

109TH CONGRESS
1ST SESSION

S. 1216

To require financial institutions and financial service providers to notify customers of the unauthorized use of personal financial information, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JUNE 9, 2005

Mr. CORZINE introduced the following bill; which was read twice and referred to the Committee on Banking, Housing, and Urban Affairs

A BILL

To require financial institutions and financial service providers to notify customers of the unauthorized use of personal financial information, 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 “Financial Privacy
5 Breach Notification Act of 2005”.

6 **SEC. 2. TIMELY NOTIFICATION OF UNAUTHORIZED ACCESS**
7 **TO PERSONAL FINANCIAL INFORMATION.**

8 Subtitle B of title V of the Gramm-Leach-Bliley Act
9 (15 U.S.C. 6821 et seq.) is amended—

1 (1) by redesignating sections 526 and 527 as
 2 sections 528 and 529, respectively; and

3 (2) by inserting after section 525 the following:

4 **“SEC. 526. NOTIFICATION TO CUSTOMERS OF UNAUTHOR-**
 5 **IZED ACCESS TO PERSONAL FINANCIAL IN-**
 6 **FORMATION.**

7 “(a) DEFINITIONS.—In this section:

8 “(1) BREACH.—The term ‘breach’—

9 “(A) means the unauthorized acquisition,
 10 or loss, of computerized data or paper records
 11 which compromises the security, confidentiality,
 12 or integrity of personal financial information
 13 maintained by or on behalf of a financial insti-
 14 tution; and

15 “(B) does not include a good faith acquisi-
 16 tion of personal financial information by an em-
 17 ployee or agent of a financial institution for a
 18 business purpose of the institution, if the per-
 19 sonal financial information is not subject to fur-
 20 ther unauthorized disclosure.

21 “(2) PERSONAL FINANCIAL INFORMATION.—

22 The term ‘personal financial information’ means the
 23 last name of an individual in combination with any
 24 1 or more of the following data elements, when ei-

1 ther the name or the data elements are not
2 encrypted:

3 “(A) Social security number.

4 “(B) Driver’s license number or State
5 identification 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 the financial account of an in-
10 dividual.

11 “(b) NOTIFICATION TO CUSTOMERS RELATING TO
12 UNAUTHORIZED ACCESS OF PERSONAL FINANCIAL IN-
13 FORMATION.—

14 “(1) FINANCIAL INSTITUTION REQUIREMENT.—

15 In any case in which there has been a breach of per-
16 sonal financial information at a financial institution,
17 or such a breach is reasonably believed to have oc-
18 curred, the financial institution shall promptly no-
19 tify—

20 “(A) each customer affected by the viola-
21 tion or suspected violation;

22 “(B) each consumer reporting agency de-
23 scribed in section 603(p) of the Fair Credit Re-
24 porting Act (15 U.S.C. 1681a); and

1 “(C) appropriate law enforcement agencies,
2 in any case in which the financial institution
3 has reason to believe that the breach or sus-
4 pected breach affects a large number of cus-
5 tomers, including as described in subsection
6 (e)(1)(C), subject to regulations of the Federal
7 Trade Commission.

8 “(2) OTHER ENTITIES.—For purposes of para-
9 graph (1), any person that maintains personal finan-
10 cial information for or on behalf of a financial insti-
11 tution shall promptly notify the financial institution
12 of any case in which such customer information has
13 been, or is reasonably believed to have been,
14 breached.

15 “(c) TIMELINESS OF NOTIFICATION.—Notification
16 required by this section shall be made—

17 “(1) promptly and without unreasonable delay,
18 upon discovery of the breach or suspected breach;
19 and

20 “(2) consistent with—

21 “(A) the legitimate needs of law enforce-
22 ment, as provided in subsection (d); and

23 “(B) any measures necessary to determine
24 the scope of the breach or restore the reason-

1 able integrity of the information security system
2 of the financial institution.

3 “(d) DELAYS FOR LAW ENFORCEMENT PURPOSES.—

4 Notification required by this section may be delayed if a
5 law enforcement agency determines that the notification
6 would impede a criminal investigation, and in any such
7 case, notification shall be made promptly after the law en-
8 forcement agency determines that it would not com-
9 promise the investigation.

10 “(e) FORM OF NOTICE.—Notification required by
11 this section may be provided—

12 “(1) to a customer—

13 “(A) in written notification;

14 “(B) in electronic form, if the notice pro-
15 vided is consistent with the provisions regarding
16 electronic records and signatures set forth in
17 section 101 of the Electronic Signatures in
18 Global and National Commerce Act (15 U.S.C.
19 7001);

20 “(C) if the Federal Trade Commission de-
21 termines that the number of all customers af-
22 fected by, or the cost of providing notifications
23 relating to, a single breach or suspected breach
24 would make other forms of notification prohibi-
25 tive, or in any case in which the financial insti-

1 tution certifies in writing to the Federal Trade
2 Commission that it does not have sufficient cus-
3 tomer contact information to comply with other
4 forms of notification, in the form of—

5 “(i) an e-mail notice, if the financial
6 institution has access to an e-mail address
7 for the affected customer that it has rea-
8 son to believe is accurate;

9 “(ii) a conspicuous posting on the
10 Internet website of the financial institu-
11 tion, if the financial institution maintains
12 such a website; or

13 “(iii) notification through the media
14 that a breach of personal financial infor-
15 mation has occurred or is suspected that
16 compromises the security, confidentiality,
17 or integrity of customer information of the
18 financial institution; or

19 “(D) in such other form as the Federal
20 Trade Commission may by rule prescribe; and

21 “(2) to consumer reporting agencies and law
22 enforcement agencies (where appropriate), in such
23 form as the Federal Trade Commission may pre-
24 scribe, by rule.

1 “(f) CONTENT OF NOTIFICATION.—Each notification
2 to a customer under subsection (b) shall include—

3 “(1) a statement that—

4 “(A) credit reporting agencies have been
5 notified of the relevant breach or suspected
6 breach; and

7 “(B) the credit report and file of the cus-
8 tomer will contain a fraud alert to make credi-
9 tors aware of the breach or suspected breach,
10 and to inform creditors that the express author-
11 ization of the customer is required for any new
12 issuance or extension of credit (in accordance
13 with section 605(g) of the Fair Credit Report-
14 ing Act); and

15 “(2) such other information as the Federal
16 Trade Commission determines is appropriate.

17 “(g) COMPLIANCE.—Notwithstanding subsection (e),
18 a financial institution shall be deemed to be in compliance
19 with this section, if—

20 “(1) the financial institution has established a
21 comprehensive information security program that is
22 consistent with the standards prescribed by the ap-
23 propriate regulatory body under section 501(b);

24 “(2) the financial institution notifies affected
25 customers and consumer reporting agencies in ac-

1 cordance with its own internal information security
2 policies in the event of a breach or suspected breach
3 of personal financial information; and

4 “(3) such internal security policies incorporate
5 notification procedures that are consistent with the
6 requirements of this section and the rules of the
7 Federal Trade Commission under this section.

8 “(h) CIVIL PENALTIES.—

9 “(1) DAMAGES.—Any customer injured by a
10 violation of this section may institute a civil action
11 to recover damages arising from that violation.

12 “(2) INJUNCTIONS.—Actions of a financial in-
13 stitution in violation or potential violation of this
14 section may be enjoined.

15 “(3) CUMULATIVE EFFECT.—The rights and
16 remedies available under this section are in addition
17 to any other rights and remedies available under ap-
18 plicable law.

19 “(i) RULES OF CONSTRUCTION.—

20 “(1) IN GENERAL.—Compliance with this sec-
21 tion by a financial institution shall not be construed
22 to be a violation of any provision of subtitle (A), or
23 any other provision of Federal or State law prohib-
24 iting the disclosure of financial information to third
25 parties.

1 “(2) LIMITATION.—Except as specifically pro-
2 vided in this section, nothing in this section requires
3 or authorizes a financial institution to disclose infor-
4 mation that it is otherwise prohibited from disclosing
5 under subtitle A or any other provision of Federal
6 or State law.

7 “(j) ENFORCEMENT.—The Federal Trade Commis-
8 sion is authorized to enforce compliance with this section,
9 including the assessment of fines for violations of sub-
10 section (b)(1).”.

11 **SEC. 3. EFFECTIVE DATE.**

12 This Act shall take effect on the expiration of the
13 date which is 6 months after the date of enactment of
14 this Act.

○