I

109TH CONGRESS
1ST SESSION

H. R. 1069

To require Federal agencies, and persons engaged in interstate commerce, in possession of electronic data containing personal information, to disclose any unauthorized acquisition of such information, to amend the Gramm-Leach-Bliley Act to require financial institutions to disclose to customers and consumer reporting agencies any unauthorized access to personal information, to amend the Fair Credit Reporting Act to require consumer reporting agencies to implement a fraud alert with respect to any consumer when the agency is notified of any such unauthorized access, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MARCH 3, 2005

Ms. BEAN (for herself, Mr. EMANUEL, Mr. GUTIERREZ, Ms. SLAUGHTER, Mr. VAN HOLLEN, Mr. TOWNS, Mrs. MALONEY, Mr. LIPINSKI, Mr. MCDERMOTT, Ms. SCHAKOWSKY, Mr. BRADY of Pennsylvania, and Mr. DEFAZIO) introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committees on Government Reform and Financial Services, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To require Federal agencies, and persons engaged in interstate commerce, in possession of electronic data containing personal information, to disclose any unauthorized acquisition of such information, to amend the Gramm-Leach-Bliley Act to require financial institutions to disclose to customers and consumer reporting agencies any unauthorized access to personal information, to

amend the Fair Credit Reporting Act to require consumer reporting agencies to implement a fraud alert with respect to any consumer when the agency is notified of any such unauthorized access, 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 ''Notification of Risk to Personal Data Act''.

SEC. 2. DEFINITIONS.

In this Act, the following definitions shall apply:

(1) AGENCY.—The term ''agency'' has the same meaning given such term in section 551(1) of title 5, United States Code.

(2) BREACH OF SECURITY OF THE SYSTEM.—The term ''breach of security of the system''—

(A) means the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition or loss of, and access to, personal information maintained by the person or business; and

(B) does not include good faith acquisition of personal information by an employee or agent of the person or business for the purposes

of the person or business, if the personal information is not used or subject to further unauthorized disclosure.

(3) PERSON.—The term ''person'' has the same meaning given such term in section 551(2) of title 5, United States Code.

(4) PERSONAL INFORMATION.—The term ''personal information'' means an individual's last name in combination with any 1 or more of the following data elements, when either 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 an individual's financial account.

(5) SUBSTITUTE NOTICE.—The term ''substitute notice'' means—

(A) e-mail notice, if the agency or person has an e-mail address for the subject persons;

(B) conspicuous posting of the notice on the Internet site of the agency or person, if the agency or person maintains an Internet site; or

(C) notification to major media.

SEC. 3. DATABASE SECURITY FOR AGENCIES AND NON-FINANCIAL INSTITUTIONS.

(a) DISCLOSURE OF SECURITY BREACH.—

(1) IN GENERAL.—Any agency, or person engaged in interstate commerce, that owns or licenses electronic data containing personal information shall, following the discovery of a breach of security of the system containing such data, notify—

(A) any resident of the United States whose unencrypted personal information was, or is reasonably believed to have been, lost or acquired by an unauthorized person; and

(B) each consumer reporting agency described in section 603(p) of the Fair Credit Reporting Act of such loss or unauthorized acquisition with respect to such consumer.

(2) NOTIFICATION OF OWNER OR LICENSEE.—Any agency, or person engaged in interstate commerce, in possession of electronic data containing personal information that the agency does not own or license shall notify the owner or licensee of the in-

formation if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of security of the system containing such data.

(3) TIMELINESS OF NOTIFICATION.—Except as provided in paragraph (4), all notifications required under paragraph (1) or (2) shall be made as expediently as possible and without unreasonable delay following—

(A) the discovery by the agency or person of a breach of security of the system; and

(B) any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.

(4) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT PURPOSES.—If a law enforcement agency determines that the notification required under this subsection would impede a criminal investigation, such notification may be delayed until such law enforcement agency determines that the notification will no longer compromise such investigation.

(5) METHODS OF NOTICE.—An agency, or person engaged in interstate commerce, shall be in com-

pliance with this subsection if it provides the resident, owner, or licensee, as appropriate, with—

(A) written notification;

(B) e-mail notice, if the person or business has an e-mail address for the subject person; or

(C) substitute notice, if—

(i) the agency or person demonstrates that the cost of providing direct notice would exceed $250,000;

(ii) the affected class of subject persons to be notified exceeds 500,000; or

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

(6) ALTERNATIVE NOTIFICATION PROCEDURES.—Notwithstanding any other obligation under this subsection, an agency, or person engaged in interstate commerce, shall be deemed to be in compliance with this subsection if the agency or person—

(A) maintains its own reasonable notification procedures as part of an information security policy for the treatment of personal information; and

(B) notifies subject persons in accordance with its information security policy in the event of a breach of security of the system.

(7) REASONABLE NOTIFICATION PROCEDURES.—As used in paragraph (6), with respect to a breach of security of the system involving personal information described in section 2(4)(C), the term ''reasonable notification procedures'' means procedures that—

(A) use a security program reasonably designed to block unauthorized transactions before they are charged to the customer's account; and

(B) provide for notice to be given by the owner or licensee of the database, or another party acting on behalf of such owner or licensee, after the security program indicates that the breach of security of the system has resulted in fraud or unauthorized transactions, but does not necessarily require notice in other circumstances.

(8) NOTICE TO INFORMATION CLEARINGHOUSE.—In addition to any other notice requirement under this subsection, an agency or person engaged in interstate commerce shall—

(A) notify the information clearinghouse established by the Federal Trade Commission under section 7 upon the occurrence of any breach for which notice is required under paragraph (1); and

(B) provide such information as the Commission may require with respect to the circumstances and manner of the breach and the system on which the breach occurred.

(b) CIVIL REMEDIES.—

(1) PENALTIES.—Any agency, or person engaged in interstate commerce, that violates this section shall be subject to a fine of not more than $5,000 per violation, to a maximum of $25,000 per day while such violations persist.

(2) EQUITABLE RELIEF.—Any person engaged in interstate commerce that violates, proposes to violate, or has violated this section may be enjoined from further violations by a court of competent jurisdiction.

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

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

(d) COORDINATION WITH OTHER PROVISIONS OF LAW.—This section shall not apply with respect to a financial institution (as defined in section 509(3) of the Gramm-Leach-Bliley Act) that is subject to section 526 of such Act.

SEC. 4. TIMELY NOTIFICATION BY FINANCIAL INSTITUTIONS OF UNAUTHORIZED ACCESS TO PERSONAL 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 INFORMATION.

"(a) DEFINITIONS.—For purposes of this section, the following definitions shall apply:

"(1) BREACH.—The term 'breach'—

"(A) means unauthorized acquisition or loss of computerized data or paper records which compromises the security, confidentiality,

or integrity of personal information maintained by or on behalf of a financial institution; and

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

''(2) PERSONAL INFORMATION.—With respect to a customer of a financial institution, the term 'personal information' means the first name or first initial and last name of the customer, in combination with any 1 or more of the following data elements, when either the name or the data element is not encrypted:

''(A) A social security number.

''(B) A driver's license number or other officially recognized form of identification.

''(C) A credit card number, debit card number, or any required security code, access code, or password that would permit access to financial account information relating to that customer.

''(b) NOTIFICATION RELATING TO BREACH OF PERSONAL INFORMATION.—

"(1) FINANCIAL INSTITUTION REQUIREMENT.—In any case in which there has been a breach of personal 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;

"(C) the information clearinghouse established by the Federal Trade Commission under section 7 of the Notification of Risk to Personal Data Act (together with such information as the Commission may require with respect to the circumstances and manner of the breach and the system on which the breach occurred); 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 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 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) TIMING.—Any 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 reasonable integrity of the information security system of the financial institution.

''(d) DELAYS FOR LAW ENFORCEMENT PURPOSES.—Any 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.—Any notification required by this section may be provided—

"(1) to a customer—

"(A) in writing;

"(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;

"(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 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, 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 institu-

tion, if the financial institution maintains such a website; or

''(iii) notification through the media that a breach of personal 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 accordance with its own internal information security policies in the event of a breach or suspected breach of personal 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.

''(3) NO NEW RECORDKEEPING OBLIGATION.—No provision of this section shall be construed as creating an obligation on the part of a financial institution to obtain, retain, or maintain information or records that are not otherwise required to be ob-

tained, retained, or maintained in the ordinary course of business of the financial institution or under other applicable law.''.

SEC. 5. INCLUSION OF FRAUD ALERTS IN CONSUMER CREDIT REPORTS.

Section 605A(a) of the Fair Credit Reporting Act (15 U.S.C. 1681c–1(a)) is amended by adding at the end the following new paragraph:

''(3) TREATMENT OF NOTICE OF A BREACH AS A REQUEST FROM THE CONSUMER FOR AN INITIAL ALERT.—A consumer reporting agency described in section 603(p) shall take the action required under paragraph (1) with respect to any consumer and the file of any consumer upon receiving notice of a breach of personal information with respect to such consumer from—

''(A) an agency or person engaged in interstate commerce pursuant to section 3(a) of the Notification of Risk to Personal Data Act; or

''(B) a financial institution pursuant to section 526(b)(1)(B) of the Gramm-Leach-Bliley Act .''.

SEC. 6. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) IN GENERAL.—

(1) CIVIL ACTIONS.—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 the engagement of any person in a practice that is prohibited under this Act or the amendments made by this Act, the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to—

(A) enjoin that practice;

(B) enforce compliance with this Act;

(C) obtain damage, restitution, or other compensation on behalf of residents of the State; or

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

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Attorney General (or the Federal functional regulator, in the case of a financial institution (as such terms are defined in section 509 of the Gramm-Leach-Bliley Act))—

(i) written notice of the action; and

(ii) a copy of the complaint for the action.

(B) EXEMPTION.—

(i) IN GENERAL.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the State attorney general determines that it is not feasible to provide the notice described in such subparagraph before the filing of the action.

(ii) NOTIFICATION.—In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the Attorney General or the Federal functional regulator at the time the State attorney general files the action.

(b) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on such attorney general by the laws of that State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

(3) compel the attendance of witnesses or the production of documentary and other evidence.

(c) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

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

(A) is an inhabitant; or

(B) may be found.

SEC. 7. FEDERAL INFORMATION CLEARINGHOUSE.

(a) IN GENERAL.—The Federal Trade Commission shall establish and maintain a clearinghouse to collect and analyze information submitted under section 3(a)(7) of this Act and section 526(b)(1)(C) of the Gramm-Leach-Bliley Act.

(b) ANNUAL REPORT.—The Federal Trade Commission, in consultation with the Federal functional regulators, shall submit an annual report to the Congress containing—

(1) containing a summary of the types of breaches that have occurred during the period cov-

ered by the report and an identification of trends in the manner in which unauthorized access to and acquisition of personal information is being accomplished; and

(2) such recommendations for administrative or legislative action as the Commission or any Federal functional regulator may determine to be appropriate.

SEC. 8. EFFECT ON STATE LAW.

The provisions of this Act shall supersede any inconsistent provisions of law of any State or unit of local government relating to the notification of any resident of the United States of any breach of security of an electronic database containing such resident's personal information (as defined in this Act), except as provided under sections 1798.82 and 1798.29 of the California Civil Code.

SEC. 9. EFFECTIVE DATE.

This Act, and the amendments made by this Act, shall take effect at the end of the 6-month period beginning on the date of the enactment of this Act.

○