

.....
(Original Signature of Member)

115TH CONGRESS
1ST SESSION

H. R.

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

IN THE HOUSE OF REPRESENTATIVES

Mr. LANGEVIN introduced the following bill; which was referred to the Committee on _____

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 2017”.

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

- Sec. 1. Short title; table of contents.
- Sec. 2. Notification to individuals.
- Sec. 3. Exemptions from notification to individuals.
- Sec. 4. Methods of notification.

- Sec. 5. Content of notification.
- Sec. 6. Coordination of notification with credit reporting agencies.
- Sec. 7. Notification for law enforcement and other purposes.
- Sec. 8. Enforcement by the Federal Trade Commission.
- Sec. 9. Enforcement by State attorneys general.
- Sec. 10. Effect on State law.
- Sec. 11. Reporting on security breaches.
- Sec. 12. Excluded business entities.
- Sec. 13. Definitions.
- Sec. 14. Effective date.

1 SEC. 2. NOTIFICATION TO INDIVIDUALS.

2 (a) IN GENERAL.—Except as provided for in section
3 3, any business entity engaged in or affecting interstate
4 commerce, that uses, accesses, transmits, stores, disposes
5 of, or collects sensitive personally identifiable information
6 about more than 10,000 individuals during any 12-month
7 period shall, following the discovery of a security breach
8 of such information, notify, in accordance with sections
9 4 and 5, any individual whose sensitive personally identifi-
10 able information has been, or is reasonably believed to
11 have been, accessed or acquired.

12 (b) OBLIGATIONS OF AND TO OWNER OR LI-
13 CENSEE.—

14 (1) NOTIFICATION TO OWNER OR LICENSEE.—

15 Any business entity engaged in or affecting inter-
16 state commerce, that uses, accesses, transmits,
17 stores, disposes of, or collects sensitive personally
18 identifiable information that the business entity does
19 not own or license shall notify the owner or licensee
20 of the information following the discovery of a secu-

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

4 (2) NOTIFICATION BY OWNER, LICENSEE, OR
5 OTHER DESIGNATED THIRD PARTY.—Nothing in this
6 Act shall prevent or abrogate an agreement between
7 a business entity required to provide notification
8 under this section and a designated third party, in-
9 cluding an owner or licensee of the sensitive person-
10 ally identifiable information subject to the security
11 breach, to provide the notifications required under
12 subsection (a).

13 (3) BUSINESS ENTITY RELIEVED FROM GIVING
14 NOTIFICATION.—A business entity required to pro-
15 vide notification under subsection (a) shall not be re-
16 quired to provide such notification if an owner or li-
17 censee of the sensitive personally identifiable infor-
18 mation subject to the security breach, or other des-
19 ignated third party, provides such notification.

20 (c) TIMELINESS OF NOTIFICATION.—

21 (1) IN GENERAL.—All notifications required
22 under this section shall be made without unreason-
23 able delay following the discovery by the business en-
24 tity of a security breach. A business entity shall,
25 upon the request of the Commission, provide records

1 or other evidence of the notifications required under
2 this section.

3 (2) REASONABLE DELAY.—

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

15 (B) EXTENSION.—If the Commission de-
16 termines that additional time is reasonably nec-
17 essary as described in subparagraph (A), the
18 Commission may extend the time period for no-
19 tification for additional periods of up to 30 days
20 each. Any such extension shall be provided in
21 writing by the Commission.

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

1 with records or other evidence of the reasons neces-
2 sitating delay of notification.

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

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

13 (2) EXTENDED DELAY OF NOTIFICATION.—If
14 the time period for notification required under sub-
15 section (a) is extended pursuant to paragraph (1), a
16 business entity shall provide the notification within
17 such time period unless the Director of the United
18 States Secret Service or the Director of the Federal
19 Bureau of Investigation provides written notification
20 that further extension of the time period is nec-
21 essary. The Director of the United States Secret
22 Service or the Director of the Federal Bureau of In-
23 vestigation may extend the time period for additional
24 periods of up to 30 days each.

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

8 (e) DESIGNATION OF BREACH NOTIFICATION ENTI-
9 TY.—Not later than 60 days after the date of the enact-
10 ment of this Act, the Secretary of Homeland Security shall
11 designate a Federal Government entity to receive notices,
12 reports, and information about information security inci-
13 dents, threats, and vulnerabilities under this Act.

14 **SEC. 3. EXEMPTIONS FROM NOTIFICATION TO INDIVID-**
15 **UALS.**

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

18 (1) IN GENERAL.—Notwithstanding section 2,
19 if the Director of the United States Secret Service
20 or the Director of the Federal Bureau of Investiga-
21 tion determines that notification of the security
22 breach required by such section could be expected to
23 reveal sensitive sources and methods or similarly im-
24 pede the ability of a Federal, State, or local law en-
25 forcement agency to conduct law enforcement inves-

1 tigungen, or if the Director of the Federal Bureau
2 of Investigation determines that notification of the
3 security breach could be expected to cause damage
4 to national security, such notification is not re-
5 quired.

6 (2) IMMUNITY.—No cause of action for which
7 jurisdiction is based under section 1346(b) of title
8 28, United States Code, shall lie against any Federal
9 law enforcement agency for acts relating to provision
10 of an exemption from notification for law enforce-
11 ment or national security purposes under this sec-
12 tion.

13 (b) SAFE HARBOR.—

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

17 (A) RISK ASSESSMENT.—A risk assess-
18 ment, in accordance with paragraph (3), is con-
19 ducted by or on behalf of the business entity
20 that concludes that there is no reasonable risk
21 that a security breach has resulted in, or will
22 result in, harm to the individuals whose sen-
23 sitive personally identifiable information was
24 subject to the security breach.

1 (B) NOTICE TO COMMISSION.—Without
2 unreasonable delay and not later than 30 days
3 after the discovery of a security breach, unless
4 extended by the Commission, the Director of
5 the United States Secret Service, or the Direc-
6 tor of the Federal Bureau of Investigation
7 under section 2 (in which case, before the ex-
8 tended deadline), the business entity notifies
9 the Commission, in writing, of—

10 (i) the results of the risk assessment;

11 and

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

15 (C) DETERMINATION BY COMMISSION.—

16 During the period beginning on the date on
17 which the notification described in subpara-
18 graph (B) is submitted and ending 10 days
19 after such date, the Commission has not issued
20 a determination in writing that a notification
21 should be provided under section 2.

22 (2) REBUTTABLE PRESUMPTION.—For pur-
23 poses of paragraph (1)—

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

1 unreadable, or indecipherable through a secu-
2 rity technology generally accepted by experts in
3 the field of information security shall establish
4 a rebuttable presumption that such reasonable
5 risk does not exist; and

6 (B) any such presumption shall be rebut-
7 table by facts demonstrating that the security
8 technologies or methodologies in a specific case
9 have been, or are reasonably likely to have
10 been, compromised.

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

14 (A) PROPERLY CONDUCTED.—The risk as-
15 sessment is conducted in a reasonable manner
16 or according to standards generally accepted by
17 experts in the field of information security.

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

23 (i) for each communication or at-
24 tempted communication with a database or
25 data system containing sensitive personally

1 identifiable information, the data system
2 communication information for the com-
3 munication or attempted communication,
4 including any Internet addresses, and the
5 date and time associated with the commu-
6 nication or attempted communication; and
7 (ii) all log-in information associated
8 with databases or data systems containing
9 sensitive personally identifiable informa-
10 tion, including both administrator and user
11 log-in information.

12 (C) FRAUDULENT OR MISLEADING INFOR-
13 MATION.—The risk assessment does not contain
14 fraudulent or deliberately misleading informa-
15 tion.

16 (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

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

21 (A) effectively blocks the use of the sen-
22 sitive personally identifiable information to ini-
23 tiate unauthorized financial transactions before
24 they are charged to the account of the indi-
25 vidual; and

1 (B) provides notification to affected indi-
2 viduals after a security breach that has resulted
3 in fraud or unauthorized transactions.

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

10 **SEC. 4. METHODS OF NOTIFICATION.**

11 A business entity shall be in compliance with the re-
12 quirements of this section if, with respect to the method
13 of notification as required under section 2, the following
14 requirements are met:

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

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

20 (B) Telephone notification to the individual
21 personally.

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

1 tions under section 101 of the Electronic Signa-
2 tures in Global and National Commerce Act (15
3 U.S.C. 7001).

4 (2) MEDIA NOTIFICATION.—If the number of
5 residents of a State whose sensitive personally iden-
6 tifiable information was, or is reasonably believed to
7 have been, accessed or acquired by an unauthorized
8 person exceeds 5,000, notification is provided to
9 media reasonably calculated to reach such individ-
10 uals, such as major media outlets serving a State or
11 jurisdiction.

12 **SEC. 5. CONTENT OF NOTIFICATION.**

13 The notification provided to individuals required by
14 section 2 shall include, to the extent possible, the fol-
15 lowing:

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

20 (2) A toll-free number—

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

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

1 information the business entity maintained
2 about that individual.

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

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

8 (5) Notwithstanding section 10, any informa-
9 tion regarding victim protection assistance required
10 by the State in which the individual resides.

11 **SEC. 6. COORDINATION OF NOTIFICATION WITH CREDIT**
12 **REPORTING AGENCIES.**

13 (a) REQUIREMENT TO NOTIFY CREDIT REPORTING
14 AGENCIES.—If a business entity is required to notify more
15 than 5,000 individuals under section 2, the business entity
16 shall also notify each consumer reporting agency that com-
17 piles and maintains files on consumers on a nationwide
18 basis (as defined in section 603(p) of the Fair Credit Re-
19 porting Act (15 U.S.C. 1681a(p))) of the timing and dis-
20 tribution of the notifications. Such notification shall be
21 given to the consumer credit reporting agencies without
22 unreasonable delay and, if it will not delay notification to
23 the affected individuals, prior to the distribution of notifi-
24 cations to the affected individuals.

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

15 **SEC. 7. NOTIFICATION FOR LAW ENFORCEMENT AND**
16 **OTHER PURPOSES.**

17 (a) NOTIFICATION TO LAW ENFORCEMENT AND NA-
18 TIONAL SECURITY AUTHORITIES.—Any business entity
19 shall notify the breach notification entity, and the breach
20 notification entity shall promptly notify and provide that
21 information to the United States Secret Service, the Fed-
22 eral Bureau of Investigation, and the Commission for civil
23 law enforcement purposes, and shall make it available as
24 appropriate to other Federal agencies for law enforcement,
25 national security, or computer security purposes, if—

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

5 (2) the security breach involves a database,
6 networked or integrated databases, or other data
7 system containing the sensitive personally identifi-
8 able information of more than 500,000 individuals
9 nationwide;

10 (3) the security breach involves databases
11 owned by the Federal Government; or

12 (4) the security breach involves primarily sen-
13 sitive personally identifiable information of individ-
14 uals known to the business entity to be employees
15 and contractors of the Federal Government involved
16 in national security or law enforcement.

17 (b) REGULATIONS.—Not later than one year after the
18 date of enactment of this Act, the Commission shall pro-
19 mulgate regulations (in accordance with section 553 of
20 title 5, United States Code), in consultation with the At-
21 torney General and the Secretary of Homeland Security,
22 that describe what information is required to be included
23 in the notification under subsection (a). In addition, the
24 Commission shall, as necessary, promulgate regulations
25 (in accordance with section 553 of title 5, United States

1 Code), in consultation with the Attorney General, to ad-
2 just the thresholds for notification to law enforcement and
3 national security authorities under subsection (a) and to
4 facilitate the purposes of this section.

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

10 **SEC. 8. ENFORCEMENT BY THE FEDERAL TRADE COMMIS-**
11 **SION.**

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 Federal Trade
19 Commission shall enforce this Act and the regulations pro-
20 mulgated under this Act in the same manner, by the same
21 means, and with the same jurisdiction, powers, and duties
22 as though all applicable terms and provisions of the Fed-
23 eral Trade Commission Act (15 U.S.C. 41 et seq.) were
24 incorporated into and made a part of this Act, except that
25 the exceptions described in section 5(a)(2) of such Act (15

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

6 (c) FEDERAL COMMUNICATIONS COMMISSION.—In a
7 case in which enforcement under this Act involves a busi-
8 ness entity that is subject to the authority of the Federal
9 Communications Commission, in enforcement actions by
10 the Commission, the Commission shall consult with the
11 Federal Communications Commission.

12 (d) CONSUMER FINANCIAL PROTECTION BUREAU.—
13 In a case in which enforcement under this Act relates to
14 financial information or information associated with the
15 provision of a consumer financial product or service, in
16 enforcement actions by the Commission, the Commission
17 shall consult with the Consumer Financial Protection Bu-
18 reau.

19 (e) CONSULTATION WITH THE ATTORNEY GENERAL
20 REQUIRED.—The Commission shall consult with the At-
21 torney General before opening an investigation. If the At-
22 torney General determines that such an investigation
23 would impede an ongoing criminal investigation or na-
24 tional security activity, the Commission may not open such
25 investigation.

1 (f) REGULATIONS.—

2 (1) IN GENERAL.—The Commission may pro-
3 mulgate regulations, in addition to the regulations
4 promulgated pursuant to section 7(b), relating to the
5 duties of the Commission under this Act, in accord-
6 ance with section 553 of title 5, United States Code,
7 as the Commission determines to be necessary to
8 carry out this Act.

9 (2) FEDERAL COMMUNICATIONS COMMISSION.—

10 With regard to a regulation promulgated under this
11 section that relates to an entity subject to the au-
12 thority of the Federal Communications Commission,
13 the Commission may only promulgate such regula-
14 tion after consultation with the Federal Communica-
15 tions Commission.

16 (3) CONSUMER FINANCIAL PROTECTION BU-
17 REAU.—With regard to a regulation promulgated
18 under this section that relates to financial informa-
19 tion or information associated with the provision of
20 a consumer financial product or service, the Com-
21 mission may only promulgate such regulation after
22 consultation with the Consumer Financial Protection
23 Bureau.

24 **SEC. 9. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

25 (a) IN GENERAL.—

1 (1) CIVIL ACTIONS.—In any case in which the
2 attorney general of a State or an official or agency
3 of a State has reason to believe that an interest of
4 the residents of that State has been or is threatened
5 or adversely affected by an act or practice in viola-
6 tion of this Act or a regulation promulgated under
7 this Act, the State, as *parens patriae*, may bring a
8 civil action on behalf of the residents of the State in
9 an appropriate State court or an appropriate district
10 court of the United States to—

11 (A) enjoin that practice;

12 (B) enforce compliance with this Act; or

13 (C) impose civil penalties of not more than
14 \$1,000 per day per individual whose sensitive
15 personally identifiable information was, or is
16 reasonably believed to have been, accessed or
17 acquired by an unauthorized person, up to a
18 maximum of \$1,000,000 per violation, unless
19 such conduct is found to be willful or inten-
20 tional.

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

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

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

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

7 (b) AUTHORITY OF FEDERAL TRADE COMMISSION.—
8 Upon receiving notice under subsection (a)(2), the Com-
9 mission may—

10 (1) move to stay the action, pending the final
11 disposition of a pending Federal proceeding or ac-
12 tion;

13 (2) initiate an action in the appropriate United
14 States district court under section 8 and move to
15 consolidate all pending actions, including State ac-
16 tions, in such court;

17 (3) intervene in the action brought under sub-
18 section (a); or

19 (4) file petitions for appeal.

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

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

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

9 (1) conduct investigations;

10 (2) administer oaths or affirmations; or

11 (3) compel the attendance of witnesses or the
12 production of documentary and other evidence.

13 (e) VENUE; SERVICE OF PROCESS.—

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

16 (A) the district court of the United States
17 that meets applicable requirements relating to
18 venue under section 1391 of title 28, United
19 States Code; or

20 (B) another court of competent jurisdic-
21 tion.

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

25 (A) is an inhabitant; or

1 (B) may be found.

2 **SEC. 10. EFFECT ON STATE LAW.**

3 The provisions of this Act shall supersede any provi-
4 sion of the law of any State, or a political subdivision
5 thereof, relating to notification by a business entity en-
6 gaged in interstate commerce of a security breach, except
7 as provided in section 5(5).

8 **SEC. 11. REPORTING ON SECURITY BREACHES.**

9 (a) REPORT REQUIRED ON NATIONAL SECURITY AND
10 LAW ENFORCEMENT EXEMPTIONS.—Not later than 18
11 months after the date of enactment of this Act, and annu-
12 ally thereafter, the Director of the United States Secret
13 Service and the Director of the Federal Bureau of Inves-
14 tigation shall submit to the Committee on Energy and
15 Commerce of the House of Representatives and the Com-
16 mittee on Commerce, Science, and Transportation of the
17 Senate on a report on the number and nature of security
18 breaches subject to the national security and law enforce-
19 ment exemptions under section 3(a).

20 (b) REPORT REQUIRED ON SAFE HARBOR EXEMP-
21 TIONS.—Not later than 18 months after the date of enact-
22 ment of this Act, and annually thereafter, the Commission
23 shall submit to the Committee on Energy and Commerce
24 of the House of Representatives and the Committee on
25 Commerce, Science, and Transportation of the Senate a

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

5 **SEC. 12. EXCLUDED BUSINESS ENTITIES.**

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

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

14 (2) business entities to the extent that they act
15 as vendors of personal health records (as such term
16 is defined in section 13400 of such Act (42 U.S.C.
17 17921)) and third-party service providers subject to
18 section 13407 of such Act (42 U.S.C. 17937).

19 **SEC. 13. DEFINITIONS.**

20 In this Act:

21 (1) **BREACH NOTIFICATION ENTITY.**—The term
22 “breach notification entity” means the Federal Gov-
23 ernment entity designated pursuant to section 2(e).

24 (2) **BUSINESS ENTITY.**—The term “business
25 entity” means any organization, corporation, trust,

1 partnership, sole proprietorship, unincorporated as-
2 sociation, or venture, whether or not established to
3 make a profit.

4 (3) COMMISSION.—The term “Commission”
5 means the Federal Trade Commission.

6 (4) CONSUMER FINANCIAL PRODUCT OR SERV-
7 ICE.—The term “consumer financial product or
8 service” has the meaning given that term in section
9 1002 of the Dodd-Frank Wall Street Reform and
10 Consumer Protection Act (12 U.S.C. 5481).

11 (5) DATA SYSTEM COMMUNICATION INFORMA-
12 TION.—The term “data system communication in-
13 formation” means dialing, routing, addressing, or
14 signaling information that identifies the origin, di-
15 rection, destination, processing, transmission, or ter-
16 mination of each communication initiated, at-
17 tempted, or received.

18 (6) DATE AND TIME.—The term “date and
19 time” includes the date, time, and specification of
20 the time zone offset from Coordinated Universal
21 Time.

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

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

5 (9) INTERNET ADDRESS.—The term “Internet
6 address” means an Internet Protocol address as
7 specified by the Internet Protocol version 4 or 6 pro-
8 tocol, or any successor protocol or any unique num-
9 ber for a specific host on the Internet.

10 (10) SECURITY BREACH.—

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

16 (i) the unauthorized acquisition of
17 sensitive personally identifiable informa-
18 tion; or

19 (ii) access to sensitive personally iden-
20 tifiable information that is for an unau-
21 thorized purpose, or in excess of authoriza-
22 tion.

23 (B) EXCLUSION.—The term “security
24 breach” does not include any lawfully author-
25 ized investigative, protective, or intelligence ac-

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

5 (11) SENSITIVE PERSONALLY IDENTIFIABLE IN-
6 FORMATION.—The term “sensitive personally identi-
7 fiable information” means any information or com-
8 pilation of information, in electronic or digital form
9 that includes one or more of the following:

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

13 (i) Home address or telephone num-
14 ber.

15 (ii) Mother’s maiden name.

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

17 (B) A social security number (but not in-
18 cluding only the last four digits of a social secu-
19 rity number), driver’s license number, passport
20 number, or alien registration number or other
21 government-issued unique identification num-
22 ber.

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

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

5 (E) A user name or electronic mail ad-
6 dress, in combination with a password or secu-
7 rity question and answer that would permit ac-
8 cess to an online account.

9 (F) Any combination of the following data
10 elements:

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

13 (ii) A unique account identifier, in-
14 cluding a financial account number or
15 credit or debit card number, electronic
16 identification number, user name, or rout-
17 ing code.

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

21 (12) MODIFIED DEFINITION BY RULE-
22 MAKING.—The Commission may, by rule promul-
23 gated under section 553 of title 5, United States
24 Code, amend the definition of “sensitive personally
25 identifiable information” to the extent that such

1 amendment will accomplish the purposes of this Act.

2 In amending the definition, the Commission may de-

3 termine—

4 (A) that any particular combinations of in-

5 formation are sensitive personally identifiable

6 information; or

7 (B) that any particular piece of informa-

8 tion, on its own, is sensitive personally identifi-

9 able information.

10 **SEC. 14. EFFECTIVE DATE.**

11 This Act shall take effect 90 days after the date of

12 enactment of this Act.