

114TH CONGRESS
1ST SESSION

H. R. 1704

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

IN THE HOUSE OF REPRESENTATIVES

MARCH 26, 2015

Mr. LANGEVIN 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.

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; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Personal Data Notification and Protection Act of 2015”.

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

Sec. 1. Short title; table of contents.

TITLE I—NATIONAL DATA BREACH NOTIFICATION STANDARD

- Sec. 101. Notification to individuals.
- Sec. 102. Exemptions from notification to individuals.
- Sec. 103. Methods of notification.
- Sec. 104. Content of notification.
- Sec. 105. Coordination of notification with credit reporting agencies.
- Sec. 106. Notification for law enforcement and other purposes.
- Sec. 107. Enforcement by the Federal Trade Commission.
- Sec. 108. Enforcement by State attorneys general.
- Sec. 109. Effect on State law.
- Sec. 110. Reporting on security breaches.
- Sec. 111. Excluded business entities.
- Sec. 112. Definitions.
- Sec. 113. Effective date.

TITLE II—EXTRATERRITORIAL APPLICATION OF CYBER CRIME
LAW

- Sec. 201. Extraterritorial jurisdiction.

1 **TITLE I—NATIONAL DATA**
2 **BREACH NOTIFICATION**
3 **STANDARD**

4 **SEC. 101. NOTIFICATION TO INDIVIDUALS.**

5 (a) IN GENERAL.—Except as provided for in section
6 102, any business entity engaged in or affecting interstate
7 commerce, that uses, accesses, transmits, stores, disposes
8 of, or collects sensitive personally identifiable information
9 about more than 10,000 individuals during any 12-month
10 period shall, following the discovery of a security breach
11 of such information, notify, in accordance with sections
12 103 and 104, any individual whose sensitive personally
13 identifiable information has been, or is reasonably believed
14 to have been, accessed or acquired.

15 (b) OBLIGATIONS OF AND TO OWNER OR LI-
16 CENSEE.—

1 (1) NOTIFICATION TO OWNER OR LICENSEE.—
2 Any business entity engaged in or affecting inter-
3 state commerce, that uses, accesses, transmits,
4 stores, disposes of, or collects sensitive personally
5 identifiable information that the business entity does
6 not own or license shall notify the owner or licensee
7 of the information following the discovery of a secu-
8 rity breach involving such information, unless there
9 is no reasonable risk of harm or fraud to such owner
10 or licensee.

11 (2) NOTIFICATION BY OWNER, LICENSEE, OR
12 OTHER DESIGNATED THIRD PARTY.—Nothing in this
13 title shall prevent or abrogate an agreement between
14 a business entity required to provide notification
15 under this section and a designated third party, in-
16 cluding an owner or licensee of the sensitive person-
17 ally identifiable information subject to the security
18 breach, to provide the notifications required under
19 subsection (a).

20 (3) BUSINESS ENTITY RELIEVED FROM GIVING
21 NOTIFICATION.—A business entity required to pro-
22 vide notification under subsection (a) shall not be re-
23 quired to provide such notification if an owner or li-
24 censee of the sensitive personally identifiable infor-

1 mation subject to the security breach, or other des-
2 ignated third party, provides such notification.

3 (c) TIMELINESS OF NOTIFICATION.—

4 (1) IN GENERAL.—All notifications required
5 under this section shall be made without unreason-
6 able delay following the discovery by the business en-
7 tity of a security breach. A business entity shall,
8 upon the request of the Commission, provide records
9 or other evidence of the notifications required under
10 this section.

11 (2) REASONABLE DELAY.—

12 (A) IN GENERAL.—Except as provided in
13 subsection (d), reasonable delay under this sub-
14 section shall not exceed 30 days, unless the
15 business entity seeking additional time requests
16 an extension of time and the Commission deter-
17 mines that additional time is reasonably nec-
18 essary to determine the scope of the security
19 breach, prevent further disclosures, conduct the
20 risk assessment, restore the reasonable integrity
21 of the data system, or provide notice to the
22 breach notification entity.

23 (B) EXTENSION.—If the Commission de-
24 termines that additional time is reasonably nec-
25 essary as described in subparagraph (A), the

1 Commission may extend the time period for no-
2 tification for additional periods of up to 30 days
3 each. Any such extension shall be provided in
4 writing by the Commission.

5 (3) BURDEN OF PRODUCTION.—If a business
6 entity requires additional time under paragraph (2),
7 the business entity shall provide the Commission
8 with records or other evidence of the reasons neces-
9 sitating delay of notification.

10 (d) DELAY OF NOTIFICATION FOR LAW ENFORCE-
11 MENT OR NATIONAL SECURITY.—

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

20 (2) EXTENDED DELAY OF NOTIFICATION.—If
21 the time period for notification required under sub-
22 section (a) is extended pursuant to paragraph (1), a
23 business entity shall provide the notification within
24 such time period unless the Director of the United
25 States Secret Service or the Director of the Federal

1 Bureau of Investigation provides written notification
2 that further extension of the time period is nec-
3 essary. The Director of the United States Secret
4 Service or the Director of the Federal Bureau of In-
5 vestigation may extend the time period for additional
6 periods of up to 30 days each.

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

14 (e) DESIGNATION OF BREACH NOTIFICATION ENTI-
15 TY.—Not later than 60 days after the date of the enact-
16 ment of this Act, the Secretary of Homeland Security shall
17 designate a Federal Government entity to receive notices,
18 reports, and information about information security inci-
19 dents, threats, and vulnerabilities under this title.

20 **SEC. 102. EXEMPTIONS FROM NOTIFICATION TO INDIVID-**
21 **UALS.**

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

24 (1) IN GENERAL.—Notwithstanding section
25 101, if the Director of the United States Secret

1 Service or the Director of the Federal Bureau of In-
2 vestigation determines that notification of the secu-
3 rity breach required by such section could be ex-
4 pected to reveal sensitive sources and methods or
5 similarly impede the ability of a Federal, State, or
6 local law enforcement agency to conduct law enforce-
7 ment investigations, or if the Director of the Federal
8 Bureau of Investigation determines that notification
9 of the security breach could be expected to cause
10 damage to national security, such notification is not
11 required.

12 (2) IMMUNITY.—No cause of action for which
13 jurisdiction is based under section 1346(b) of title
14 28, United States Code, shall lie against any Federal
15 law enforcement agency for acts relating to the ex-
16 tension of the deadline for notification for law en-
17 forcement or national security purposes under this
18 section.

19 (b) SAFE HARBOR.—

20 (1) IN GENERAL.—A business entity is exempt
21 from the notification requirement under section 101,
22 if the following requirements are met:

23 (A) RISK ASSESSMENT.—A risk assess-
24 ment, in accordance with paragraph (3), is con-
25 ducted by or on behalf of the business entity

1 that concludes that there is no reasonable risk
2 that a security breach has resulted in, or will
3 result in, harm to the individuals whose sen-
4 sitive personally identifiable information was
5 subject to the security breach.

6 (B) NOTICE TO COMMISSION.—Without
7 unreasonable delay and not later than 30 days
8 after the discovery of a security breach, unless
9 extended by the Commission, the Director of
10 the United States Secret Service, or the Direc-
11 tor of the Federal Bureau of Investigation
12 under section 101 (in which case, before the ex-
13 tended deadline), the business entity notifies
14 the Commission, in writing, of—

15 (i) the results of the risk assessment;

16 and

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

20 (C) DETERMINATION BY COMMISSION.—
21 During the period beginning on the date on
22 which the notification described in subpara-
23 graph (B) is submitted and ending 10 days
24 after such date, the Commission has not issued

1 a determination in writing that a notification
2 should be provided under section 101.

3 (2) REBUTTABLE PRESUMPTION.—For pur-
4 poses of paragraph (1)—

5 (A) the rendering of sensitive personally
6 identifiable information at issue unusable,
7 unreadable, or indecipherable through a secu-
8 rity technology generally accepted by experts in
9 the field of information security shall establish
10 a rebuttable presumption that such reasonable
11 risk does not exist; and

12 (B) any such presumption shall be rebutta-
13 ble by facts demonstrating that the security
14 technologies or methodologies in a specific case
15 have been, or are reasonably likely to have
16 been, compromised.

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

20 (A) PROPERLY CONDUCTED.—The risk as-
21 sessment is conducted in a reasonable manner
22 or according to standards generally accepted by
23 experts in the field of information security.

24 (B) LOGGING DATA REQUIRED.—The risk
25 assessment includes logging data, as applicable

1 and to the extent available, for a period of at
2 least six months before the discovery of a secu-
3 rity breach described in section 101(a)—

4 (i) for each communication or at-
5 tempted communication with a database or
6 data system containing sensitive personally
7 identifiable information, the data system
8 communication information for the com-
9 munication or attempted communication,
10 including any Internet addresses, and the
11 date and time associated with the commu-
12 nication or attempted communication; and

13 (ii) all log-in information associated
14 with databases or data systems containing
15 sensitive personally identifiable informa-
16 tion, including both administrator and user
17 log-in information.

18 (C) FRAUDULENT OR MISLEADING INFOR-
19 MATION.—The risk assessment does not contain
20 fraudulent or deliberately misleading informa-
21 tion.

22 (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

23 (1) IN GENERAL.—A business entity is exempt
24 from the notification requirement under section 101

1 if the business entity uses or participates in a secu-
2 rity program that—

3 (A) effectively blocks the use of the sen-
4 sitive personally identifiable information to ini-
5 tiate unauthorized financial transactions before
6 they are charged to the account of the indi-
7 vidual; and

8 (B) provides notification to affected indi-
9 viduals after a security breach that has resulted
10 in fraud or unauthorized transactions.

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

17 **SEC. 103. METHODS OF NOTIFICATION.**

18 A business entity shall be in compliance with the re-
19 quirements of this section if, with respect to the method
20 of notification as required under section 101, the following
21 requirements are met:

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

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

4 (B) Telephone notification to the individual
5 personally.

6 (C) E-mail notification, if the individual
7 has consented to receive such notification and
8 the notification is consistent with the provisions
9 permitting electronic transmission of notifica-
10 tions under section 101 of the Electronic Signa-
11 tures in Global and National Commerce Act (15
12 U.S.C. 7001).

13 (2) MEDIA NOTIFICATION.—If the number of
14 residents of a State whose sensitive personally iden-
15 tifiable information was, or is reasonably believed to
16 have been, accessed or acquired by an unauthorized
17 person exceeds 5,000, notification is provided to
18 media reasonably calculated to reach such individ-
19 uals, such as major media outlets serving a State or
20 jurisdiction.

21 **SEC. 104. CONTENT OF NOTIFICATION.**

22 The notification provided to individuals required by
23 section 101 shall include, to the extent possible, the fol-
24 lowing:

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

5 (2) A toll-free number—

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

9 (B) from which the individual may learn
10 what types of sensitive personally identifiable
11 information the business entity maintained
12 about that individual.

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

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

18 (5) Notwithstanding section 109, any informa-
19 tion regarding victim protection assistance required
20 by the State in which the individual resides.

21 **SEC. 105. COORDINATION OF NOTIFICATION WITH CREDIT**
22 **REPORTING AGENCIES.**

23 (a) **REQUIREMENT TO NOTIFY CREDIT REPORTING**
24 **AGENCIES.**—If a business entity is required to notify more
25 than 5,000 individuals under section 101, the business en-

1 tity shall also notify each consumer reporting agency that
2 compiles and maintains files on consumers on a nation-
3 wide basis (as defined in section 603(p) of the Fair Credit
4 Reporting Act (15 U.S.C. 1681a(p))) of the timing and
5 distribution of the notifications. Such notification shall be
6 given to the consumer credit reporting agencies without
7 unreasonable delay and, if it will not delay notification to
8 the affected individuals, prior to the distribution of notifi-
9 cations to the affected individuals.

10 (b) REASONABLE DELAY.—Reasonable delay under
11 subsection (a) shall not exceed 30 days following the dis-
12 covery of a security breach, except as provided in sub-
13 section (c) or (d) of section 101 (in which case, before
14 the extended deadline), or unless the business entity pro-
15 viding notification can demonstrate to the Commission
16 that additional time is reasonably necessary to determine
17 the scope of the security breach, prevent further disclo-
18 sures, conduct the risk assessment, restore the reasonable
19 integrity of the data system, and provide notice to the
20 breach notification entity. If the Commission determines
21 that additional time is necessary, the Commission may ex-
22 tend the time period for notification for additional periods
23 of up to 30 days each. Any such extension shall be pro-
24 vided in writing.

1 **SEC. 106. NOTIFICATION FOR LAW ENFORCEMENT AND**
2 **OTHER PURPOSES.**

3 (a) NOTIFICATION TO LAW ENFORCEMENT AND NA-
4 TIONAL SECURITY AUTHORITIES.—Any business entity
5 shall notify the breach notification entity, and the breach
6 notification entity shall promptly notify and provide that
7 information to the United States Secret Service, the Fed-
8 eral Bureau of Investigation, and the Commission for civil
9 law enforcement purposes, and shall make it available as
10 appropriate to other Federal agencies for law enforcement,
11 national security, or computer security purposes, if—

12 (1) the number of individuals whose sensitive
13 personally identifiable information was, or is reason-
14 ably believed to have been, accessed or acquired by
15 an unauthorized person exceeds 5,000;

16 (2) the security breach involves a database,
17 networked or integrated databases, or other data
18 system containing the sensitive personally identifi-
19 able information of more than 500,000 individuals
20 nationwide;

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

23 (4) the security breach involves primarily sen-
24 sitive personally identifiable information of individ-
25 uals known to the business entity to be employees

1 and contractors of the Federal Government involved
2 in national security or law enforcement.

3 (b) REGULATIONS.—Not later than one year after the
4 date of enactment of this Act, the Commission shall pro-
5 mulgate regulations (in accordance with section 553 of
6 title 5, United States Code) in consultation with the Attor-
7 ney General and the Secretary of Homeland Security, that
8 describe what information is required to be included in the
9 notification under subsection (a). In addition the Commis-
10 sion shall promulgate regulations, as necessary, (in ac-
11 cordance with section 553 of title 5, United States Code)
12 in consultation with the Attorney General, to adjust the
13 thresholds for notification to law enforcement and national
14 security authorities under subsection (a) and to facilitate
15 the purposes of this section.

16 (c) TIMING OF NOTIFICATION.—The notification re-
17 quired under this section shall be provided as promptly
18 as possible and at least 72 hours before notification of an
19 individual pursuant to section 101 or 10 days after dis-
20 covery of the breach requiring notification, whichever
21 comes first.

22 **SEC. 107. ENFORCEMENT BY THE FEDERAL TRADE COM-**
23 **MISSION.**

24 (a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—
25 A violation of this title or a regulation promulgated under

1 this title shall be treated as a violation of a regulation
2 under section 18(a)(1)(B) of the Federal Trade Commis-
3 sion Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or de-
4 ceptive acts or practices.

5 (b) POWERS OF COMMISSION.—The Federal Trade
6 Commission shall enforce this title and the regulations
7 promulgated under this title in the same manner, by the
8 same means, and with the same jurisdiction, powers, and
9 duties as though all applicable terms and provisions of the
10 Federal Trade Commission Act (15 U.S.C. 41 et seq.)
11 were incorporated into and made a part of this Act, except
12 that the exceptions described in section 5(a)(2) of such
13 Act (15 U.S.C. 45(a)(2)) shall not apply. Any business
14 entity who violates this title or a regulation promulgated
15 under this title shall be subject to the penalties and enti-
16 tled to the privileges and immunities provided in the Fed-
17 eral Trade Commission Act.

18 (c) FEDERAL COMMUNICATIONS COMMISSION.—In a
19 case in which enforcement under this title involves a busi-
20 ness entity that is subject to the authority of the Federal
21 Communications Commission, enforcement actions by the
22 Commission, the Commission shall consult with the Fed-
23 eral Communications Commission.

24 (d) CONSUMER FINANCIAL PROTECTION BUREAU.—
25 In a case in which enforcement under this title relates to

1 financial information or information associated with the
2 provision of a consumer financial product or service, en-
3 forcement actions by the Commission, the Commission
4 shall consult with the Consumer Financial Protection Bu-
5 reau.

6 (e) CONSULTATION WITH THE ATTORNEY GENERAL
7 REQUIRED.—The Commission shall consult with the At-
8 torney General before opening an investigation. If the At-
9 torney General determines that such an investigation
10 would impede an ongoing criminal investigation or na-
11 tional security activity, the Commission may not open such
12 investigation.

13 (f) REGULATIONS.—

14 (1) IN GENERAL.—The Commission may pro-
15 mulgate regulations, in addition to the regulations
16 promulgated pursuant to section 106(b), relating to
17 the duties of the Commission under this title, in ac-
18 cordance with section 553 of title 5, United States
19 Code, as the Commission determines to be necessary
20 to carry out this title.

21 (2) FEDERAL COMMUNICATIONS COMMISSION.—
22 With regard to a regulation promulgated under this
23 section that relates to an entity subject to the au-
24 thority of the Federal Communications Commission,
25 the Commission may only promulgate such regula-

1 tion after consultation with the Federal Communica-
2 tions Commission.

3 (3) CONSUMER FINANCIAL PROTECTION BU-
4 REAU.—With regard to a regulation promulgated
5 under this section that relates to financial informa-
6 tion or information associated with the provision of
7 a consumer financial product or service, the Com-
8 mission may only promulgate such regulation after
9 consultation with the Consumer Financial Protection
10 Bureau.

11 **SEC. 108. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

12 (a) IN GENERAL.—

13 (1) CIVIL ACTIONS.—In any case in which the
14 attorney general of a State or an official or agency
15 of a State has reason to believe that an interest of
16 the residents of that State has been or is threatened
17 or adversely affected by an act or practice in viola-
18 tion of this title or a regulation promulgated under
19 this title, the State, as *parens patriae*, may bring a
20 civil action on behalf of the residents of the State in
21 an appropriate State court or an appropriate district
22 court of the United States to—

23 (A) enjoin that practice;

24 (B) enforce compliance with this title; or

1 (C) impose civil penalties of not more than
2 \$1,000 per day per individual whose sensitive
3 personally identifiable information was, or is
4 reasonably believed to have been, accessed or
5 acquired by an unauthorized person, up to a
6 maximum of \$1,000,000 per violation, unless
7 such conduct is found to be willful or inten-
8 tional.

9 (2) NOTICE.—Before filing an action under
10 paragraph (1), the attorney general, official, or
11 agency of the State involved shall provide to the At-
12 torney General and the Commission—

13 (A) a written notice of the action; and

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

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

20 (b) AUTHORITY OF FEDERAL TRADE COMMISSION.—

21 Upon receiving notice under subsection (a)(2), the Com-
22 mission may—

23 (1) move to stay the action, pending the final
24 disposition of a pending Federal proceeding or ac-
25 tion;

1 (2) initiate an action in the appropriate United
2 States district court under section 107 and move to
3 consolidate all pending actions, including State ac-
4 tions, in such court;

5 (3) intervene in the action brought under sub-
6 section (a); or

7 (4) file petitions for appeal.

8 (c) PENDING PROCEEDINGS.—If the Commission has
9 instituted a proceeding or action for a violation of this title
10 or any regulations promulgated under this title, a State
11 attorney general, official, or agency may not bring an ac-
12 tion under this title during the pendency of the Federal
13 action against any defendant named in such proceeding
14 or action for any violation that is alleged in that pro-
15 ceeding or action.

16 (d) CONSTRUCTION.—For purposes of bringing any
17 civil action under subsection (a), nothing in this title shall
18 be construed to prevent an attorney general, official, or
19 agency of a State from exercising the powers conferred
20 on such attorney general, official, or agency by the laws
21 of that State to—

22 (1) conduct investigations;

23 (2) administer oaths or affirmations; or

24 (3) compel the attendance of witnesses or the
25 production of documentary and other evidence.

1 (e) VENUE; SERVICE OF PROCESS.—

2 (1) VENUE.—Any action brought under sub-
3 section (a) may be brought in—

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

8 (B) another court of competent jurisdic-
9 tion.

10 (2) SERVICE OF PROCESS.—In an action
11 brought under subsection (a), process may be served
12 in any district in which the defendant—

13 (A) is an inhabitant; or

14 (B) may be found.

15 **SEC. 109. EFFECT ON STATE LAW.**

16 The provisions of this title shall supersede any provi-
17 sion of the law of any State, or a political subdivision
18 thereof, relating to notification by a business entity en-
19 gaged in interstate commerce of a security breach, except
20 as provided in section 104(5).

21 **SEC. 110. REPORTING ON SECURITY BREACHES.**

22 (a) REPORT REQUIRED ON NATIONAL SECURITY AND
23 LAW ENFORCEMENT EXEMPTIONS.—Not later than 18
24 months after the date of enactment of this title, and annu-
25 ally thereafter, the Director of the United States Secret

1 Service and the Director of the Federal Bureau of Inves-
2 tigation shall submit to the Committee on Energy and
3 Commerce of the House of Representatives and the Com-
4 mittee on Commerce, Science, and Transportation of the
5 Senate on a report on the number and nature of security
6 breaches subject to the national security and law enforce-
7 ment exemptions under section 102(a).

8 (b) REPORT REQUIRED ON SAFE HARBOR EXEMP-
9 TIONS.—Not later than 18 months after the date of enact-
10 ment of this title, and annually thereafter, the Commission
11 shall submit to the Committee on Energy and Commerce
12 of the House of Representatives and the Committee on
13 Commerce, Science, and Transportation of the Senate a
14 report on the number and nature of the security breaches
15 described in the notices filed by business entities invoking
16 the risk assessment exemption under section 102(b) and
17 the response of the Commission to such notices.

18 **SEC. 111. EXCLUDED BUSINESS ENTITIES.**

19 Nothing in this title, or the regulations promulgated
20 under this title, shall apply to—

21 (1) business entities to the extent that such en-
22 tities act as covered entities or business associates
23 (as such terms are defined in section 13400 of the
24 Health Information Technology for Economic and

1 Clinical Health Act (42 U.S.C. 17921)) subject to
2 section 13402 of such Act (42 U.S.C. 17932); and

3 (2) business entities to the extent that they act
4 as vendors of personal health records (as such term
5 is defined in section 13400 of such Act (42 U.S.C.
6 17921)) and third-party service providers subject to
7 section 13407 of such Act (42 U.S.C. 17937).

8 **SEC. 112. DEFINITIONS.**

9 In this title:

10 (1) **AFFILIATE.**—The term “affiliate” means
11 persons related by common ownership or by cor-
12 porate control.

13 (2) **BREACH NOTIFICATION ENTITY.**—The term
14 “breach notification entity” means the Federal Gov-
15 ernment entity designated pursuant to section
16 101(e).

17 (3) **BUSINESS ENTITY.**—The term “business
18 entity” means any organization, corporation, trust,
19 partnership, sole proprietorship, unincorporated as-
20 sociation, or venture, whether or not established to
21 make a profit.

22 (4) **COMMISSION.**—The term “Commission”
23 means the Federal Trade Commission.

24 (5) **CONSUMER FINANCIAL PRODUCT OR SERV-**
25 **ICE.**—The term “consumer financial product or

1 service” has the meaning given that term in section
2 1002 of the Dodd-Frank Wall Street Reform and
3 Consumer Protection Act (12 U.S.C. 5481).

4 (6) DATA SYSTEM COMMUNICATION INFORMA-
5 TION.—The term “data system communication in-
6 formation” means dialing, routing, addressing, or
7 signaling information that identifies the origin, di-
8 rection, destination, processing, transmission, or ter-
9 mination of each communication initiated, at-
10 tempted, or received.

11 (7) DATE AND TIME.—The term “date and
12 time” includes the date, time, and specification of
13 the time zone offset from Coordinated Universal
14 Time.

15 (8) FEDERAL AGENCY.—The term “Federal
16 agency” has the meaning given the term “agency”
17 in section 3502 of title 44, United States Code.

18 (9) INTELLIGENCE COMMUNITY.—The term
19 “intelligence community” has the meaning given
20 that term in section 3(4) of the National Security
21 Act of 1947 (50 U.S.C. 3003(4)).

22 (10) INTERNET ADDRESS.—The term “Internet
23 address” means an Internet Protocol address as
24 specified by the Internet Protocol version 4 or 6 pro-

1 protocol, or any successor protocol or any unique num-
2 ber for a specific host on the Internet.

3 (11) SECURITY BREACH.—

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

9 (i) the unauthorized acquisition of
10 sensitive personally identifiable informa-
11 tion; or

12 (ii) access to sensitive personally iden-
13 tifiable information that is for an unau-
14 thorized purpose, or in excess of authoriza-
15 tion.

16 (B) EXCLUSION.—The term “security
17 breach” does not include any lawfully author-
18 ized investigative, protective, or intelligence ac-
19 tivity of a law enforcement agency of the
20 United States, a State, or a political subdivision
21 of a State, or of an element of the intelligence
22 community.

23 (12) SENSITIVE PERSONALLY IDENTIFIABLE IN-
24 FORMATION.—The term “sensitive personally identi-
25 fiable information” means any information or com-

1 pilation of information, in electronic or digital form
2 that includes one or more of the following:

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

6 (i) Home address or telephone num-
7 ber.

8 (ii) Mother's maiden name.

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

10 (B) A social security number (but not in-
11 cluding only the last four digits of a social secu-
12 rity number), driver's license number, passport
13 number, or alien registration number or other
14 government-issued unique identification num-
15 ber.

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

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

23 (E) A user name or electronic mail ad-
24 dress, in combination with a password or secu-

1 rity question and answer that would permit ac-
2 cess to an online account.

3 (F) Any combination of the following data
4 elements:

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

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

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

15 (13) MODIFIED DEFINITION BY RULE-
16 MAKING.—The Commission may, by rule promul-
17 gated under section 553 of title 5, United States
18 Code, amend the definition of “sensitive personally
19 identifiable information” to the extent that such
20 amendment will accomplish the purposes of this
21 title. In amending the definition, the Commission
22 may determine—

23 (A) that any particular combinations of in-
24 formation are sensitive personally identifiable
25 information; or

1 (B) that any particular piece of informa-
2 tion, on its own, is sensitive personally identifi-
3 able information.

4 **SEC. 113. EFFECTIVE DATE.**

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

7 **TITLE II—EXTRATERRITORIAL**
8 **APPLICATION OF CYBER**
9 **CRIME LAW**

10 **SEC. 201. EXTRATERRITORIAL JURISDICTION.**

11 Subsection (h) of section 1029 of title 18, United
12 States Code, is amended to read as follows:

13 “(h) Any person who, outside the jurisdiction of the
14 United States, engages in any act that, if committed with-
15 in the jurisdiction of the United States, would constitute
16 an offense under subsection (a) or (b), shall be subject
17 to the fines, penalties, imprisonment, and forfeiture pro-
18 vided in this title if the offense involves an access device
19 issued, owned, managed, or controlled by a financial insti-
20 tution, account issuer, credit card system member, or
21 other entity organized under the laws of the United
22 States, or any State, the District of Columbia, or other
23 territory of the United States.”.

○