II

109TH CONGRESS
1ST SESSION

S. 1594

To require financial services providers to maintain customer information security systems and to notify customers of unauthorized access to personal information, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JULY 29, 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 services providers to maintain customer information security systems and to notify customers of unauthorized access to personal 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 Protection Act of 2005''.

SEC. 2. PREVENTION OF IDENTITY THEFT; NOTIFICATION OF UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION.

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

(1) by striking section 525;

(2) by redesignating sections 522 through 524 as sections 523 through 525, respectively;

(3) in section 525, as redesignated, by striking ''section 522'' and inserting ''section 523''; and

(4) by inserting after section 521 the following:

''SEC. 522. PREVENTION OF IDENTITY THEFT; NOTIFICATION OF UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION.

''(a) CUSTOMER INFORMATION SECURITY SYSTEM REQUIRED.—

''(1) IN GENERAL.—In accordance with regulations issued under paragraph (2), each financial institution shall develop and maintain a customer information security system, including policies, procedures, and controls designed to prevent any breach with respect to the customer information of the financial institution.

''(2) REGULATIONS.—

''(A) IN GENERAL.—Each of the Federal functional regulators shall issue regulations re-

garding the policies, procedures, and controls required by paragraph (1) applicable to the financial institutions that are subject to their respective enforcement authority under section 523.

''(B) SPECIFIC REQUIREMENTS.—The regulations required by subparagraph (A) shall—

''(i) require the chief compliance officer or chief executive officer of a financial institution to personally attest that the customer information security system of the financial institution is in compliance with Federal and other applicable standards and is subject to an ongoing system of monitoring;

''(ii) require audits by the issuing agency (or submitted to the issuing agency by an independent auditor paid for by the financial institution to audit the financial institution on behalf of the issuing agency) of the customer information security system of a financial institution not less frequently than once every 5 years;

''(iii) require the imposition by the issuing agency of appropriate monetary

penalties for failure to comply with applicable customer information security standards; and

''(iv) include such other requirements or restrictions as the issuing agency considers appropriate to carry out this section.

''(C) EFFECTIVE DATE.—Regulations issued under this paragraph shall become effective 6 months after the effective date of the Financial Privacy Protection Act of 2005.

''(b) NOTIFICATION TO CUSTOMERS OF UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION.—

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

''(A) each customer whose customer information was or is reasonably believed to have been accessed in connection with the breach or suspected breach;

''(B) the appropriate Federal functional regulator or regulators with respect to the financial institutions that are subject to their respective enforcement authority;

''(C) each consumer reporting agency described in section 603(p) of the Fair Credit Reporting Act; and

''(D) 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 paragraph (5)(A)(iii), subject to regulations of the Federal Trade Commission.

''(2) OTHER ENTITIES.—For purposes of paragraph (1), any person that maintains customer 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.

''(3) TIMELINESS OF NOTIFICATION.—Notification required by this subsection shall be made—

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

''(B) consistent with—

''(i) the legitimate needs of law enforcement, as provided in paragraph (4); and

''(ii) any measures necessary to determine the scope of the breach or restore the reasonable integrity of the customer information security system of the financial institution.

''(4) DELAYS FOR LAW ENFORCEMENT PURPOSES.—Notification required by this subsection may be delayed if a law enforcement agency determines that the notification would seriously 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.

''(5) FORM OF NOTICE.—Notification required by this subsection may be provided—

''(A) to a customer—

''(i) in writing;

''(ii) 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;

''(iii) if the number of people affected by the breach exceeds 500,000 or the cost

of notification exceeds $500,000, or a higher number or numbers determined by the Federal Trade Commission, such that 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 institution certifies in writing to the Federal Trade Commission that it does not have sufficient customer contact information to comply with other forms of notification with respect to some customers, then for those customers, in the form of—

''(I) a conspicuous posting on the Internet website of the financial institution, if the financial institution maintains such a website; and

''(II) notification through major media in all major cities and regions in which the customers whose customer information is suspected to have been breached reside, that a breach has occurred, or is suspected, that compromises the security, confidentiality, or integrity of customer

information of the financial institution; or

''(iv) in such additional forms as the Federal Trade Commission may by rule prescribe; and

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

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

''(A) a statement that—

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

''(ii) notwithstanding any other provision of law, the customer may elect to place a fraud alert in the file of the consumer 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 accord-

ance with section 605A of the Fair Credit Reporting Act); and

"(B) such other information as the Federal Trade Commission determines is appropriate.

"(7) COMPLIANCE.—Notwithstanding paragraph (5), a financial institution shall be deemed to be in compliance with this subsection, if—

"(A) the financial institution has established a comprehensive customer information security system that is consistent with the standards prescribed by the appropriate Federal functional regulator under subsection (a);

"(B) the financial institution notifies affected customers and consumer reporting agencies in accordance with its own internal information security policies in the event of a breach or suspected breach; and

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

"(8) RULES OF CONSTRUCTION.—

"(A) IN GENERAL.—Compliance with this subsection 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.

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

''(c) CIVIL PENALTIES.—

''(1) DAMAGES.—Any customer adversely affected by an act or practice that violates 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 any other provision of applicable State or Federal law.

''(d) CIVIL ACTIONS BY STATE ATTORNEYS GENERAL.—

''(1) AUTHORITY OF STATE ATTORNEYS GENERAL.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by an act or practice that violates this section, the State may bring a civil action on behalf of the residents of that State in a district court of the United States of appropriate jurisdiction, or any other court of competent jurisdiction—

''(A) to enjoin that act or practice;

''(B) to enforce compliance with this section;

''(C) to obtain—

''(i) damages in the sum of actual damages, restitution, or other compensation on behalf of affected residents of the State; and

''(ii) punitive damages, if the violation is willful or intentional; or

''(D) obtain such other legal and equitable relief as the court may consider to be appropriate.

''(2) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this section shall be construed to prevent

an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State—

"(A) to conduct investigations;

"(B) to administer oaths and affirmations; or

"(C) to compel the attendance of witnesses or the production of documentary and other evidence.

"(3) VENUE.—Any action brought under this subsection may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1931 of title 28, United States Code.

"(4) SERVICE OF PROCESS.—In an action brought under this subsection, process may be served in any district in which the defendant—

"(A) is an inhabitant; or

"(B) may be found.".

SEC. 3. DEFINITIONS.

Section 527 of the Gramm-Leach-Bliley Act (15 U.S.C. 6827) is amended—

(1) by redesignating paragraph (4) as paragraph (6);

(2) by redesignating paragraphs (1) through (3) as paragraphs (2) through (4), respectively;

(3) by inserting before paragraph (2), as redesignated, the following:

''(1) BREACH.—The term 'breach'—

''(A) means the unauthorized acquisition, disclosure, or loss of computerized data or paper records which compromises the security, confidentiality, or integrity of customer information, including activities proscribed under section 521; and

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

(4) in paragraph (2), as redesignated—

(A) by striking ''person) to whom'' and inserting the following: ″person)—

''(A) to whom''; and

(B) by striking the period at the end and inserting the following: ''; and

''(B) with respect to whom the financial institution maintains information in any form, re-

gardless of whether the financial institution is providing a product or service to or on behalf of that person.'';

(5) in paragraph (3), as redesignated—

(A) by striking ''institution' means any'' and inserting the following: ''institution'—

''(A) means any'';

(B) by inserting ''(regardless of whether the financial institution is providing any product or service to or on behalf of that customer)'' before ''and is identified''; and

(C) by striking the period at the end and inserting the following: ''; and

''(B) for purposes of section 522, includes the last name of an individual in combination with any 1 or more of the following data elements, when either the name or the data elements are not encrypted:

''(i) Social security number.

''(ii) Driver's license number or State identification number.

''(iii) Account number, credit or debit card number, or any required security code, access code, or password that would

permit access to a financial account of the individual.

''(iv) Such other information as the Federal functional regulators determine is appropriate with respect to the financial institutions that are subject to their respective enforcement authority.''; and

(6) by inserting before paragraph (6), as redesignated, the following:

''(5) FEDERAL FUNCTIONAL REGULATOR.—The term 'Federal functional regulator' has the same meaning as in section 509, and includes the Federal Trade Commission.''.

SEC. 4. INCLUSION OF FRAUD ALERTS IN CONSUMER CREDIT REPORTS.

Section 605A of the Fair Credit Reporting Act (15 U.S.C. 1681c–1) is amended–

(1) in subsection (b)(1), by inserting ''or proof of a notification of a breach or suspected breach under section 522(b)(1)(C) of the Gramm-Leach-Bliley Act'' after ''theft report''; and

(2) by adding at the end the following:

''(i) NO ADVERSE ACTION BASED SOLELY ON FRAUD ALERT.—It shall be a violation of this title for the user of a consumer report to take any adverse action with re-

spect to a consumer based solely on the inclusion of a fraud alert, extended alert, or active duty alert in the file of that consumer, as required by this subsection.''.

SEC. 5. STUDIES AND REPORTS ON IMPROVING PROTECTION OF CUSTOMER INFORMATION.

(a) ALTERNATIVE INFORMATION STORAGE METHODS.—

(1) STUDY.—The Federal Trade Commission shall conduct a study of alternative technologies, including biometrics, that may be used by financial institutions and other businesses to enhance the safeguarding of the customer information of financial institutions and other sensitive personal information. Such study shall include an analysis of how to ensure that such information does not become widespread or subject to theft.

(2) REPORT TO CONGRESS.—The Commission shall submit a report to the Congress on the results of the study conducted under paragraph (1) not later than 6 months after the date of enactment of this Act.

(b) TRANSPORTATION OF CUSTOMER INFORMATION.—

(1) STUDY.—The Comptroller General of the United States, in consultation with the Federal func-

tional regulators and appropriate law enforcement agencies, shall conduct a study of the cross country transport of the customer information of financial institutions and other sensitive personal information by or on behalf of financial institutions and other businesses.

(2) REPORT TO CONGRESS.—The Comptroller General shall submit a report to the Congress on the results of the study conducted under paragraph (1) not later than 6 months after the date of enactment of this Act, including any recommendations on ways that financial institutions may best reduce the risk of compromise, breach, or loss of the customer information of financial institutions and other sensitive personal information during transport.

SEC. 6. EFFECTIVE DATE.

This Act and the amendments made by this Act shall take effect 6 months after the date of enactment of this Act.

○