109TH CONGRESS
2D SESSION

S. _____

To protect information relating to consumers, to require notice of security breaches, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. BENNETT (for himself and Mr. CARPER) introduced the following bill; which was read twice and referred to the Committee on

---

A BILL

To protect information relating to consumers, to require notice of security breaches, 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 ''Data Security Act of 2006''.

SEC. 2. DEFINITIONS.

For purposes of this Act, the following definitions shall apply:

(1) AFFILIATE.—The term ''affiliate'' means any company that controls, is controlled by, or is under common control with another company.

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

(3) BREACH OF DATA SECURITY.—

(A) IN GENERAL.—The term ''breach of data security'' means the unauthorized acquisition of sensitive account information or sensitive personal information.

(B) EXCEPTION FOR DATA THAT IS NOT IN USABLE FORM.—

(i) IN GENERAL.—The term ''breach of data security'' does not include the unauthorized acquisition of sensitive account information or sensitive personal information that is maintained or communicated in a manner that is not usable—

(I) to commit identity theft; or

(II) to make fraudulent transactions on financial accounts.

(ii) RULE OF CONSTRUCTION.—For purposes of this subparagraph, information that is maintained or communicated in a

manner that is not usable includes any information that is maintained or communicated in an encrypted, redacted, altered, edited, or coded form.

(4) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(5) CONSUMER.—The term ''consumer'' means an individual.

(6) CONSUMER REPORTING AGENCY THAT COMPILES AND MAINTAINS FILES ON CONSUMERS ON A NATIONWIDE BASIS.—The term ''consumer reporting agency that compiles and maintains files on consumers on a nationwide basis'' has the same meaning as in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

(7) COVERED ENTITY.—

(A) IN GENERAL.—The term ''covered entity'' means any—

(i) entity, the business of which is engaging in financial activities, as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k));

(ii) financial institution, including any institution described in section 313.3(k) of

title 16, Code of Federal Regulations, as in effect on the date of enactment of this Act;

(iii) entity that maintains or otherwise possesses information that is subject to section 628 of the Fair Credit Reporting Act (15 U.S.C. 1681w); or

(iv) other individual, partnership, corporation, trust, estate, cooperative, association, or entity that maintains or communicates sensitive account information or sensitive personal information.

(B) EXCEPTION.—The term ''covered entity'' does not include any agency or any other unit of Federal, State, or local government or any subdivision of such unit.

(8) FINANCIAL INSTITUTION.—The term ''financial institution'' has the same meaning as in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809).

(9) SENSITIVE ACCOUNT INFORMATION.—The term ''sensitive account information'' means a financial account number relating to a consumer, including a credit card number or debit card number, in combination with any security code, access code,

password, or other personal identification information required to access the financial account.

(10) SENSITIVE PERSONAL INFORMATION.—

(A) IN GENERAL.—The term ''sensitive personal information'' means the first and last name, address, or telephone number of a consumer, in combination with any of the following relating to such consumer:

(i) Social security account number.

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

(iii) Taxpayer identification number.

(B) EXCEPTION.—The term ''sensitive personal information'' does not include publicly available information that is lawfully made available to the general public from—

(i) Federal, State, or local government records; or

(ii) widely distributed media.

(11) SUBSTANTIAL HARM OR INCONVENIENCE.—

(A) IN GENERAL.—The term ''substantial harm or inconvenience'' means—

(i) material financial loss to, or civil or criminal penalties imposed on, a con-

sumer, due to the unauthorized use of sensitive account information or sensitive personal information relating to such consumer; or

(ii) the need for a consumer to expend significant time and effort to correct erroneous information relating to the consumer, including information maintained by a consumer reporting agency, financial institution, or government entity, in order to avoid material financial loss, increased costs, or civil or criminal penalties, due to the unauthorized use of sensitive account information or sensitive personal information relating to such consumer.

(B) EXCEPTION.—The term ''substantial harm or inconvenience'' does not include—

(i) changing a financial account number or closing a financial account; or

(ii) harm or inconvenience that does not result from identity theft or account fraud.

SEC. 3. PROTECTION OF INFORMATION AND SECURITY BREACH NOTIFICATION.

(a) SECURITY PROCEDURES REQUIRED.—

(1) IN GENERAL.—Each covered entity shall implement, maintain, and enforce reasonable policies and procedures to protect the confidentiality and security of sensitive account information and sensitive personal information which is maintained or is being communicated by or on behalf of a covered entity, from the unauthorized use of such information that is reasonably likely to result in substantial harm or inconvenience to the consumer to whom such information relates.

(2) LIMITATION.—Any policy or procedure implemented or maintained under paragraph (1) shall be appropriate to the—

(A) size and complexity of a covered entity;

(B) nature and scope of the activities of such entity; and

(C) sensitivity of the consumer information to be protected.

(b) INVESTIGATION REQUIRED.—

(1) IN GENERAL.—If a covered entity determines that a breach of data security has or may have occurred in relation to sensitive account information or sensitive personal information that is maintained or is being communicated by, or on be-

half of, such covered entity, the covered entity shall conduct an investigation—

(A) to assess the nature and scope of the breach;

(B) to identify any sensitive account information or sensitive personal information that may have been involved in the breach; and

(C) to determine if such information is reasonably likely to be misused in a manner causing substantial harm or inconvenience to the consumers to whom the information relates.

(2) NEURAL NETWORKS AND INFORMATION SECURITY PROGRAMS.—In determining the likelihood of misuse of sensitive account information under paragraph (1)(C), a covered entity shall consider whether any neural network or security program has detected, or is likely to detect or prevent, fraudulent transactions resulting from the breach of security.

(c) NOTICE REQUIRED.—If a covered entity determines under subsection (b)(1)(C) that sensitive account information or sensitive personal information involved in a breach of data security is reasonably likely to be misused in a manner causing substantial harm or inconvenience to the consumers to whom the information relates, such

covered entity, or a third party acting on behalf of such covered entity, shall—

(1) notify, in the following order—

(A) the appropriate agency or authority identified in section 5;

(B) an appropriate law enforcement agency;

(C) any entity that owns, or is obligated on, a financial account to which the sensitive account information relates, if the breach involves a breach of sensitive account information;

(D) each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, if the breach involves sensitive personal information relating to 5,000 or more consumers; and

(E) all consumers to whom the sensitive account information or sensitive personal information relates; and

(2) take reasonable measures to restore the security and confidentiality of the sensitive account information or sensitive personal information involved in the breach.

(d) COMPLIANCE.—

(1) IN GENERAL.—A financial institution shall be deemed to be in compliance with—

(A) subsection (a), and any regulations prescribed under such subsection, if such institution maintains policies and procedures to protect the confidentiality and security of sensitive account information and sensitive personal information that are consistent with the policies and procedures of such institution that are designed to comply with the requirements of section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) and any regulations or guidance prescribed under that section that are applicable to such institution; and

(B) subsections (b) and (c), and any regulations prescribed under such subsections, if such institution—

(i)(I) maintains policies and procedures to investigate and provide notice to consumers of breaches of data security that are consistent with the policies and procedures of such institution that are designed to comply with the investigation and notice requirements established by regulations or guidance under section 501(b) of

the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) that are applicable to such institution; or

(II) is an affiliate of a bank holding company that maintains policies and procedures to investigate and provide notice to consumers of breaches of data security that are consistent with the policies and procedures of a bank that is an affiliate of such institution, and that bank's policies and procedures are designed to comply with the investigation and notice requirements established by any regulations or guidance under section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) that are applicable to that bank; and

(ii) provides for notice to the entities described under subparagraphs (B), (C), and (D) of subsection (c)(1), if notice is provided to consumers pursuant to the policies and procedures of such institution described in clause (i).

(2) DEFINITIONS.—For purposes of this subsection, the terms ''bank holding company'' and

''bank'' shall have the same meaning given such terms under section 2 of the Bank Holding Company Act of 1956 (12 U.S.C. 1841).

SEC. 4. IMPLEMENTING REGULATIONS.

(a) IN GENERAL.—Except as provided under section 6, the agencies and authorities identified in section 5, with respect to the covered entities that are subject to the respective enforcement authority of such agencies and authorities, shall prescribe regulations to implement this Act.

(b) COORDINATION.—Each agency and authority required to prescribe regulations under subsection (a) shall consult and coordinate with each other agency and authority identified in section 5 so that, to the extent possible, the regulations prescribed by each agency and authority are consistent and comparable.

(c) METHOD OF PROVIDING NOTICE TO CONSUMERS.—The regulations required under subsection (a) shall—

(1) prescribe the methods by which a covered entity shall notify a consumer of a breach of data security under section 3; and

(2) allow a covered entity to provide such notice by—

(A) written, telephonic, or e-mail notification; or

(B) substitute notification, if providing written, telephonic, or e-mail notification is not feasible due to—

(i) lack of sufficient contact information for the consumers that must be notified; or

(ii) excessive cost to the covered entity.

(d) CONTENT OF CONSUMER NOTICE.—The regulations required under subsection (a) shall—

(1) prescribe the content that shall be included in a notice of a breach of data security that is required to be provided to consumers under section 3; and

(2) require such notice to include—

(A) a description of the type of sensitive account information or sensitive personal information involved in the breach of data security;

(B) a general description of the actions taken by the covered entity to restore the security and confidentiality of the sensitive account information or sensitive personal information involved in the breach of data security; and

(C) the summary of rights of victims of identity theft prepared by the Commission

under section 609(d) of the Fair Credit Reporting Act (15 U.S.C. 1681g), if the breach of data security involves sensitive personal information.

(e) TIMING OF NOTICE.—The regulations required under subsection (a) shall establish standards for when a covered entity shall provide any notice required under section 3.

(f) LAW ENFORCEMENT DELAY.—The regulations required under subsection (a) shall allow a covered entity to delay providing notice of a breach of data security to consumers under section 3 if a law enforcement agency requests such a delay in writing.

(g) SERVICE PROVIDERS.—The regulations required under subsection (a) shall—

(1) require any party that maintains or communicates sensitive account information or sensitive personal information on behalf of a covered entity to provide notice to that covered entity if such party determines that a breach of data security has, or may have, occurred with respect to such information; and

(2) ensure that there is only 1 notification responsibility with respect to a breach of data security.

(h) TIMING OF REGULATIONS.—The regulations required under subsection (a) shall—

(1) be issued in final form not later than 6 months after the date of enactment of this Act; and

(2) take effect not later than 6 months after the date on which they are issued in final form.

SEC. 5. ADMINISTRATIVE ENFORCEMENT.

(a) IN GENERAL.—Section 3, and the regulations required under section 4, shall be enforced exclusively under—

(1) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), in the case of—

(A) a national bank, a Federal branch or Federal agency of a foreign bank, or any subsidiary thereof (other than a broker, dealer, person providing insurance, investment company, or investment adviser), by the Office of the Comptroller of the Currency;

(B) a member bank of the Federal Reserve System (other than a national bank), a branch or agency of a foreign bank (other than a Federal branch, Federal agency, or insured State branch of a foreign bank), a commercial lending company owned or controlled by a foreign bank, an organization operating under section 25 or

25A of the Federal Reserve Act (12 U.S.C. 601,604), or a bank holding company and its nonbank subsidiary or affiliate (other than a broker, dealer, person providing insurance, investment company, or investment adviser), by the Board of Governors of the Federal Reserve System;

(C) a bank, the deposits of which are insured by the Federal Deposit Insurance Corporation (other than a member of the Federal Reserve System), an insured State branch of a foreign bank, or any subsidiary thereof (other than a broker, dealer, person providing insurance, investment company, or investment adviser), by the Board of Directors of the Federal Deposit Insurance Corporation; and

(D) a savings association, the deposits of which are insured by the Federal Deposit Insurance Corporation, or any subsidiary thereof (other than a broker, dealer, person providing insurance, investment company, or investment adviser), by the Director of the Office of Thrift Supervision;

(2) the Federal Credit Union Act (12 U.S.C. 1751 et seq.), by the National Credit Union Admin-

istration Board with respect to any federally insured credit union;

(3) the Securities Exchange Act of 1934 (15 U.S.C.78a et seq.), by the Securities and Exchange Commission with respect to any broker or dealer;

(4) the Investment Company Act of 1940 (15 U.S.C. 80a-1 et seq.), by the Securities and Exchange Commission with respect to any investment company;

(5) the Investment Advisers Act of 1940 (15 U.S.C. 80b-1 et seq.), by the Securities and Exchange Commission with respect to any investment adviser registered with the Securities and Exchange Commission under that Act;

(6) the Commodity Exchange Act (7 U.S.C. 1 et seq.), by the Commodity Futures Trading Commission with respect to any futures commission merchant, commodity trading advisor, commodity pool operator, or introducing broker;

(7) the provisions of title XIII of the Housing and Community Development Act of 1992 (12 U.S.C. 4501 et seq.), by the Director of Federal Housing Enterprise Oversight (and any successor to such functional regulatory agency) with respect to the Federal National Mortgage Association, the Fed-

eral Home Loan Mortgage Corporation, and any other entity or enterprise (as defined in that title) subject to the jurisdiction of such functional regulatory agency under that title, including any affiliate of any such enterprise;

(8) State insurance law, in the case of any person engaged in providing insurance, by the applicable State insurance authority of the State in which the person is domiciled; and

(9) the Federal Trade Commission Act (15 U.S.C. 41 et seq.), by the Commission for any other covered entity that is not subject to the jurisdiction of any agency or authority described under paragraphs (1) through (8).

(b) EXTENSION OF FEDERAL TRADE COMMISSION ENFORCEMENT AUTHORITY.—The authority of the Commission to enforce compliance with section 3, and the regulations required under section 4, under subsection (a)(8) shall—

(1) notwithstanding the Federal Aviation Act of 1958 (49 U.S.C. App. 1301 et seq.), include the authority to enforce compliance by air carriers and foreign air carriers; and

(2) notwithstanding the Packers and Stockyards Act (7 U.S.C. 181 et seq.), include the author-

ity to enforce compliance by persons, partnerships, and corporations subject to the provisions of that Act.

(c) NO PRIVATE RIGHT OF ACTION.—

(1) IN GENERAL.—This Act, and the regulations prescribed under this Act, may not be construed to provide a private right of action, including a class action with respect to any act or practice regulated under this Act.

(2) CIVIL AND CRIMINAL ACTIONS.—No civil or criminal action relating to any act or practice governed under this Act, or the regulations prescribed under this Act, shall be commenced or maintained in any State court or under State law, including a pendent State claim to an action under Federal law.

SEC. 6. PROTECTION OF INFORMATION AT FEDERAL AGENCIES.

(a) DATA SECURITY STANDARDS.—Each agency shall implement appropriate standards relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of the sensitive account information and sensitive personal information that is maintained or is being communicated by, or on behalf of, that agency;

(2) to protect against any anticipated threats or hazards to the security of such information; and

(3) to protect against misuse of such information, which could result in substantial harm or inconvenience to a consumer.

(b) SECURITY BREACH NOTIFICATION STANDARDS.—Each agency shall implement appropriate standards providing for notification of consumers when such agency determines that sensitive account information or sensitive personal information that is maintained or is being communicated by, or on behalf of, such agency—

(1) has been acquired without authorization; and

(2) is reasonably likely to be misused in a manner causing substantial harm or inconvenience to the consumers to whom the information relates.

SEC. 7. RELATION TO STATE LAW.

No requirement or prohibition may be imposed under the laws of any State with respect to the responsibilities of any person to—

(1) protect the security of information relating to consumers that is maintained or communicated by, or on behalf of, such person;

(2) safeguard information relating to consumers from potential misuse;

(3) investigate or provide notice of the unauthorized access to information relating to consumers, or the potential misuse of such information for fraudulent, illegal, or other purposes; or

(4) mitigate any loss or harm resulting from the unauthorized access or misuse of information relating to consumers.

SEC. 8. DELAYED EFFECTIVE DATE FOR CERTAIN PROVISIONS.

(a) COVERED ENTITIES.—Sections 3 and 7 shall take effect on the later of—

(1) 1 year after the date of enactment of this Act; or

(2) the effective date of the final regulations required under section 4.

(b) AGENCIES.—Section 6 shall take effect 1 year after the date of enactment of this Act.