensitive account infor-
23 mation or sensitive personal information that is
24 maintained or is being communicated by, or on be-

1 half of, such covered entity, the covered entity shall
2 conduct an investigation—

3 (A) to assess the nature and scope of the
4 breach;

5 (B) to identify any sensitive account infor-
6 mation or sensitive personal information that
7 may have been involved in the breach; and

8 (C) to determine if such information is
9 reasonably likely to be misused in a manner
10 causing substantial harm or inconvenience to
11 the consumers to whom the information relates.

12 (2) NEURAL NETWORKS AND INFORMATION SE-
13 CURITY PROGRAMS.—In determining the likelihood
14 of misuse of sensitive account information under
15 paragraph (1)(C), a covered entity shall consider
16 whether any neural network or security program has
17 detected, or is likely to detect or prevent, fraudulent
18 transactions resulting from the breach of security.

19 (c) NOTICE REQUIRED.—If a covered entity deter-
20 mines under subsection (b)(1)(C) that sensitive account
21 information or sensitive personal information involved in
22 a breach of data security is reasonably likely to be misused
23 in a manner causing substantial harm or inconvenience
24 to the consumers to whom the information relates, such

1 covered entity, or a third party acting on behalf of such
 2 covered entity, shall—

3 (1) notify, in the following order—

4 (A) the appropriate agency or authority
 5 identified in section 5;

6 (B) an appropriate law enforcement agen-
 7 cy;

8 (C) any entity that owns, or is obligated
 9 on, a financial account to which the sensitive
 10 account information relates, if the breach in-
 11 volves a breach of sensitive account informa-
 12 tion;

13 (D) each consumer reporting agency that
 14 compiles and maintains files on consumers on a
 15 nationwide basis, if the breach involves sensitive
 16 personal information relating to 5,000 or more
 17 consumers; and

18 (E) all consumers to whom the sensitive
 19 account information or sensitive personal infor-
 20 mation relates; and

21 (2) take reasonable measures to restore the se-
 22 curity and confidentiality of the sensitive account in-
 23 formation or sensitive personal information involved
 24 in the breach.

25 (d) COMPLIANCE.—

1 (1) IN GENERAL.—A financial institution shall
2 be deemed to be in compliance with—

3 (A) subsection (a), and any regulations
4 prescribed under such subsection, if such insti-
5 tution maintains policies and procedures to pro-
6 tect the confidentiality and security of sensitive
7 account information and sensitive personal in-
8 formation that are consistent with the policies
9 and procedures of such institution that are de-
10 signed to comply with the requirements of sec-
11 tion 501(b) of the Gramm-Leach-Bliley Act (15
12 U.S.C. 6801(b)) and any regulations or guid-
13 ance prescribed under that section that are ap-
14 plicable to such institution; and

15 (B) subsections (b) and (c), and any regu-
16 lations prescribed under such subsections, if
17 such institution—

18 (i)(I) maintains policies and proce-
19 dures to investigate and provide notice to
20 consumers of breaches of data security
21 that are consistent with the policies and
22 procedures of such institution that are de-
23 signed to comply with the investigation and
24 notice requirements established by regula-
25 tions or guidance under section 501(b) of

1 the Gramm-Leach-Bliley Act (15 U.S.C.
2 6801(b)) that are applicable to such insti-
3 tution; or

4 (II) is an affiliate of a bank holding
5 company that maintains policies and proce-
6 dures to investigate and provide notice to
7 consumers of breaches of data security
8 that are consistent with the policies and
9 procedures of a bank that is an affiliate of
10 such institution, and that bank's policies
11 and procedures are designed to comply
12 with the investigation and notice require-
13 ments established by any regulations or
14 guidance under section 501(b) of the
15 Gramm-Leach-Bliley Act (15 U.S.C.
16 6801(b)) that are applicable to that bank;
17 and

18 (ii) provides for notice to the entities
19 described under subparagraphs (B), (C),
20 and (D) of subsection (c)(1), if notice is
21 provided to consumers pursuant to the
22 policies and procedures of such institution
23 described in clause (i).

24 (2) DEFINITIONS.—For purposes of this sub-
25 section, the terms “bank holding company” and

1 “bank” shall have the same meaning given such
2 terms under section 2 of the Bank Holding Com-
3 pany Act of 1956 (12 U.S.C. 1841).

4 **SEC. 4. IMPLEMENTING REGULATIONS.**

5 (a) IN GENERAL.—Except as provided under section
6 6, the agencies and authorities identified in section 5, with
7 respect to the covered entities that are subject to the re-
8 spective enforcement authority of such agencies and au-
9 thorities, shall prescribe regulations to implement this Act.

10 (b) COORDINATION.—Each agency and authority re-
11 quired to prescribe regulations under subsection (a) shall
12 consult and coordinate with each other agency and author-
13 ity identified in section 5 so that, to the extent possible,
14 the regulations prescribed by each agency and authority
15 are consistent and comparable.

16 (c) METHOD OF PROVIDING NOTICE TO CON-
17 SUMERS.—The regulations required under subsection (a)
18 shall—

19 (1) prescribe the methods by which a covered
20 entity shall notify a consumer of a breach of data se-
21 curity under section 3; and

22 (2) allow a covered entity to provide such notice
23 by—

24 (A) written, telephonic, or e-mail notifica-
25 tion; or

1 (B) substitute notification, if providing
2 written, telephonic, or e-mail notification is not
3 feasible due to—

4 (i) lack of sufficient contact informa-
5 tion for the consumers that must be noti-
6 fied; or

7 (ii) excessive cost to the covered enti-
8 ty.

9 (d) CONTENT OF CONSUMER NOTICE.—The regula-
10 tions required under subsection (a) shall—

11 (1) prescribe the content that shall be included
12 in a notice of a breach of data security that is re-
13 quired to be provided to consumers under section 3;
14 and

15 (2) require such notice to include—

16 (A) a description of the type of sensitive
17 account information or sensitive personal infor-
18 mation involved in the breach of data security;

19 (B) a general description of the actions
20 taken by the covered entity to restore the secu-
21 rity and confidentiality of the sensitive account
22 information or sensitive personal information
23 involved in the breach of data security; and

24 (C) the summary of rights of victims of
25 identity theft prepared by the Commission

1 under section 609(d) of the Fair Credit Report-
2 ing Act (15 U.S.C. 1681g), if the breach of
3 data security involves sensitive personal infor-
4 mation.

5 (e) TIMING OF NOTICE.—The regulations required
6 under subsection (a) shall establish standards for when
7 a covered entity shall provide any notice required under
8 section 3.

9 (f) LAW ENFORCEMENT DELAY.—The regulations
10 required under subsection (a) shall allow a covered entity
11 to delay providing notice of a breach of data security to
12 consumers under section 3 if a law enforcement agency
13 requests such a delay in writing.

14 (g) SERVICE PROVIDERS.—The regulations required
15 under subsection (a) shall—

16 (1) require any party that maintains or commu-
17 nicates sensitive account information or sensitive
18 personal information on behalf of a covered entity to
19 provide notice to that covered entity if such party
20 determines that a breach of data security has, or
21 may have, occurred with respect to such information;
22 and

23 (2) ensure that there is only 1 notification re-
24 sponsibility with respect to a breach of data security.

1 (h) TIMING OF REGULATIONS.—The regulations re-
 2 quired under subsection (a) shall—

- 3 (1) be issued in final form not later than 6
 4 months after the date of enactment of this Act; and
 5 (2) take effect not later than 6 months after
 6 the date on which they are issued in final form.

7 **SEC. 5. ADMINISTRATIVE ENFORCEMENT.**

8 (a) IN GENERAL.—Section 3, and the regulations re-
 9 quired under section 4, shall be enforced exclusively
 10 under—

- 11 (1) section 8 of the Federal Deposit Insurance
 12 Act (12 U.S.C. 1818), in the case of—

13 (A) a national bank, a Federal branch or
 14 Federal agency of a foreign bank, or any sub-
 15 sidiary thereof (other than a broker, dealer,
 16 person providing insurance, investment com-
 17 pany, or investment adviser), by the Office of
 18 the Comptroller of the Currency;

19 (B) a member bank of the Federal Reserve
 20 System (other than a national bank), a branch
 21 or agency of a foreign bank (other than a Fed-
 22 eral branch, Federal agency, or insured State
 23 branch of a foreign bank), a commercial lending
 24 company owned or controlled by a foreign bank,
 25 an organization operating under section 25 or

1 25A of the Federal Reserve Act (12 U.S.C.
2 601,604), or a bank holding company and its
3 nonbank subsidiary or affiliate (other than a
4 broker, dealer, person providing insurance, in-
5 vestment company, or investment adviser), by
6 the Board of Governors of the Federal Reserve
7 System;

8 (C) a bank, the deposits of which are in-
9 sured by the Federal Deposit Insurance Cor-
10 poration (other than a member of the Federal
11 Reserve System), an insured State branch of a
12 foreign bank, or any subsidiary thereof (other
13 than a broker, dealer, person providing insur-
14 ance, investment company, or investment ad-
15 viser), by the Board of Directors of the Federal
16 Deposit Insurance Corporation; and

17 (D) a savings association, the deposits of
18 which are insured by the Federal Deposit In-
19 surance Corporation, or any subsidiary thereof
20 (other than a broker, dealer, person providing
21 insurance, investment company, or investment
22 adviser), by the Director of the Office of Thrift
23 Supervision;

24 (2) the Federal Credit Union Act (12 U.S.C.
25 1751 et seq.), by the National Credit Union Admin-

1 istration Board with respect to any federally insured
2 credit union;

3 (3) the Securities Exchange Act of 1934 (15
4 U.S.C.78a et seq.), by the Securities and Exchange
5 Commission with respect to any broker or dealer;

6 (4) the Investment Company Act of 1940 (15
7 U.S.C. 80a–1 et seq.), by the Securities and Ex-
8 change Commission with respect to any investment
9 company;

10 (5) the Investment Advisers Act of 1940 (15
11 U.S.C. 80b–1 et seq.), by the Securities and Ex-
12 change Commission with respect to any investment
13 adviser registered with the Securities and Exchange
14 Commission under that Act;

15 (6) the Commodity Exchange Act (7 U.S.C. 1
16 et seq.), by the Commodity Futures Trading Com-
17 mission with respect to any futures commission mer-
18 chant, commodity trading advisor, commodity pool
19 operator, or introducing broker;

20 (7) the provisions of title XIII of the Housing
21 and Community Development Act of 1992 (12
22 U.S.C. 4501 et seq.), by the Director of Federal
23 Housing Enterprise Oversight (and any successor to
24 such functional regulatory agency) with respect to
25 the Federal National Mortgage Association, the Fed-

1 eral Home Loan Mortgage Corporation, and any
 2 other entity or enterprise (as defined in that title)
 3 subject to the jurisdiction of such functional regu-
 4 latory agency under that title, including any affiliate
 5 of any such enterprise;

6 (8) State insurance law, in the case of any per-
 7 son engaged in providing insurance, by the applica-
 8 ble State insurance authority of the State in which
 9 the person is domiciled; and

10 (9) the Federal Trade Commission Act (15
 11 U.S.C. 41 et seq.), by the Commission for any other
 12 covered entity that is not subject to the jurisdiction
 13 of any agency or authority described under para-
 14 graphs (1) through (8).

15 (b) EXTENSION OF FEDERAL TRADE COMMISSION
 16 ENFORCEMENT AUTHORITY.—The authority of the Com-
 17 mission to enforce compliance with section 3, and the reg-
 18 ulations required under section 4, under subsection (a)(8)
 19 shall—

20 (1) notwithstanding the Federal Aviation Act of
 21 1958 (49 U.S.C. App. 1301 et seq.), include the au-
 22 thority to enforce compliance by air carriers and for-
 23 eign air carriers; and

24 (2) notwithstanding the Packers and Stock-
 25 yards Act (7 U.S.C. 181 et seq.), include the author-

1 ity to enforce compliance by persons, partnerships,
2 and corporations subject to the provisions of that
3 Act.

4 (c) NO PRIVATE RIGHT OF ACTION.—

5 (1) IN GENERAL.—This Act, and the regula-
6 tions prescribed under this Act, may not be con-
7 strued to provide a private right of action, including
8 a class action with respect to any act or practice
9 regulated under this Act.

10 (2) CIVIL AND CRIMINAL ACTIONS.—No civil or
11 criminal action relating to any act or practice gov-
12 erned under this Act, or the regulations prescribed
13 under this Act, shall be commenced or maintained in
14 any State court or under State law, including a
15 pendent State claim to an action under Federal law.

16 **SEC. 6. PROTECTION OF INFORMATION AT FEDERAL AGEN-**
17 **CIES.**

18 (a) DATA SECURITY STANDARDS.—Each agency
19 shall implement appropriate standards relating to admin-
20 istrative, technical, and physical safeguards—

21 (1) to insure the security and confidentiality of
22 the sensitive account information and sensitive per-
23 sonal information that is maintained or is being
24 communicated by, or on behalf of, that agency;

1 (2) to protect against any anticipated threats or
2 hazards to the security of such information; and
3 (3) to protect against misuse of such informa-
4 tion, which could result in substantial harm or in-
5 convenience to a consumer.

6 (b) SECURITY BREACH NOTIFICATION STAND-
7 ARDS.—Each agency shall implement appropriate stand-
8 ards providing for notification of consumers when such
9 agency determines that sensitive account information or
10 sensitive personal information that is maintained or is
11 being communicated by, or on behalf of, such agency—

12 (1) has been acquired without authorization;
13 and

14 (2) is reasonably likely to be misused in a man-
15 ner causing substantial harm or inconvenience to the
16 consumers to whom the information relates.

17 **SEC. 7. RELATION TO STATE LAW.**

18 No requirement or prohibition may be imposed under
19 the laws of any State with respect to the responsibilities
20 of any person to—

21 (1) protect the security of information relating
22 to consumers that is maintained or communicated
23 by, or on behalf of, such person;

24 (2) safeguard information relating to consumers
25 from potential misuse;

1 (3) investigate or provide notice of the unau-
2 thorized access to information relating to consumers,
3 or the potential misuse of such information for
4 fraudulent, illegal, or other purposes; or

5 (4) mitigate any loss or harm resulting from
6 the unauthorized access or misuse of information re-
7 lating to consumers.

8 **SEC. 8. DELAYED EFFECTIVE DATE FOR CERTAIN PROVI-**
9 **SIONS.**

10 (a) COVERED ENTITIES.—Sections 3 and 7 shall take
11 effect on the later of—

12 (1) 1 year after the date of enactment of this
13 Act; or

14 (2) the effective date of the final regulations re-
15 quired under section 4.

16 (b) AGENCIES.—Section 6 shall take effect 1 year
17 after the date of enactment of this Act.

○