I

115TH CONGRESS
1ST SESSION

H. R. 3806

To establish a national data breach notification standard, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 18, 2017

Mr. LANGEVIN (for himself and Mr. TED LIEU of California) introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committee on the Judiciary, 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 establish a national data breach notification standard, 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; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Personal Data Notification and Protection Act of 2017''.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

SEC. 2. NOTIFICATION TO INDIVIDUALS.

(a) IN GENERAL.—Except as provided for in section 3, any business entity engaged in or affecting interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information about more than 10,000 individuals during any 12-month period shall, following the discovery of a security breach of such information, notify, in accordance with sections 4 and 5, any individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed or acquired.

(b) OBLIGATIONS OF AND TO OWNER OR LICENSEE.—

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

rity breach involving such information, unless there is no reasonable risk of harm or fraud to such owner or licensee.

(2) NOTIFICATION BY OWNER, LICENSEE, OR OTHER DESIGNATED THIRD PARTY.—Nothing in this Act shall prevent or abrogate an agreement between a business entity required to provide notification 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 NOTIFICATION.—A business entity required to provide notification under subsection (a) shall not be required to provide such notification 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 business entity of a security breach. A business entity shall, upon the request of the Commission, provide records

or other evidence of the notifications required under this section.

(2) REASONABLE DELAY.—

(A) IN GENERAL.—Except as provided in subsection (d), reasonable delay under this subsection shall not exceed 30 days, unless the business entity seeking additional time requests an extension of time and the Commission determines that additional time is reasonably necessary to determine the scope of the security breach, prevent further disclosures, conduct the risk assessment, restore the reasonable integrity of the data system, or provide notice to the breach notification entity.

(B) EXTENSION.—If the Commission determines that additional time is reasonably necessary as described in subparagraph (A), the Commission may extend the time period for notification for additional periods of up to 30 days each. Any such extension shall be provided in writing by the Commission.

(3) BURDEN OF PRODUCTION.—If a business entity requires additional time under paragraph (2), the business entity shall provide the Commission

with records or other evidence of the reasons necessitating delay of notification.

(d) DELAY OF NOTIFICATION FOR LAW ENFORCEMENT OR NATIONAL SECURITY.—

(1) IN GENERAL.—If the Director of the United States Secret Service or the Director of the Federal Bureau of Investigation determines that the notification required under this section would impede a criminal investigation or national security activity, the time period for notification shall be extended 30 days upon written notice from such Director to the business entity that experienced the breach.

(2) EXTENDED DELAY OF NOTIFICATION.—If the time period for notification required under subsection (a) is extended pursuant to paragraph (1), a business entity shall provide the notification within such time period unless the Director of the United States Secret Service or the Director of the Federal Bureau of Investigation provides written notification that further extension of the time period is necessary. The Director of the United States Secret Service or the Director of the Federal Bureau of Investigation may extend the time period for additional periods of up to 30 days each.

(3) IMMUNITY.—No cause of action for which jurisdiction is based under section 1346(b) of title 28, United States Code, shall lie against any Federal law enforcement agency for acts relating to the extension of the deadline for notification for law enforcement or national security purposes under this section.

(e) DESIGNATION OF BREACH NOTIFICATION ENTITY.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security shall designate a Federal Government entity to receive notices, reports, and information about information security incidents, threats, and vulnerabilities under this Act.

SEC. 3. EXEMPTIONS FROM NOTIFICATION TO INDIVIDUALS.

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

(1) IN GENERAL.—Notwithstanding section 2, if the Director of the United States Secret Service or the Director of the Federal Bureau of Investigation determines that notification of the security breach required by such section could be expected to reveal sensitive sources and methods or similarly impede the ability of a Federal, State, or local law enforcement agency to conduct law enforcement inves-

tigations, or if the Director of the Federal Bureau of Investigation determines that notification of the security breach could be expected to cause damage to national security, such notification is not required.

(2) IMMUNITY.—No cause of action for which jurisdiction is based under section 1346(b) of title 28, United States Code, shall lie against any Federal law enforcement agency for acts relating to provision of an exemption from notification for law enforcement or national security purposes under this section.

(b) SAFE HARBOR.—

(1) IN GENERAL.—A business entity is exempt from the notification requirement under section 2, if the following requirements are met:

(A) RISK ASSESSMENT.—A risk assessment, in accordance with paragraph (3), is conducted by or on behalf of the business entity that concludes that there is no reasonable risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach.

(B) NOTICE TO COMMISSION.—Without unreasonable delay and not later than 30 days after the discovery of a security breach, unless extended by the Commission, the Director of the United States Secret Service, or the Director of the Federal Bureau of Investigation under section 2 (in which case, before the extended deadline), the business entity notifies the Commission, in writing, of—

(i) the results of the risk assessment; and

(ii) the decision by the business entity to invoke the risk assessment exemption described under subparagraph (A).

(C) DETERMINATION BY COMMISSION.—During the period beginning on the date on which the notification described in subparagraph (B) is submitted and ending 10 days after such date, the Commission has not issued a determination in writing that a notification should be provided under section 2.

(2) REBUTTABLE PRESUMPTION.—For purposes of paragraph (1)—

(A) the rendering of sensitive personally identifiable information at issue unusable,

unreadable, or indecipherable through a security technology generally accepted by experts in the field of information security shall establish a rebuttable presumption that such reasonable risk does not exist; and

(B) any such presumption shall be rebuttable by facts demonstrating that the security technologies or methodologies in a specific case have been, or are reasonably likely to have been, compromised.

(3) RISK ASSESSMENT REQUIREMENTS.—A risk assessment is in accordance with this paragraph if the following requirements are met:

(A) PROPERLY CONDUCTED.—The risk assessment is conducted in a reasonable manner or according to standards generally accepted by experts in the field of information security.

(B) LOGGING DATA REQUIRED.—The risk assessment includes logging data, as applicable and to the extent available, for a period of at least six months before the discovery of a security breach described in section 2(a)—

(i) for each communication or attempted communication with a database or data system containing sensitive personally

identifiable information, the data system communication information for the communication or attempted communication, including any Internet addresses, and the date and time associated with the communication or attempted communication; and

(ii) all log-in information associated with databases or data systems containing sensitive personally identifiable information, including both administrator and user log-in information.

(C) FRAUDULENT OR MISLEADING INFORMATION.—The risk assessment does not contain fraudulent or deliberately misleading information.

(c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

(1) IN GENERAL.—A business entity is exempt from the notification requirement under section 2 if the business entity uses or participates in a security program that—

(A) effectively blocks 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 notification to affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

(2) LIMITATION.—The exemption in paragraph (1) does not apply if the information subject to the security breach includes the individual's first and last name or any other type of sensitive personally identifiable information other than a credit card number or credit card security code.

SEC. 4. METHODS OF NOTIFICATION.

A business entity shall be in compliance with the requirements of this section if, with respect to the method of notification as required under section 2, the following requirements are met:

(1) INDIVIDUAL NOTIFICATION.—Notification to an individual is by one of the following means:

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

(B) Telephone notification to the individual personally.

(C) E-mail notification, if the individual has consented to receive such notification and the notification is consistent with the provisions permitting electronic transmission of notifica-

tions under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).

(2) MEDIA NOTIFICATION.—If the number of residents of a State whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person exceeds 5,000, notification is provided to media reasonably calculated to reach such individuals, such as major media outlets serving a State or jurisdiction.

SEC. 5. CONTENT OF NOTIFICATION.

The notification provided to individuals required by section 2 shall include, to the extent possible, the following:

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

(2) A toll-free number—

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

(B) from which the individual may learn what types of sensitive personally identifiable

information the business entity maintained about that individual.

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

(4) The name of the business entity that has a direct business relationship with the individual.

(5) Notwithstanding section 10, any information regarding victim protection assistance required by the State in which the individual resides.

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

(a) REQUIREMENT TO NOTIFY CREDIT REPORTING AGENCIES.—If a business entity is required to notify more than 5,000 individuals under section 2, the business entity shall also notify each consumer reporting agency that compiles and maintains 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 notifications. Such notification shall be given to the consumer credit reporting agencies without unreasonable delay and, if it will not delay notification to the affected individuals, prior to the distribution of notifications to the affected individuals.

(b) REASONABLE DELAY.—Reasonable delay under subsection (a) shall not exceed 30 days following the discovery of a security breach, except as provided in subsection (c) or (d) of section 2 (in which case, before the extended deadline), or unless the business entity providing notification can demonstrate to the Commission that additional time is reasonably necessary to determine the scope of the security breach, prevent further disclosures, conduct the risk assessment, restore the reasonable integrity of the data system, and provide notice to the breach notification entity. If the Commission determines that additional time is necessary, the Commission may extend the time period for notification for additional periods of up to 30 days each. Any such extension shall be provided in writing.

SEC. 7. NOTIFICATION FOR LAW ENFORCEMENT AND OTHER PURPOSES.

(a) NOTIFICATION TO LAW ENFORCEMENT AND NATIONAL SECURITY AUTHORITIES.—Any business entity shall notify the breach notification entity, and the breach notification entity shall promptly notify and provide that information to the United States Secret Service, the Federal Bureau of Investigation, and the Commission for civil law enforcement purposes, and shall make it available as appropriate to other Federal agencies for law enforcement, national security, or computer security purposes, if—

(1) the number of individuals whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person exceeds 5,000;

(2) the security breach involves a database, networked or integrated databases, or other data system containing the sensitive personally identifiable information of more than 500,000 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 business entity to be employees and contractors of the Federal Government involved in national security or law enforcement.

(b) REGULATIONS.—Not later than one year after the date of enactment of this Act, the Commission shall promulgate regulations (in accordance with section 553 of title 5, United States Code), in consultation with the Attorney General and the Secretary of Homeland Security, that describe what information is required to be included in the notification under subsection (a). In addition, the Commission shall, as necessary, promulgate regulations (in accordance with section 553 of title 5, United States

Code), in consultation with the Attorney General, to adjust the thresholds for notification to law enforcement and national security authorities under subsection (a) and to facilitate the purposes of this section.

(c) TIMING OF NOTIFICATION.—The notification required under this section shall be provided as promptly as possible and at least 72 hours before notification of an individual pursuant to section 2 or 10 days after discovery of the breach requiring notification, whichever comes first.

SEC. 8. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act or a regulation promulgated under this Act shall be treated as a violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(b) POWERS OF COMMISSION.—The Federal Trade Commission shall enforce this Act and the regulations promulgated under this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act, except that the exceptions described in section 5(a)(2) of such Act (15

U.S.C. 45(a)(2)) shall not apply. Any business entity who violates this Act or a regulation promulgated under this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

(c) FEDERAL COMMUNICATIONS COMMISSION.—In a case in which enforcement under this Act involves a business entity that is subject to the authority of the Federal Communications Commission, in enforcement actions by the Commission, the Commission shall consult with the Federal Communications Commission.

(d) CONSUMER FINANCIAL PROTECTION BUREAU.—In a case in which enforcement under this Act relates to financial information or information associated with the provision of a consumer financial product or service, in enforcement actions by the Commission, the Commission shall consult with the Consumer Financial Protection Bureau.

(e) CONSULTATION WITH THE ATTORNEY GENERAL REQUIRED.—The Commission shall consult with the Attorney General before opening an investigation. If the Attorney General determines that such an investigation would impede an ongoing criminal investigation or national security activity, the Commission may not open such investigation.

(f) REGULATIONS.—

(1) IN GENERAL.—The Commission may promulgate regulations, in addition to the regulations promulgated pursuant to section 7(b), relating to the duties of the Commission under this Act, in accordance with section 553 of title 5, United States Code, as the Commission determines to be necessary to carry out this Act.

(2) FEDERAL COMMUNICATIONS COMMISSION.—With regard to a regulation promulgated under this section that relates to an entity subject to the authority of the Federal Communications Commission, the Commission may only promulgate such regulation after consultation with the Federal Communications Commission.

(3) CONSUMER FINANCIAL PROTECTION BUREAU.—With regard to a regulation promulgated under this section that relates to financial information or information associated with the provision of a consumer financial product or service, the Commission may only promulgate such regulation after consultation with the Consumer Financial Protection Bureau.

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 an official or agency 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 in violation of this Act or a regulation promulgated under this Act, the State, as parens patriae, may bring a civil action on behalf of the residents of the State in an appropriate State court or an appropriate district court of the United States to—

(A) enjoin that practice;

(B) enforce compliance with this Act; or

(C) impose 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.—Before filing an action under paragraph (1), the attorney general, official, or agency of the State involved shall provide to the Attorney General and the Commission—

(A) a written notice of the action; and

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

(3) ATTORNEY GENERAL CERTIFICATION.—An action may not be filed under paragraph (1) if the Attorney General determines that the filing would impede a criminal investigation or national security activity.

(b) AUTHORITY OF FEDERAL TRADE COMMISSION.—Upon receiving notice under subsection (a)(2), the Commission may—

(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 the action brought under subsection (a); or

(4) file petitions for appeal.

(c) PENDING PROCEEDINGS.—If the Commission has instituted a proceeding or action for a violation of this Act or any regulations promulgated under this Act, a State attorney general, official, or agency may not bring an action under this Act during the pendency of the Federal proceeding or action against any defendant named in such

proceeding or action for any violation that is alleged in such proceeding or action.

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

SEC. 10. EFFECT ON STATE LAW.

The provisions of this Act shall supersede any provision of the law of any State, or a political subdivision thereof, relating to notification by a business entity engaged in interstate commerce of a security breach, except as provided in section 5(5).

SEC. 11. REPORTING ON SECURITY BREACHES.

(a) REPORT REQUIRED ON NATIONAL SECURITY AND LAW ENFORCEMENT EXEMPTIONS.—Not later than 18 months after the date of enactment of this Act, and annually thereafter, the Director of the United States Secret Service and the Director of the Federal Bureau of Investigation shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate on a report on the number and nature of security breaches subject to the national security and law enforcement exemptions under section 3(a).

(b) REPORT REQUIRED ON SAFE HARBOR EXEMPTIONS.—Not later than 18 months after the date of enactment of this Act, and annually thereafter, the Commission shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a

report on the number and nature of the security breaches described in the notices filed by business entities invoking the risk assessment exemption under section 3(b) and the response of the Commission to such notices.

SEC. 12. EXCLUDED BUSINESS ENTITIES.

Nothing in this Act, or the regulations promulgated under this Act, shall apply to—

(1) business entities to the extent that such entities act as covered entities or business associates (as such terms are defined in section 13400 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17921)) subject to section 13402 of such Act (42 U.S.C. 17932); and

(2) business entities to the extent that they act as vendors of personal health records (as such term is defined in section 13400 of such Act (42 U.S.C. 17921)) and third-party service providers subject to section 13407 of such Act (42 U.S.C. 17937).

SEC. 13. DEFINITIONS.

In this Act:

(1) BREACH NOTIFICATION ENTITY.—The term ''breach notification entity'' means the Federal Government entity designated pursuant to section 2(e).

(2) BUSINESS ENTITY.—The term ''business entity'' means any organization, corporation, trust,

partnership, sole proprietorship, unincorporated association, or venture, whether or not established to make a profit.

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

(4) CONSUMER FINANCIAL PRODUCT OR SERVICE.—The term ''consumer financial product or service'' has the meaning given that term in section 1002 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (12 U.S.C. 5481).

(5) DATA SYSTEM COMMUNICATION INFORMATION.—The term ''data system communication information'' means dialing, routing, addressing, or signaling information that identifies the origin, direction, destination, processing, transmission, or termination of each communication initiated, attempted, or received.

(6) DATE AND TIME.—The term ''date and time'' includes the date, time, and specification of the time zone offset from Coordinated Universal Time.

(7) FEDERAL AGENCY.—The term ''Federal agency'' has the meaning given the term ''agency'' in section 3502 of title 44, United States Code.

(8) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(9) INTERNET ADDRESS.—The term ''Internet address'' means an Internet Protocol address as specified by the Internet Protocol version 4 or 6 protocol, or any successor protocol or any unique number for a specific host on the Internet.

(10) SECURITY BREACH.—

(A) IN GENERAL.—The term ''security breach'' means a compromise of the security, confidentiality, or integrity of, or the loss of, computerized data that results in, or there is a reasonable basis to conclude has resulted in—

(i) the unauthorized acquisition of sensitive personally identifiable information; or

(ii) access to sensitive personally identifiable information that is for an unauthorized purpose, or in excess of authorization.

(B) EXCLUSION.—The term ''security breach'' does not include any lawfully authorized investigative, protective, or intelligence ac-

tivity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an element of the intelligence community.

(11) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term ''sensitive personally identifiable information'' means any information or compilation of information, in electronic or digital form that includes one or more of the following:

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

(i) Home address or telephone number.

(ii) Mother's maiden name.

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

(B) A Social Security number (but not including only the last four digits of a Social Security number), driver's license number, passport number, or alien registration number or other Government-issued unique identification number.

(C) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation.

(D) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.

(E) A user name or electronic mail address, in combination with a password or security question and answer that would permit access to an online account.

(F) Any combination of the following data elements:

(i) An individual's first and last name or first initial and last name.

(ii) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.

(iii) Any security code, access code, or password, or source code that could be used to generate such codes or passwords.

(12) MODIFIED DEFINITION BY RULEMAKING.—The Commission may, by rule promulgated under section 553 of title 5, United States Code, amend the definition of ''sensitive personally identifiable information'' to the extent that such

amendment will accomplish the purposes of this Act. In amending the definition, the Commission may determine—

(A) that any particular combinations of information are sensitive personally identifiable information; or

(B) that any particular piece of information, on its own, is sensitive personally identifiable information.

SEC. 14. EFFECTIVE DATE.

This Act shall take effect 90 days after the date of enactment of this Act.

○