I

115TH CONGRESS
1ST SESSION

H. R. 3975

To require covered entities to provide notification in the case of a breach of unsecured sensitive personally identifiable information in electronic or digital form, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 5, 2017

Mr. CORREA (for himself, Ms. NORTON, Ms. HANABUSA, and Mr. BRENDAN F. BOYLE of Pennsylvania) introduced the following bill; which was referred to the Committee on Energy and Commerce

---

A BILL

To require covered entities to provide notification in the case of a breach of unsecured sensitive personally identifiable information in electronic or digital form, 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 ''Cyber Breach Notification Act of 2017''.

SEC. 2. NOTIFICATION OF INFORMATION SECURITY BREACH.

(a) NOTIFICATION REQUIRED.—

(1) BY COVERED ENTITY.—A covered entity that collects, uses, accesses, transmits, stores, or disposes of unsecured sensitive personally identifiable information in electronic or digital form shall, in the case of a breach of such information that is discovered by the covered entity, notify—

(A) appropriate Federal agencies;

(B) each individual whose unsecured sensitive personally identifiable information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach;

(C) the attorney general of each State in which an individual described in subparagraph (B) resides; and

(D) if there are 500 or more individuals described in subparagraph (B) who reside in a State or other jurisdiction, prominent media outlets serving such State or other jurisdiction.

(2) BY THIRD PARTY.—

(A) TO COVERED ENTITY.—A third party that collects, uses, accesses, transmits, stores, or disposes of unsecured sensitive personally identifiable information in electronic or digital form that is owned or licensed by a covered en-

tity shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notification shall include the identification of each individual whose unsecured sensitive personally identifiable information has been, or is reasonably believed by the third party to have been, accessed, acquired, or disclosed during such breach and the information described in paragraphs (1), (2), and (4) of subsection (d) with respect to such breach. The covered entity shall make the notifications required by paragraph (1) with respect to such breach.

(B) TO FTC AND FBI.—If there are 500 or more individuals described in subparagraph (A) with respect to a breach, the third party shall provide the notification required by such subparagraph to the Commission and the Federal Bureau of Investigation, as well as to the covered entity. Notification by the third party under this subparagraph does not relieve the covered entity of the requirement to notify the Commission and the Federal Bureau of Investigation under paragraph (1)(A).

(b) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—All notifications required under subsection (a) shall be made in the most expedient time possible and without unreasonable delay, but in no case later than 30 calendar days after the discovery of a breach by the covered entity involved (or by the third party involved in the case of a notification required under subsection (a)(2)(A)).

(2) EXPEDITED NOTIFICATION TO FTC AND FBI.—Notwithstanding paragraph (1), if there are 500 or more individuals to which a covered entity is required to provide notification of a breach under subsection (a)(1)(B), the covered entity shall notify the Commission and the Federal Bureau of Investigation of such breach as required under subsection (a)(1)(A) not later than 48 hours after the discovery of such breach by the covered entity.

(3) EXPEDITED NOTIFICATION BY THIRD PARTIES.—Notwithstanding paragraph (1), a third party subject to subsection (a)(2)(B) with respect to a breach shall make the notifications required by such subsection not later than 48 hours after discovery of the breach by the third party.

(4) BURDEN OF PROOF.—The covered entity involved (or the third party involved in the case of a notification required under subsection (a)(2)) shall

have the burden of demonstrating that all notifications were made as required under subsection (a), including evidence demonstrating the necessity of any delay.

(5) BREACHES TREATED AS DISCOVERED.—For purposes of this section, a breach shall be treated as discovered by a covered entity or, in the case of a breach described in subsection (a)(2), by a third party, as of the first day on which such breach is known to such covered entity or third party, respectively (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such covered entity or third party, respectively) or should reasonably have been known to such covered entity or third party (or person) to have occurred.

(c) METHODS OF INDIVIDUAL NOTIFICATION.—Notification required to be provided to an individual under subsection (a)(1)(B) with respect to a breach shall be provided in the following form:

(1) Written notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or, if specified as a preference by the indi-

vidual, by electronic mail. The notification may be provided in one or more mailings as information is available.

(2) In the case in which there is insufficient or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes direct written or (if specified by the individual) electronic notification to the individual, a substitute form of notification shall be provided, including, in the case that there are 500 or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting for a minimum of 30 days on the homepage of the website of the covered entity involved. Such a website posting shall include a toll-free telephone number that an individual can call to learn whether or not the individual's unsecured sensitive personally identifiable information is possibly included in the breach.

(3) In any case considered by the covered entity involved to require urgency because of possible imminent misuse of unsecured sensitive personally identifiable information, the covered entity, in addition to notification as required by paragraphs (1) and (2),

may provide information to individuals by telephone or other means, as appropriate.

(d) CONTENT OF NOTIFICATION.—Each notification of a breach under subsection (a)(1) shall include, to the extent possible, the following:

(1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

(2) A description of the types of unsecured sensitive personally identifiable information that were involved in the breach.

(3) The steps individuals should take to protect themselves from potential harm resulting from the breach.

(4) A brief description of what the entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.

(5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, a website, and a postal address.

(e) POSTING ON FTC PUBLIC WEBSITE.—The Commission shall make available to the public on the website of the Commission a list that identifies each covered entity that is required to notify 500 or more individuals of a

breach under subsection (a)(1)(B), except to the extent notification with respect to such breach is subject to a delay for law enforcement or national security purposes under subsection (f).

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

(1) IN GENERAL.—If the Director of the Federal Bureau of Investigation determines that the notifications required under subparagraphs (B), (C), and (D) of subsection (a)(1) would impede a criminal investigation or national security activity, the time period for such notifications shall be extended 30 days upon written notice from the Director to the covered entity that experienced the breach and to the Commission.

(2) EXTENDED DELAY OF NOTIFICATION.—If the time period for notification required under subparagraphs (B), (C), and (D) of subsection (a)(1) is extended pursuant to paragraph (1), a covered entity shall provide the notification within such time period unless the Director of the Federal Bureau of Investigation provides written notice to the covered entity and to the Commission that further extension of the time period is necessary. The Director 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 subsection.

SEC. 3. ENFORCEMENT BY FEDERAL TRADE COMMISSION; REGULATIONS.

(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 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. Any person 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) REGULATIONS.—Not later than 180 days after the date of the enactment of this Act, the Commission shall promulgate regulations in accordance with section 553 of title 5, United States Code, to implement this Act.

SEC. 4. REPORTS TO CONGRESS.

(a) IN GENERAL.—Not later than 12 months after the date of the enactment of this Act and annually thereafter, the Commission shall prepare and 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 containing information regarding breaches for which notification was provided to the Commission under section 2(a)(1)(A).

(b) INFORMATION REQUIRED.—Such information shall include—

(1) the number and nature of such breaches;

(2) the number of individuals affected; and

(3) actions taken in response to such breaches.

SEC. 5. EXCLUDED ENTITIES.

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

(1) covered 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)) that are subject to section 13402 of such Act (42 U.S.C. 17932); and

(2) covered 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 that are subject to section 13407 of such Act (42 U.S.C. 17937).

SEC. 6. DEFINITIONS.

In this Act:

(1) APPROPRIATE FEDERAL AGENCY.—The term ''appropriate Federal agency'' means—

(A) the Commission;

(B) the Federal Bureau of Investigation; and

(C) any other Federal agency specified by the Commission by regulation, which may include a specification of different Federal agencies depending on the types of activities in which covered entities are engaged.

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

(3) COVERED ENTITY.—The term ''covered entity'' means any person, partnership, or corporation over which the Commission has jurisdiction under section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)).

(4) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—

(A) IN GENERAL.—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:

(i) 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.

(ii) A Social Security number (but not including only the last four digits of a So-

cial Security number), driver's license number, passport number, or alien registration number or other Government-issued unique identification number.

(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, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.

(v) 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.

(vi) 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, elec-

tronic 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.

(B) 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—

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

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

(5) STATE.—The term ''State'' means each State of the United States, the District of Columbia, each commonwealth, territory, or possession of the United States, and each federally recognized Indian tribe.

(6) UNSECURED SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term ''unsecured sensitive personally identifiable information'' means sensitive personally identifiable information that is not secured by a technology standard that—

(A) renders information unusable, unreadable, or indecipherable to unauthorized individuals; and

(B) is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

SEC. 7. RELATIONSHIP TO STATE LAW.

This Act does not annul, alter, or affect, or exempt any person subject to the provisions of this Act from complying with, the laws of any State with respect to notification of a breach of personal information in electronic or digital form, except to the extent that those laws are inconsistent with any provision of this Act, and then only to the extent of the inconsistency. For purposes of this section, a State law is not inconsistent with this Act if the protection such law affords any consumer is greater than the protection provided by this Act.

SEC. 8. EFFECTIVE DATE.

This Act shall apply with respect to breaches that are discovered on or after the date that is 30 days after the

date on which the Commission promulgates the regulations required by section 3(c).

○