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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Financial Privacy Breach Notification Act of 2005''.

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

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

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

(2) by inserting after section 525 the following:

"SEC. 526. NOTIFICATION TO CUSTOMERS OF UNAUTHORIZED ACCESS TO PERSONAL FINANCIAL INFORMATION.

''(a) DEFINITIONS.—In this section:

''(1) BREACH.—The term 'breach'—

''(A) means the unauthorized acquisition, or loss, of computerized data or paper records which compromises the security, confidentiality, or integrity of personal financial information maintained by or on behalf of a financial institution; and

''(B) does not include a good faith acquisition of personal financial information by an employee or agent of a financial institution for a business purpose of the institution, if the personal financial information is not subject to further unauthorized disclosure.

''(2) PERSONAL FINANCIAL INFORMATION.—The term 'personal financial information' means the last name of an individual in combination with any 1 or more of the following data elements, when ei-

ther the name or the data elements are not encrypted:

"(A) Social security number.

"(B) Driver's license number or State identification number.

"(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to the financial account of an individual.

"(b) NOTIFICATION TO CUSTOMERS RELATING TO UNAUTHORIZED ACCESS OF PERSONAL FINANCIAL INFORMATION.—

"(1) FINANCIAL INSTITUTION REQUIREMENT.—In any case in which there has been a breach of personal financial information at a financial institution, or such a breach is reasonably believed to have occurred, the financial institution shall promptly notify—

"(A) each customer affected by the violation or suspected violation;

"(B) each consumer reporting agency described in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a); and

''(C) appropriate law enforcement agencies, in any case in which the financial institution has reason to believe that the breach or suspected breach affects a large number of customers, including as described in subsection (e)(1)(C), subject to regulations of the Federal Trade Commission.

''(2) OTHER ENTITIES.—For purposes of paragraph (1), any person that maintains personal financial information for or on behalf of a financial institution shall promptly notify the financial institution of any case in which such customer information has been, or is reasonably believed to have been, breached.

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

''(1) promptly and without unreasonable delay, upon discovery of the breach or suspected breach; and

''(2) consistent with—

''(A) the legitimate needs of law enforcement, as provided in subsection (d); and

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

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

''(d) DELAYS FOR LAW ENFORCEMENT PURPOSES.—Notification required by this section may be delayed if a law enforcement agency determines that the notification would impede a criminal investigation, and in any such case, notification shall be made promptly after the law enforcement agency determines that it would not compromise the investigation.

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

''(1) to a customer—

''(A) in written notification;

''(B) in electronic form, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001);

''(C) if the Federal Trade Commission determines that the number of all customers affected by, or the cost of providing notifications relating to, a single breach or suspected breach would make other forms of notification prohibitive, or in any case in which the financial insti-

tution certifies in writing to the Federal Trade Commission that it does not have sufficient customer contact information to comply with other forms of notification, in the form of—

"(i) an e-mail notice, if the financial institution has access to an e-mail address for the affected customer that it has reason to believe is accurate;

"(ii) a conspicuous posting on the Internet website of the financial institution, if the financial institution maintains such a website; or

"(iii) notification through the media that a breach of personal financial information has occurred or is suspected that compromises the security, confidentiality, or integrity of customer information of the financial institution; or

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

"(2) to consumer reporting agencies and law enforcement agencies (where appropriate), in such form as the Federal Trade Commission may prescribe, by rule.

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

''(1) a statement that—

''(A) credit reporting agencies have been notified of the relevant breach or suspected breach; and

''(B) the credit report and file of the customer will contain a fraud alert to make creditors aware of the breach or suspected breach, and to inform creditors that the express authorization of the customer is required for any new issuance or extension of credit (in accordance with section 605(g) of the Fair Credit Reporting Act); and

''(2) such other information as the Federal Trade Commission determines is appropriate.

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

''(1) the financial institution has established a comprehensive information security program that is consistent with the standards prescribed by the appropriate regulatory body under section 501(b);

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

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

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

''(h) CIVIL PENALTIES.—

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

''(2) INJUNCTIONS.—Actions of a financial institution in violation or potential violation of this section may be enjoined.

''(3) CUMULATIVE EFFECT.—The rights and remedies available under this section are in addition to any other rights and remedies available under applicable law.

''(i) RULES OF CONSTRUCTION.—

''(1) IN GENERAL.—Compliance with this section by a financial institution shall not be construed to be a violation of any provision of subtitle (A), or any other provision of Federal or State law prohibiting the disclosure of financial information to third parties.

''(2) LIMITATION.—Except as specifically provided in this section, nothing in this section requires or authorizes a financial institution to disclose information that it is otherwise prohibited from disclosing under subtitle A or any other provision of Federal or State law.

''(j) ENFORCEMENT.—The Federal Trade Commission is authorized to enforce compliance with this section, including the assessment of fines for violations of subsection (b)(1).''.

SEC. 3. EFFECTIVE DATE.

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

○