

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Cyber Breach Notifica-
5 tion Act of 2017”.

6 **SEC. 2. NOTIFICATION OF INFORMATION SECURITY** 7 **BREACH.**

8 (a) NOTIFICATION REQUIRED.—

1 (1) BY COVERED ENTITY.—A covered entity
2 that collects, uses, accesses, transmits, stores, or dis-
3 poses of unsecured sensitive personally identifiable
4 information in electronic or digital form shall, in the
5 case of a breach of such information that is discov-
6 ered by the covered entity, notify—

7 (A) appropriate Federal agencies;

8 (B) each individual whose unsecured sen-
9 sitive personally identifiable information has
10 been, or is reasonably believed by the covered
11 entity to have been, accessed, acquired, or dis-
12 closed as a result of such breach;

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

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

20 (2) BY THIRD PARTY.—

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

1 tity shall, following the discovery of a breach of
2 such information, notify the covered entity of
3 such breach. Such notification shall include the
4 identification of each individual whose unse-
5 cured sensitive personally identifiable informa-
6 tion has been, or is reasonably believed by the
7 third party to have been, accessed, acquired, or
8 disclosed during such breach and the informa-
9 tion described in paragraphs (1), (2), and (4)
10 of subsection (d) with respect to such breach.
11 The covered entity shall make the notifications
12 required by paragraph (1) with respect to such
13 breach.

14 (B) TO FTC AND FBI.—If there are 500 or
15 more individuals described in subparagraph (A)
16 with respect to a breach, the third party shall
17 provide the notification required by such sub-
18 paragraph to the Commission and the Federal
19 Bureau of Investigation, as well as to the cov-
20 ered entity. Notification by the third party
21 under this subparagraph does not relieve the
22 covered entity of the requirement to notify the
23 Commission and the Federal Bureau of Inves-
24 tigation under paragraph (1)(A).

25 (b) TIMELINESS OF NOTIFICATION.—

1 (1) IN GENERAL.—All notifications required
2 under subsection (a) shall be made in the most expe-
3 dient time possible and without unreasonable delay,
4 but in no case later than 30 calendar days after the
5 discovery of a breach by the covered entity involved
6 (or by the third party involved in the case of a noti-
7 fication required under subsection (a)(2)(A)).

8 (2) EXPEDITED NOTIFICATION TO FTC AND
9 FBI.—Notwithstanding paragraph (1), if there are
10 500 or more individuals to which a covered entity is
11 required to provide notification of a breach under
12 subsection (a)(1)(B), the covered entity shall notify
13 the Commission and the Federal Bureau of Inves-
14 tigation of such breach as required under subsection
15 (a)(1)(A) not later than 48 hours after the discovery
16 of such breach by the covered entity.

17 (3) EXPEDITED NOTIFICATION BY THIRD PAR-
18 TIES.—Notwithstanding paragraph (1), a third
19 party subject to subsection (a)(2)(B) with respect to
20 a breach shall make the notifications required by
21 such subsection not later than 48 hours after dis-
22 covery of the breach by the third party.

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

1 have the burden of demonstrating that all notifica-
2 tions were made as required under subsection (a),
3 including evidence demonstrating the necessity of
4 any delay.

5 (5) BREACHES TREATED AS DISCOVERED.—For
6 purposes of this section, a breach shall be treated as
7 discovered by a covered entity or, in the case of a
8 breach described in subsection (a)(2), by a third
9 party, as of the first day on which such breach is
10 known to such covered entity or third party, respec-
11 tively (including any person, other than the indi-
12 vidual committing the breach, that is an employee,
13 officer, or other agent of such covered entity or third
14 party, respectively) or should reasonably have been
15 known to such covered entity or third party (or per-
16 son) to have occurred.

17 (c) METHODS OF INDIVIDUAL NOTIFICATION.—Noti-
18 fication required to be provided to an individual under
19 subsection (a)(1)(B) with respect to a breach shall be pro-
20 vided in the following form:

21 (1) Written notification by first-class mail to
22 the individual (or the next of kin of the individual
23 if the individual is deceased) at the last known ad-
24 dress of the individual or the next of kin, respec-
25 tively, 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),

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

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

6 (1) A brief description of what happened, in-
7 cluding the date of the breach and the date of the
8 discovery of the breach, if known.

9 (2) A description of the types of unsecured sen-
10 sitive personally identifiable information that were
11 involved in the breach.

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

15 (4) A brief description of what the entity in-
16 volved is doing to investigate the breach, to mitigate
17 losses, and to protect against any further breaches.

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

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

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

5 (f) DELAY OF NOTIFICATION FOR LAW ENFORCE-
6 MENT OR NATIONAL SECURITY.—

7 (1) IN GENERAL.—If the Director of the Fed-
8 eral Bureau of Investigation determines that the no-
9 tifications required under subparagraphs (B), (C),
10 and (D) of subsection (a)(1) would impede a crimi-
11 nal investigation or national security activity, the
12 time period for such notifications shall be extended
13 30 days upon written notice from the Director to the
14 covered entity that experienced the breach and to
15 the Commission.

16 (2) EXTENDED DELAY OF NOTIFICATION.—If
17 the time period for notification required under sub-
18 paragraphs (B), (C), and (D) of subsection (a)(1) is
19 extended pursuant to paragraph (1), a covered enti-
20 ty shall provide the notification within such time pe-
21 riod unless the Director of the Federal Bureau of
22 Investigation provides written notice to the covered
23 entity and to the Commission that further extension
24 of the time period is necessary. The Director may

1 extend the time period for additional periods of up
2 to 30 days each.

3 (3) IMMUNITY.—No cause of action for which
4 jurisdiction is based under section 1346(b) of title
5 28, United States Code, shall lie against any Federal
6 law enforcement agency for acts relating to the ex-
7 tension of the deadline for notification for law en-
8 forcement or national security purposes under this
9 subsection.

10 **SEC. 3. ENFORCEMENT BY FEDERAL TRADE COMMISSION;**
11 **REGULATIONS.**

12 (a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—
13 A violation of this Act or a regulation promulgated under
14 this Act shall be treated as a violation of a regulation
15 under section 18(a)(1)(B) of the Federal Trade Commis-
16 sion Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or de-
17 ceptive acts or practices.

18 (b) POWERS OF COMMISSION.—The Commission
19 shall enforce this Act and the regulations promulgated
20 under this Act in the same manner, by the same means,
21 and with the same jurisdiction, powers, and duties as
22 though all applicable terms and provisions of the Federal
23 Trade Commission Act (15 U.S.C. 41 et seq.) were incor-
24 porated into and made a part of this Act. Any person who
25 violates this Act or a regulation promulgated under this

1 Act shall be subject to the penalties and entitled to the
2 privileges and immunities provided in the Federal Trade
3 Commission Act.

4 (c) REGULATIONS.—Not later than 180 days after
5 the date of the enactment of this Act, the Commission
6 shall promulgate regulations in accordance with section
7 553 of title 5, United States Code, to implement this Act.

8 **SEC. 4. REPORTS TO CONGRESS.**

9 (a) IN GENERAL.—Not later than 12 months after
10 the date of the enactment of this Act and annually there-
11 after, the Commission shall prepare and submit to the
12 Committee on Energy and Commerce of the House of
13 Representatives and the Committee on Commerce,
14 Science, and Transportation of the Senate a report con-
15 taining information regarding breaches for which notifica-
16 tion was provided to the Commission under section
17 2(a)(1)(A).

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

- 20 (1) the number and nature of such breaches;
- 21 (2) the number of individuals affected; and
- 22 (3) actions taken in response to such breaches.

23 **SEC. 5. EXCLUDED ENTITIES.**

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

1 (1) covered entities to the extent that such enti-
2 ties act as covered entities or business associates (as
3 such terms are defined in section 13400 of the
4 Health Information Technology for Economic and
5 Clinical Health Act (42 U.S.C. 17921)) that are
6 subject to section 13402 of such Act (42 U.S.C.
7 17932); and

8 (2) covered entities to the extent that they act
9 as vendors of personal health records (as such term
10 is defined in section 13400 of such Act (42 U.S.C.
11 17921)) and third-party service providers that are
12 subject to section 13407 of such Act (42 U.S.C.
13 17937).

14 **SEC. 6. DEFINITIONS.**

15 In this Act:

16 (1) APPROPRIATE FEDERAL AGENCY.—The
17 term “appropriate Federal agency” means—

18 (A) the Commission;

19 (B) the Federal Bureau of Investigation;

20 and

21 (C) any other Federal agency specified by
22 the Commission by regulation, which may in-
23 clude a specification of different Federal agen-
24 cies depending on the types of activities in
25 which covered entities are engaged.

1 (2) COMMISSION.—The term “Commission”
2 means the Federal Trade Commission.

3 (3) COVERED ENTITY.—The term “covered en-
4 tity” means any person, partnership, or corporation
5 over which the Commission has jurisdiction under
6 section 5(a)(2) of the Federal Trade Commission
7 Act (15 U.S.C. 45(a)(2)).

8 (4) SENSITIVE PERSONALLY IDENTIFIABLE IN-
9 FORMATION.—

10 (A) IN GENERAL.—The term “sensitive
11 personally identifiable information” means any
12 information, or compilation of information, in
13 electronic or digital form that includes one or
14 more of the following:

15 (i) An individual’s first and last name
16 or first initial and last name in combina-
17 tion with any two of the following data ele-
18 ments:

19 (I) Home address or telephone
20 number.

21 (II) Mother’s maiden name.

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

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

1 cial Security number), driver's license
2 number, passport number, or alien reg-
3 istration number or other Government-
4 issued unique identification number.

5 (iii) Unique biometric data such as a
6 finger print, voice print, a retina or iris
7 image, or any other unique physical rep-
8 resentation.

9 (iv) A unique account identifier, in-
10 cluding a financial account number or
11 credit or debit card number, electronic
12 identification number, user name, or rout-
13 ing code.

14 (v) A user name or electronic mail ad-
15 dress, in combination with a password or
16 security question and answer that would
17 permit access to an online account.

18 (vi) Any combination of the following
19 data elements:

20 (I) An individual's first and last
21 name or first initial and last name.

22 (II) A unique account identifier,
23 including a financial account number
24 or credit or debit card number, elec-

1 tronic identification number, user
2 name, or routing code.

3 (III) Any security code, access
4 code, or password, or source code that
5 could be used to generate such codes
6 or passwords.

7 (B) MODIFIED DEFINITION BY RULE-
8 MAKING.—The Commission may, by rule pro-
9 mulgated under section 553 of title 5, United
10 States Code, amend the definition of “sensitive
11 personally identifiable information” to the ex-
12 tent that such amendment will accomplish the
13 purposes of this Act. In amending the defini-
14 tion, the Commission may determine—

15 (i) that any particular combinations of
16 information are sensitive personally identi-
17 fiable information; or

18 (ii) that any particular piece of infor-
19 mation, on its own, is sensitive personally
20 identifiable information.

21 (5) STATE.—The term “State” means each
22 State of the United States, the District of Columbia,
23 each commonwealth, territory, or possession of the
24 United States, and each federally recognized Indian
25 tribe.

1 (6) UNSECURED SENSITIVE PERSONALLY IDEN-
2 TIFIABLE INFORMATION.—The term “unsecured sen-
3 sitive personally identifiable information” means
4 sensitive personally identifiable information that is
5 not secured by a technology standard that—

6 (A) renders information unusable, unread-
7 able, or indecipherable to unauthorized individ-
8 uals; and

9 (B) is developed or endorsed by a stand-
10 ards developing organization that is accredited
11 by the American National Standards Institute.

12 **SEC. 7. RELATIONSHIP TO STATE LAW.**

13 This Act does not annul, alter, or affect, or exempt
14 any person subject to the provisions of this Act from com-
15 plying with, the laws of any State with respect to notifica-
16 tion of a breach of personal information in electronic or
17 digital form, except to the extent that those laws are in-
18 consistent with any provision of this Act, and then only
19 to the extent of the inconsistency. For purposes of this
20 section, a State law is not inconsistent with this Act if
21 the protection such law affords any consumer is greater
22 than the protection provided by this Act.

23 **SEC. 8. EFFECTIVE DATE.**

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

- 1 date on which the Commission promulgates the regula-
- 2 tions required by section 3(c).

○