111TH CONGRESS
1ST SESSION

S. 139

To require Federal agencies, and persons engaged in interstate commerce, in possession of data containing sensitive personally identifiable information, to disclose any breach of such information.

IN THE SENATE OF THE UNITED STATES

JANUARY 6, 2009

Mrs. FEINSTEIN introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

A BILL

To require Federal agencies, and persons engaged in interstate commerce, in possession of data containing sensitive personally identifiable information, to disclose any breach of such information.

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 ''Data Breach Notification Act''.

SEC. 2. NOTICE TO INDIVIDUALS.

(a) IN GENERAL.—Any agency, or business entity engaged in interstate commerce, that uses, accesses, trans-

mits, stores, disposes of or collects sensitive personally identifiable information shall, following the discovery of a security breach of such information notify any resident of the United States whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed, or acquired.

(b) OBLIGATION OF OWNER OR LICENSEE.—

(1) NOTICE TO OWNER OR LICENSEE.—Any agency, or business entity engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information that the agency or business entity does not own or license shall notify the owner or licensee of the information following the discovery of a security breach involving such information.

(2) NOTICE BY OWNER, LICENSEE OR OTHER DESIGNATED THIRD PARTY.—Nothing in this Act shall prevent or abrogate an agreement between an agency or business entity required to give notice under this section and a designated third party, including an owner or licensee of the sensitive personally identifiable information subject to the security breach, to provide the notifications required under subsection (a).

(3) BUSINESS ENTITY RELIEVED FROM GIVING NOTICE.—A business entity obligated to give notice under subsection (a) shall be relieved of such obligation if an owner or licensee of the sensitive personally identifiable information subject to the security breach, or other designated third party, provides such notification.

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—All notifications required under this section shall be made without unreasonable delay following the discovery by the agency or business entity of a security breach.

(2) REASONABLE DELAY.—Reasonable delay under this subsection may include any time necessary to determine the scope of the security breach, prevent further disclosures, and restore the reasonable integrity of the data system and provide notice to law enforcement when required.

(3) BURDEN OF PROOF.—The agency, business entity, owner, or licensee required to provide notification under this section shall have the burden of demonstrating that all notifications were made as required under this Act, including evidence demonstrating the reasons for any delay.

(d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT PURPOSES.—

(1) IN GENERAL.—If a Federal law enforcement agency determines that the notification required under this section would impede a criminal investigation, such notification shall be delayed upon written notice from such Federal law enforcement agency to the agency or business entity that experienced the breach.

(2) EXTENDED DELAY OF NOTIFICATION.—If the notification required under subsection (a) is delayed pursuant to paragraph (1), an agency or business entity shall give notice 30 days after the day such law enforcement delay was invoked unless a Federal law enforcement agency provides written notification that further delay is necessary.

(3) LAW ENFORCEMENT IMMUNITY.—No cause of action shall lie in any court against any law enforcement agency for acts relating to the delay of notification for law enforcement purposes under this Act.

SEC. 3. EXEMPTIONS.

(a) EXEMPTION FOR NATIONAL SECURITY AND LAW ENFORCEMENT.—

(1) IN GENERAL.—Section 2 shall not apply to an agency or business entity if the agency or business entity certifies, in writing, that notification of the security breach as required by section 2 reasonably could be expected to—

(A) cause damage to the national security; or

(B) hinder a law enforcement investigation or the ability of the agency to conduct law enforcement investigations.

(2) LIMITS ON CERTIFICATIONS.—An agency or business entity may not execute a certification under paragraph (1) to—

(A) conceal violations of law, inefficiency, or administrative error;

(B) prevent embarrassment to a business entity, organization, or agency; or

(C) restrain competition.

(3) NOTICE.—In every case in which an agency or business entity issues a certification under paragraph (1), the certification, accompanied by a description of the factual basis for the certification, shall be immediately provided to the United States Secret Service.

(4) SECRET SERVICE REVIEW OF CERTIFICATIONS.—

(A) IN GENERAL.—The United States Secret Service may review a certification provided by an agency under paragraph (3), and shall review a certification provided by a business entity under paragraph (3), to determine whether an exemption under paragraph (1) is merited. Such review shall be completed not later than 10 business days after the date of receipt of the certification, except as provided in paragraph (5)(C).

(B) NOTICE.—Upon completing a review under subparagraph (A) the United States Secret Service shall immediately notify the agency or business entity, in writing, of its determination of whether an exemption under paragraph (1) is merited.

(C) EXEMPTION.—The exemption under paragraph (1) shall not apply if the United States Secret Service determines under this paragraph that the exemption is not merited.

(5) ADDITIONAL AUTHORITY OF THE SECRET SERVICE.—

(A) IN GENERAL.—In determining under paragraph (4) whether an exemption under paragraph (1) is merited, the United States Secret Service may request additional information from the agency or business entity regarding the basis for the claimed exemption, if such additional information is necessary to determine whether the exemption is merited.

(B) REQUIRED COMPLIANCE.—Any agency or business entity that receives a request for additional information under subparagraph (A) shall cooperate with any such request.

(C) TIMING.—If the United States Secret Service requests additional information under subparagraph (A), the United States Secret Service shall notify the agency or business entity not later than 10 business days after the date of receipt of the additional information whether an exemption under paragraph (1) is merited.

(b) SAFE HARBOR.—

(1) IN GENERAL.—An agency or business entity shall be exempt from the notice requirements under section 2, if—

(A) a risk assessment concludes that there is no significant risk that a security breach has resulted in, or will result in, harm to the individual whose sensitive personally identifiable information was subject to the security breach;

(B) without unreasonable delay, but not later than 45 days after the discovery of a security breach (unless extended by the United States Secret Service), the agency or business entity notifies the United States Secret Service, in writing, of—

(i) the results of the risk assessment; and

(ii) its decision to invoke the risk assessment exemption; and

(C) the United States Secret Service does not indicate, in writing, and not later than 10 business days after the date of receipt of the decision described in subparagraph (B)(ii), that notice should be given.

(2) PRESUMPTIONS.—There shall be a presumption that no significant risk of harm to the individual whose sensitive personally identifiable information was subject to a security breach if such information—

(A) was encrypted; or

(B) was rendered indecipherable through the use of best practices or methods, such as redaction, access controls, or other such mechanisms, that are widely accepted as an effective industry practice, or an effective industry standard.

(c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

(1) IN GENERAL.—A business entity will be exempt from the notice requirement under section 2 if the business entity utilizes or participates in a security program that—

(A) is designed to block the use of the sensitive personally identifiable information to initiate unauthorized financial transactions before they are charged to the account of the individual; and

(B) provides for notice to affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

(2) LIMITATION.—The exemption by this subsection does not apply if—

(A) the information subject to the security breach includes sensitive personally identifiable

information, other than a credit card number or credit card security code, of any type; or

(B) the information subject to the security breach includes both the individual's credit card number and the individual's first and last name.

SEC. 4. METHODS OF NOTICE.

An agency, or business entity shall be in compliance with section 2 if it provides both:

(1) INDIVIDUAL NOTICE.—

(A) Written notification to the last known home mailing address of the individual in the records of the agency or business entity;

(B) telephone notice to the individual personally; or

(C) e-mail notice, if the individual has consented to receive such notice and the notice is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).

(2) MEDIA NOTICE.—Notice to major media outlets serving a State or jurisdiction, if the number of residents of such State whose sensitive personally identifiable information was, or is reasonably be-

lieved to have been, acquired by an unauthorized person exceeds 5,000.

SEC. 5. CONTENT OF NOTIFICATION.

(a) IN GENERAL.—Regardless of the method by which notice is provided to individuals under section 4, such notice shall include, to the extent possible—

(1) a description of the categories of sensitive personally identifiable information that was, or is reasonably believed to have been, acquired by an unauthorized person;

(2) a toll-free number—

(A) that the individual may use to contact the agency or business entity, or the agent of the agency or business entity; and

(B) from which the individual may learn what types of sensitive personally identifiable information the agency or business entity maintained about that individual; and

(3) the toll-free contact telephone numbers and addresses for the major credit reporting agencies.

(b) ADDITIONAL CONTENT.—Notwithstanding section 10, a State may require that a notice under subsection (a) shall also include information regarding victim protection assistance provided for by that State.

SEC. 6. COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.

If an agency or business entity is required to provide notification to more than 5,000 individuals under section 2(a), the agency or business entity shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis (as defined in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)) of the timing and distribution of the notices. Such notice shall be given to the consumer credit reporting agencies without unreasonable delay and, if it will not delay notice to the affected individuals, prior to the distribution of notices to the affected individuals.

SEC. 7. NOTICE TO LAW ENFORCEMENT.

(a) SECRET SERVICE.—Any business entity or agency shall notify the United States Secret Service of the fact that a security breach has occurred if—

(1) the number of individuals whose sensitive personally identifying information was, or is reasonably believed to have been acquired by an unauthorized person exceeds 10,000;

(2) the security breach involves a database, networked or integrated databases, or other data system containing the sensitive personally identifiable information of more than 1,000,000 individuals nationwide;

(3) the security breach involves databases owned by the Federal Government; or

(4) the security breach involves primarily sensitive personally identifiable information of individuals known to the agency or business entity to be employees and contractors of the Federal Government involved in national security or law enforcement.

(b) NOTICE TO OTHER LAW ENFORCEMENT AGENCIES.—The United States Secret Service shall be responsible for notifying—

(1) the Federal Bureau of Investigation, if the security breach involves espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service under section 3056(a) of title 18, United States Code;

(2) the United States Postal Inspection Service, if the security breach involves mail fraud; and

(3) the attorney general of each State affected by the security breach.

(c) TIMING OF NOTICES.—The notices required under this section shall be delivered as follows:

(1) Notice under subsection (a) shall be delivered as promptly as possible, but not later than 14 days after discovery of the events requiring notice.

(2) Notice under subsection (b) shall be delivered not later than 14 days after the United States Secret Service receives notice of a security breach from an agency or business entity.

SEC. 8. ENFORCEMENT.

(a) CIVIL ACTIONS BY THE ATTORNEY GENERAL.—The Attorney General may bring a civil action in the appropriate United States district court against any business entity that engages in conduct constituting a violation of this Act and, upon proof of such conduct by a preponderance of the evidence, such business entity shall be subject to a civil penalty of not more than $1,000 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $1,000,000 per violation, unless such conduct is found to be willful or intentional.

(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—If it appears that a business entity has engaged, or is engaged, in any act or practice constituting a violation of this Act, the Attorney General may petition an appropriate district court of the United States for an order—

(A) enjoining such act or practice; or

(B) enforcing compliance with this Act.

(2) ISSUANCE OF ORDER.—A court may issue an order under paragraph (1), if the court finds that the conduct in question constitutes a violation of this Act.

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

(d) FRAUD ALERT.—Section 605A(b)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681c–1(b)(1)) is amended by inserting ", or evidence that the consumer has received notice that the consumer's financial information has or may have been compromised," after "identity theft report".

SEC. 9. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) IN GENERAL.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State or any State or local law

enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, 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 a business entity in a practice that is prohibited under this Act, the State or the State or local law enforcement agency on behalf of the residents of the agency's jurisdiction, may bring a civil action on behalf of the residents of the State or jurisdiction in a district court of the United States of appropriate jurisdiction or any other court of competent jurisdiction, including a State court, to—

(A) enjoin that practice;

(B) enforce compliance with this Act; or

(C) obtain civil penalties of not more than $1,000 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $1,000,000 per violation, unless such conduct is found to be willful or intentional.

(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 of the United States—

(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 Act, 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 at the time the State attorney general files the action.

(b) FEDERAL PROCEEDINGS.—Upon receiving notice under subsection (a)(2), the Attorney General shall have the right to—

(1) move to stay the action, pending the final disposition of a pending Federal proceeding or action;

(2) initiate an action in the appropriate United States district court under section 8 and move to consolidate all pending actions, including State actions, in such court;

(3) intervene in an action brought under subsection (a)(2); and

(4) file petitions for appeal.

(c) PENDING PROCEEDINGS.—If the Attorney General has instituted a proceeding or action for a violation of this Act or any regulations thereunder, no attorney general of a State may, during the pendency of such proceeding or action, bring an action under this Act against any defendant named in such criminal proceeding or civil action for any violation that is alleged in that proceeding or action.

(d) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this Act regarding notification 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.

(e) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in—

(A) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(B) another court of competent jurisdiction.

(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.

(f) NO PRIVATE CAUSE OF ACTION.—Nothing in this Act establishes a private cause of action against a business entity for violation of any provision of this Act.

SEC. 10. EFFECT ON FEDERAL AND STATE LAW.

The provisions of this Act shall supersede any other provision of Federal law or any provision of law of any State relating to notification by a business entity engaged

in interstate commerce or an agency of a security breach, except as provided in section 5(b).

SEC. 11. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated such sums as may be necessary to cover the costs incurred by the United States Secret Service to carry out investigations and risk assessments of security breaches as required under this Act.

SEC. 12. REPORTING ON RISK ASSESSMENT EXEMPTIONS.

(a) IN GENERAL.—The United States Secret Service shall report to Congress not later than 18 months after the date of enactment of this Act, and upon the request by Congress thereafter, on—

(1) the number and nature of the security breaches described in the notices filed by those business entities invoking the risk assessment exemption under section 3(b) of this Act and the response of the United States Secret Service to such notices; and

(2) the number and nature of security breaches subject to the national security and law enforcement exemptions under section 3(a) of this Act.

(b) REPORT.—Any report submitted under subsection (a) shall not disclose the contents of any risk as-

sessment provided to the United States Secret Service under this Act.

SEC. 13. DEFINITIONS.

In this Act, the following definitions shall apply:

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

(2) AFFILIATE.—The term ''affiliate'' means persons related by common ownership or by corporate control.

(3) BUSINESS ENTITY.—The term ''business entity'' means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, venture established to make a profit, or nonprofit, and any contractor, subcontractor, affiliate, or licensee thereof engaged in interstate commerce.

(4) ENCRYPTED.—The term ''encrypted''—

(A) means the protection of data in electronic form, in storage or in transit, using an encryption technology that has been adopted by an established standards setting body which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and

(B) includes appropriate management and safeguards of such cryptographic keys so as to protect the integrity of the encryption.

(5) PERSONALLY IDENTIFIABLE INFORMATION.—The term ''personally identifiable information'' means any information, or compilation of information, in electronic or digital form serving as a means of identification, as defined by section 1028(d)(7) of title 18, United State Code.

(6) SECURITY BREACH.—

(A) IN GENERAL.—The term ''security breach'' means compromise of the security, confidentiality, or integrity of computerized data through misrepresentation or actions that result in, or there is a reasonable basis to conclude has resulted in, acquisition of or access to sensitive personally identifiable information that is unauthorized or in excess of authorization.

(B) EXCLUSION.—The term ''security breach'' does not include—

(i) a good faith acquisition of sensitive personally identifiable information by a business entity or agency, or an employee or agent of a business entity or agency, if the sensitive personally identifiable infor-

mation is not subject to further unauthorized disclosure; or

(ii) the release of a public record not otherwise subject to confidentiality or nondisclosure requirements.

(7) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term ''sensitive personally identifiable information'' means any information or compilation of information, in electronic or digital form that includes—

(A) an individual's first and last name or first initial and last name in combination with any 1 of the following data elements:

(i) A non-truncated social security number, driver's license number, passport number, or alien registration number.

(ii) Any 2 of the following:

(I) Home address or telephone number.

(II) Mother's maiden name, if identified as such.

(III) Month, day, and year of birth.

(iii) Unique biometric data such as a finger print, voice print, a retina or iris

image, or any other unique physical representation.

(iv) A unique account identifier, electronic identification number, user name, or routing code in combination with any associated security code, access code, or password that is required for an individual to obtain money, goods, services or any other thing of value; or

(B) a financial account number or credit or debit card number in combination with any security code, access code or password that is required for an individual to obtain credit, withdraw funds, or engage in a financial transaction.

SEC. 14. EFFECTIVE DATE.

This Act shall take effect on the expiration of the date which is 90 days after the date of enactment of this Act.

○