

115TH CONGRESS
1ST SESSION

H. R. 3896

To require certain entities who collect and maintain personal information of individuals to secure such information and to provide notice to such individuals in the case of a breach of security involving such information, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 2, 2017

Ms. SCHAKOWSKY (for herself, Mr. PALLONE, Mr. BUTTERFIELD, Ms. MATSUI, Mr. TONKO, Mrs. DINGELL, Mr. WELCH, Mr. MCNERNEY, Mr. GENE GREEN of Texas, and Ms. KELLY of Illinois) introduced the following bill; which was referred to the Committee on Energy and Commerce

A BILL

To require certain entities who collect and maintain personal information of individuals to secure such information and to provide notice to such individuals in the case of a breach of security involving such information, 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 “Secure and Protect
5 Americans’ Data Act”.

1 **SEC. 2. REQUIREMENTS FOR INFORMATION SECURITY.**

2 (a) GENERAL SECURITY POLICIES, PRACTICES, AND
3 PROCEDURES.—

4 (1) REGULATIONS.—Not later than 1 year after
5 the date of enactment of this Act, the Commission
6 shall promulgate regulations under section 553 of
7 title 5, United States Code, to require each covered
8 entity to establish and implement reasonable poli-
9 cies, practices, and procedures regarding information
10 security practices for the treatment and protection
11 of personal information taking into consideration—

12 (A) the size of, and the nature, scope, and
13 complexity of the activities engaged in by such
14 covered entity;

15 (B) the sensitivity of any personal informa-
16 tion at issue;

17 (C) the current state of the art in adminis-
18 trative, technical, and physical safeguards for
19 protecting such information; and

20 (D) the cost of implementing such safe-
21 guards.

22 (2) REQUIREMENTS.—Such regulations shall
23 require the policies, practices, and procedures to in-
24 clude the following:

1 (A) A written security policy with respect
2 to the collection, use, sale, other dissemination,
3 and maintenance of such personal information.

4 (B) The identification of an officer or
5 other individual as the point of contact with re-
6 sponsibility for the management of information
7 security.

8 (C) A process for identifying and assessing
9 any reasonably foreseeable vulnerabilities in the
10 system or systems maintained by such covered
11 entity that contains such data, which shall in-
12 clude regular monitoring for a breach of secu-
13 rity of such system or systems.

14 (D) A process for taking preventive and
15 corrective action to mitigate against any
16 vulnerabilities identified in the process required
17 by subparagraph (C), which may include imple-
18 menting any changes to security practices and
19 the architecture, installation, or implementation
20 of network or operating software, and for regu-
21 larly testing or otherwise monitoring the effec-
22 tiveness of the safeguards.

23 (E) A process for determining if data is no
24 longer needed and disposing of data containing
25 personal information by shredding, permanently

1 erasing, or otherwise modifying the personal in-
2 formation contained in such data to make such
3 personal information permanently unreadable or
4 indecipherable.

5 (F) A process for overseeing persons who
6 have access to personal information, including
7 through Internet-connected devices, by—

8 (i) taking reasonable steps to select
9 and retain persons that are capable of
10 maintaining appropriate safeguards for the
11 personal information or Internet-connected
12 devices at issue; and

13 (ii) requiring all such persons to im-
14 plement and maintain such security meas-
15 ures.

16 (G) A process for employee training and
17 supervision for implementation of the policies,
18 practices, and procedures required by this sub-
19 section.

20 (H) A written plan or protocol for internal
21 and public response in the event of a breach of
22 security.

23 (3) PERIODIC ASSESSMENT AND CONSUMER
24 PRIVACY AND DATA SECURITY MODERNIZATION.—

25 Not less frequently than every 12 months, each cov-

1 ered entity shall monitor, evaluate, and adjust, as
2 appropriate, the consumer privacy and data security
3 program of such covered entity in light of any rel-
4 evant changes in—

5 (A) technology;

6 (B) internal or external threats and
7 vulnerabilities to personal information; and

8 (C) the changing business arrangements of
9 the covered entity, such as—

10 (i) mergers and acquisitions;

11 (ii) alliances and joint ventures;

12 (iii) outsourcing arrangements;

13 (iv) bankruptcy; and

14 (v) changes to personal information
15 systems.

16 (4) SUBMISSION OF POLICIES TO THE FTC.—

17 The regulations promulgated under this subsection
18 shall require each covered entity to submit its secu-
19 rity policies to the Commission in conjunction with
20 a notification of a breach of security under section
21 3 or upon request of the Commission.

22 (5) TREATMENT OF ENTITIES GOVERNED BY

23 OTHER FEDERAL LAW.—Any covered entity who is
24 in compliance with any other Federal law that re-
25 quires such covered entity to maintain standards

1 and safeguards for information security and protec-
2 tion of personal information that, taken as a whole
3 and as the Commission shall determine in the rule-
4 making required under this subsection, requires cov-
5 ered entities to provide protections substantially
6 similar to, or greater than, those required under this
7 subsection, shall be deemed to be in compliance with
8 this subsection.

9 (b) SPECIAL REQUIREMENTS FOR INFORMATION
10 BROKERS.—

11 (1) POST-BREACH AUDIT.—For any information
12 broker required to provide notification under section
13 3, the Commission may require the information
14 broker to conduct independent audits of such prac-
15 tices (by an independent auditor who has not au-
16 dited such information broker's security practices
17 during the preceding 5 years).

18 (2) ACCURACY OF AND INDIVIDUAL ACCESS TO
19 PERSONAL INFORMATION.—

20 (A) ACCURACY.—

21 (i) IN GENERAL.—Each information
22 broker shall establish reasonable proce-
23 dures to assure the maximum possible ac-
24 curacy of the personal information the in-
25 formation broker collects, assembles, or

1 maintains, and any other information the
2 information broker collects, assembles, or
3 maintains that specifically identifies an in-
4 dividual, other than information which
5 merely identifies an individual's name or
6 address.

7 (ii) LIMITED EXCEPTION FOR FRAUD
8 DATABASES.—The requirement in clause
9 (i) shall not prevent the collection or main-
10 tenance of information that may be inac-
11 curate with respect to a particular indi-
12 vidual when that information is being col-
13 lected or maintained solely—

14 (I) for the purpose of indicating
15 whether there may be a discrepancy
16 or irregularity in the personal infor-
17 mation that is associated with an indi-
18 vidual; and

19 (II) to help identify, or authen-
20 ticate the identity of, an individual, or
21 to protect against or investigate fraud
22 or other unlawful conduct.

23 (B) CONSUMER ACCESS TO INFORMA-
24 TION.—Each information broker shall—

1 (i) provide to each individual whose
2 personal information the information
3 broker maintains, at the individual's re-
4 quest at least once per year and at no cost
5 to the individual, and after verifying the
6 identity of such individual, a means for the
7 individual to review any personal informa-
8 tion regarding such individual maintained
9 by the information broker and any other
10 information maintained by the information
11 broker that specifically identifies such indi-
12 vidual, other than information which mere-
13 ly identifies an individual's name or ad-
14 dress; and

15 (ii) place a conspicuous notice on the
16 Internet website of the information broker
17 (if the information broker maintains such
18 a website) notifying consumers that the en-
19 tity is an information broker using specific
20 language that the Commission shall deter-
21 mine in the rulemaking required under this
22 subsection and instructing individuals how
23 to request access to the information re-
24 quired to be provided under clause (i), and,
25 as applicable, how to express a preference

1 with respect to the use of personal infor-
2 mation for marketing purposes under sub-
3 paragraph (D).

4 (C) DISPUTED INFORMATION.—Whenever
5 an individual whose information the information
6 broker maintains makes a written request dis-
7 puting the accuracy of any such information,
8 the information broker, after verifying the iden-
9 tity of the individual making such request and
10 unless there are reasonable grounds to believe
11 such request is frivolous or irrelevant, shall—

12 (i) correct any inaccuracy; or

13 (ii) in the case of information that
14 is—

15 (I) public record information, in-
16 form the individual of the source of
17 the information, and, if reasonably
18 available, where a request for correc-
19 tion may be directed and, if the indi-
20 vidual provides proof that the public
21 record has been corrected or that the
22 information broker was reporting the
23 information incorrectly, correct the in-
24 accuracy in the information broker's
25 records; or

1 (II) nonpublic information, note
2 the information that is disputed, in-
3 cluding the individual's statement dis-
4 puting such information, and take
5 reasonable steps to independently
6 verify such information under the pro-
7 cedures outlined in subparagraph (A)
8 if such information can be independ-
9 ently verified.

10 (D) ALTERNATIVE PROCEDURE FOR CER-
11 TAIN MARKETING INFORMATION.—In accord-
12 ance with regulations issued under subpara-
13 graph (F), an information broker that main-
14 tains any information described in subpara-
15 graph (A) which is used, shared, or sold by
16 such information broker for marketing pur-
17 poses, may, in lieu of complying with the access
18 and dispute requirements set forth in subpara-
19 graphs (B) and (C), provide each individual
20 whose information the information broker main-
21 tains with a reasonable means of expressing a
22 preference not to have his or her information
23 used for such purposes. If the individual ex-
24 presses such a preference, the information

1 broker may not use, share, or sell the individ-
2 ual's information for marketing purposes.

3 (E) LIMITATIONS.—An information broker
4 may limit the access to information required
5 under subparagraph (B)(i), is not required to
6 provide notice to individuals as required under
7 subparagraph (B)(ii), and is not required to
8 comply with a disputed information request
9 under subparagraph (C) in the following cir-
10 cumstances:

11 (i) If access of the individual to the
12 information is limited by law or legally rec-
13 ognized privilege.

14 (ii) If the information is used for a le-
15 gitimate governmental or fraud prevention
16 purpose that would be compromised by
17 such access.

18 (iii) If the information consists of a
19 published media record, unless that record
20 has been included in a report about an in-
21 dividual shared with a third party.

22 (F) RULEMAKING.—Not later than 1 year
23 after the date of enactment of this Act, the
24 Commission shall promulgate regulations under
25 section 553 of title 5, United States Code, to

1 carry out this paragraph and to facilitate the
2 purposes of this Act. In addition, the Commis-
3 sion shall issue regulations, as necessary, under
4 section 553 of title 5, United States Code, on
5 the scope of the application of the limitations in
6 subparagraph (E), including any additional cir-
7 cumstances in which an information broker may
8 limit access to information under such subpara-
9 graph that the Commission determines to be
10 appropriate.

11 (G) FCRA REGULATED PERSONS.—Any
12 information broker who is engaged in activities
13 subject to the Fair Credit Reporting Act and
14 who is in compliance with sections 609, 610,
15 and 611 of such Act (15 U.S.C. 1681g; 1681h;
16 1681i) with respect to information subject to
17 such Act, shall be deemed to be in compliance
18 with this paragraph with respect to such infor-
19 mation.

20 (3) REQUIREMENT OF AUDIT LOG OF ACCESSED
21 AND TRANSMITTED INFORMATION.—Not later than
22 1 year after the date of enactment of this Act, the
23 Commission shall promulgate regulations under sec-
24 tion 553 of title 5, United States Code, to require
25 information brokers to establish measures which fa-

1 facilitate the auditing or retracing of any internal or
2 external access to, or transmissions of, any data con-
3 taining personal information collected, assembled, or
4 maintained by such information broker.

5 (4) PROHIBITION ON PRETEXTING BY INFOR-
6 MATION BROKERS.—

7 (A) PROHIBITION ON OBTAINING PER-
8 SONAL INFORMATION BY FALSE PRETENSES.—

9 It shall be unlawful for an information broker
10 to obtain or attempt to obtain, or cause to be
11 disclosed or attempt to cause to be disclosed to
12 any person, personal information or any other
13 information relating to any person by—

14 (i) making a false, fictitious, or fraud-
15 ulent statement or representation to any
16 person; or

17 (ii) providing any document or other
18 information to any person that the infor-
19 mation broker knows or should know to be
20 forged, counterfeit, lost, stolen, or fraudu-
21 lently obtained, or to contain a false, ficti-
22 tious, or fraudulent statement or represen-
23 tation.

24 (B) PROHIBITION ON SOLICITATION TO
25 OBTAIN PERSONAL INFORMATION UNDER FALSE

1 PRETENSES.—It shall be unlawful for an infor-
2 mation broker to request a person to obtain
3 personal information or any other information
4 relating to any other person, if the information
5 broker knew or should have known that the per-
6 son to whom such a request is made will obtain
7 or attempt to obtain such information in the
8 manner described in subparagraph (A).

9 **SEC. 3. NOTIFICATION OF INFORMATION SECURITY**
10 **BREACH.**

11 (a) INDIVIDUAL NOTIFICATION.—

12 (1) IN GENERAL.—Each covered entity shall,
13 following the discovery of a breach of security, notify
14 each individual who is a citizen or resident of the
15 United States whose personal information was, or is
16 reasonably believed to have been, acquired or
17 accessed by an unauthorized person, or used for an
18 unauthorized purpose.

19 (2) TIMELINESS OF NOTIFICATION.—

20 (A) IN GENERAL.—Unless subject to a
21 delay authorized under subparagraph (B), a no-
22 tification required under paragraph (1) shall be
23 made as expeditiously as practicable and with-
24 out unreasonable delay, but not later than 30

1 days following the discovery of a breach of secu-
2 rity.

3 (B) DELAY OF NOTIFICATION AUTHORIZED
4 FOR LAW ENFORCEMENT OR NATIONAL SECUR-
5 RITY PURPOSES.—

6 (i) LAW ENFORCEMENT.—If a Fed-
7 eral or State law enforcement agency, in-
8 cluding an attorney general of a State, de-
9 termines that the notification required
10 under this section would impede a civil or
11 criminal investigation, such notification
12 shall be delayed upon the written request
13 of the law enforcement agency for 30 days
14 or such lesser period of time which the law
15 enforcement agency determines is reason-
16 ably necessary and requests in writing.
17 Such a law enforcement agency may, by a
18 subsequent written request, revoke such
19 delay or extend the period of time set forth
20 in the original request made under this
21 clause if further delay is necessary.

22 (ii) NATIONAL SECURITY.—If a Fed-
23 eral national security agency or homeland
24 security agency determines that the notifi-
25 cation required under this section would

1 threaten national or homeland security,
2 such notification may be delayed for a pe-
3 riod of time of up to 60 days which the na-
4 tional security agency or homeland security
5 agency determines is reasonably necessary
6 and requests in writing. A Federal national
7 security agency or homeland security agen-
8 cy may revoke such delay or extend the pe-
9 riod of time set forth in the original re-
10 quest made under this clause by a subse-
11 quent written request if further delay is
12 necessary.

13 (iii) LIMITATION ON DELAY OR EX-
14 TENSION.—Any delay or extension of noti-
15 fication permitted under this subparagraph
16 may not exceed a total time period of one
17 year.

18 (b) COORDINATION OF NOTIFICATION WITH CON-
19 SUMER REPORTING AGENCIES.—If a covered entity is re-
20 quired to provide notification to more than 5,000 individ-
21 uals under subsection (a)(1), the covered entity shall also
22 notify the major consumer reporting agencies that compile
23 and maintain files on consumers on a nationwide basis,
24 of the timing and distribution of the notifications, except
25 for a case in which the only information that is the subject

1 of the breach of security is the individual's first name or
2 initial and last name, address, or phone number, in com-
3 bination with a credit or debit card number and any re-
4 quired security code. Such notification shall be given to
5 the consumer reporting agencies without unreasonable
6 delay and, if such notification will not delay notification
7 to the affected individuals, prior to the distribution of noti-
8 fications to the affected individuals.

9 (c) METHOD AND CONTENT OF NOTIFICATION.—

10 (1) GENERAL NOTIFICATION.—A covered entity
11 required to provide notification to individuals under
12 subsection (a)(1) shall be in compliance with such
13 requirement if the covered entity provides con-
14 spicuous and clearly identified notification by one of
15 the following methods (provided the selected method
16 can reasonably be expected to reach the intended in-
17 dividual):

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

21 (B) Notification by email or other elec-
22 tronic means, if—

23 (i) the covered entity's primary meth-
24 od of communication with the individual is
25 by email or such other electronic means; or

1 (ii) the individual has consented to re-
2 ceive such notification and the notification
3 is provided in a manner that is consistent
4 with the provisions permitting electronic
5 transmission of notifications under section
6 101 of the Electronic Signatures in Global
7 and National Commerce Act (15 U.S.C.
8 7001).

9 (2) WEBSITE NOTIFICATION.—The covered en-
10 tity shall also provide conspicuous notification on the
11 Internet website of the covered entity (if such cov-
12 ered entity maintains such a website) for a period of
13 not less than 90 days.

14 (3) MEDIA NOTIFICATION.—If the number of
15 residents of a State whose personal information was,
16 or is reasonably believed to have been, acquired or
17 accessed by an unauthorized person, or used for an
18 unauthorized purpose, exceeds 5,000, the covered
19 entity shall also provide notification in print and to
20 broadcast media, including major media in metro-
21 politan and rural areas where the individuals whose
22 personal information was, or is reasonably believed
23 to have been, acquired or accessed by an unauthor-
24 ized person, or used for an unauthorized purpose,
25 reside.

1 (4) CONTENT OF NOTIFICATION.—

2 (A) IN GENERAL.—Regardless of the
3 method by which notification is provided to an
4 individual under paragraphs (1), (2), and (3),
5 such notification shall include—

6 (i) a description of the personal infor-
7 mation that was, or is reasonably believed
8 to have been, acquired or accessed by an
9 unauthorized person, or used for an unau-
10 thorized purpose;

11 (ii) a general description of the inci-
12 dent and the date or estimated date of the
13 breach of security and the date range dur-
14 ing which the personal information was
15 compromised;

16 (iii) the acts the covered entity, or the
17 agent of the covered entity, has taken to
18 protect personal information from further
19 breach of security;

20 (iv) a telephone number, website, and
21 email address that the individual may use,
22 at no cost to such individual, to contact
23 the covered entity, or agent of the covered
24 entity, to inquire about the breach of secu-

1 rity or the information the covered entity
2 maintained about that individual;

3 (v) in the case of an individual that is
4 entitled to receive services under sub-
5 section (e), notification that the individual
6 is entitled to receive such services;

7 (vi) the toll-free contact telephone
8 numbers and addresses for the major con-
9 sumer reporting agencies; and

10 (vii) a toll-free telephone number and
11 Internet website address for the Commis-
12 sion whereby the individual may obtain in-
13 formation regarding identity theft.

14 (B) DIRECT BUSINESS RELATIONSHIP.—

15 The notification required under subsection (a)
16 shall identify the covered entity that has a di-
17 rect business relationship with the individual, if
18 applicable, as well as the entity that experi-
19 enced the breach of security.

20 (5) REGULATIONS FOR SUBSTITUTE NOTIFICA-
21 TION.—Not later than 1 year after the date of en-
22 actment of this Act, the Commission shall, by regu-
23 lation under section 553 of title 5, United States
24 Code—

1 (A) establish criteria for determining cir-
2 cumstances under which substitute notification
3 may be provided in lieu of direct notification re-
4 quired by paragraph (1), including criteria for
5 determining if notification under paragraph (1)
6 is not feasible due to excessive costs to the cov-
7 ered entity required to provide such notification
8 relative to the resources of such covered entity;
9 and

10 (B) establish the form and content of sub-
11 stitute notification.

12 (d) NOTIFICATION FOR LAW ENFORCEMENT AND
13 OTHER PURPOSES.—A covered entity shall, as expedi-
14 tiously as practicable and without unreasonable delay, but
15 not later than 5 days following the discovery of a breach
16 of security, provide notification of the breach to—

17 (1) the Commission;

18 (2) the Federal Bureau of Investigation;

19 (3) the Secret Service;

20 (4) for common carriers, the Federal Commu-
21 nications Commission;

22 (5) for entities that provide a consumer finan-
23 cial product or service (as defined in section 1002 of
24 the Consumer Financial Protection Act of 2010 (12

1 U.S.C. 5481)), the Bureau of Consumer Financial
2 Protection; and

3 (6) the attorney general of each State in which
4 the personal information of a resident or residents
5 of the State was, or is reasonably believed to have
6 been, acquired or accessed by an unauthorized per-
7 son, or used for an unauthorized purpose.

8 (e) OTHER OBLIGATIONS FOLLOWING BREACH.—

9 (1) IN GENERAL.—A covered entity required to
10 provide notification under subsection (a) shall, upon
11 request of an individual whose personal information
12 was included in the breach of security, provide or ar-
13 range for the provision of, to each such individual
14 and at no cost to such individual—

15 (A) at the option of such individual, ei-
16 ther—

17 (i) consumer credit reports from all of
18 the major consumer reporting agencies be-
19 ginning not later than 60 days following
20 the individual's request and continuing on
21 a quarterly basis for a period of not less
22 than 10 years thereafter; or

23 (ii) a credit monitoring or other serv-
24 ice that—

1 (I) enables consumers to detect
2 the misuse of their personal informa-
3 tion, beginning not later than 60 days
4 following the individual's request and
5 continuing for a period of not less
6 than 10 years thereafter; and

7 (II) includes monitoring of the
8 individual's credit file at all of the
9 major consumer reporting agencies;
10 and

11 (B) a service that enables consumers to
12 control access to their personal information and
13 credit reports, beginning not later than 60 days
14 following the individual's request and con-
15 tinuing for a period of not less than 10 years
16 thereafter.

17 (2) LIMITATION.—This subsection shall not
18 apply if the only personal information which has
19 been the subject of the breach of security is the indi-
20 vidual's first name or initial and last name, address,
21 or phone number, in combination with a credit or
22 debit card number and any required security code.

23 (f) EXEMPTION.—

24 (1) GENERAL EXEMPTION.—A covered entity
25 shall be exempt from the requirements under this

1 section if the data containing personal information
2 that was, or is reasonably believed to have been, ac-
3 quired or accessed by an unauthorized person, or
4 used for an unauthorized purpose, is unusable,
5 unreadable, or indecipherable because of security
6 technologies or methodologies generally accepted by
7 experts in the field of information security at the
8 time the breach of security occurred. This exemption
9 does not apply with regard to the use of encryption
10 technology generally accepted by experts in the field
11 of information security at the time the breach of se-
12 curity occurred if any cryptographic keys necessary
13 to enable decryption of such data are also accessed
14 or acquired without authorization.

15 (2) FTC GUIDANCE.—Not later than 1 year
16 after the date of enactment of this Act, the Commis-
17 sion shall issue guidance regarding the application of
18 the exemption in paragraph (1).

19 (g) WEBSITE NOTIFICATION OF FEDERAL TRADE
20 COMMISSION.—If the Commission, upon receiving notifi-
21 cation of any breach of security that is reported to the
22 Commission under subsection (d)(1), finds that notifica-
23 tion of such a breach of security via the Commission's
24 Internet website would be in the public interest, the Com-

1 mission shall place such a notification in a clear and con-
2 spicuous location on its Internet website.

3 (h) WEBSITE NOTIFICATION OF STATE ATTORNEYS
4 GENERAL.—If a State attorney general, upon receiving
5 notification of any breach of security that is reported to
6 such State attorney general under subsection (d)(6), finds
7 that notification of such breach of security via the State
8 attorney general’s Internet website would be in the public
9 interest or for the protection of consumers, the State at-
10 torney general may place such a notification in a clear and
11 conspicuous location on its Internet website.

12 (i) FTC STUDY ON NOTIFICATION IN LANGUAGES IN
13 ADDITION TO ENGLISH.—Not later than 1 year after the
14 date of enactment of this Act, the Commission shall con-
15 duct a study on the practicality and cost effectiveness of
16 requiring the notification required by subsection (c)(1) to
17 be provided in a language in addition to English to individ-
18 uals known to speak only such other language.

19 (j) EDUCATION AND OUTREACH FOR SMALL BUSI-
20 NESSES.—The Commission shall conduct education and
21 outreach for small business concerns on data security
22 practices and how to prevent hacking and other unauthor-
23 ized access to, acquisition of, or use of data maintained
24 by such small business concerns.

1 (k) WEBSITE ON DATA SECURITY BEST PRAC-
2 TICES.—The Commission shall maintain an Internet
3 website containing nonbinding best practices for busi-
4 nesses regarding data security and how to prevent hacking
5 and other unauthorized access to, acquisition of, or use
6 of data maintained by such businesses.

7 (l) GENERAL RULEMAKING AUTHORITY.—

8 (1) IN GENERAL.—The Commission may pro-
9 mulgate regulations necessary under section 553 of
10 title 5, United States Code, to effectively enforce the
11 requirements of this section.

12 (2) LIMITATION.—In promulgating rules under
13 this Act, the Commission shall not require the de-
14 ployment or use of any specific products or tech-
15 nologies, including any specific computer software or
16 hardware.

17 (m) TREATMENT OF PERSONS GOVERNED BY OTHER
18 LAW.—A covered entity who is in compliance with any
19 other Federal law that requires such covered entity to pro-
20 vide notification to individuals following a breach of secu-
21 rity in at least the same or substantially similar cir-
22 cumstances and in at the least same or substantially simi-
23 lar manner as required to be provided under this Act,
24 taken as a whole and as determined by the Commission
25 in the rulemaking required under this section, shall be

1 deemed to be in compliance with this section with respect
2 to activities and information covered under such Federal
3 law.

4 **SEC. 4. APPLICATION AND ENFORCEMENT.**

5 (a) ENFORCEMENT BY THE FEDERAL TRADE COM-
6 MISSION.—

7 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
8 TICES.—A violation of section 2 or 3 shall be treated
9 as an unfair and deceptive act or practice in viola-
10 tion of a regulation under section 18(a)(1)(B) of the
11 Federal Trade Commission Act (15 U.S.C.
12 57a(a)(1)(B)) regarding unfair or deceptive acts or
13 practices and shall be subject to enforcement by the
14 Commission under that Act with respect to any cov-
15 ered entity. All of the functions and powers of the
16 Commission under the Federal Trade Commission
17 Act are available to the Commission to enforce com-
18 pliance by any person with the requirements imposed
19 under this Act, irrespective of whether that person
20 is engaged in commerce or meets any other jurisdic-
21 tional tests under the Federal Trade Commission
22 Act.

23 (2) COORDINATION WITH FEDERAL COMMU-
24 NICATIONS COMMISSION.—Where enforcement re-
25 lates to entities subject to the authority of the Fed-

1 eral Communications Commission, enforcement ac-
2 tions by the Commission will be coordinated with the
3 Federal Communications Commission.

4 (3) COORDINATION WITH BUREAU OF CON-
5 SUMER FINANCIAL PROTECTION.—Where enforce-
6 ment relates to entities that provide a consumer fi-
7 nancial product or service (as defined in section
8 1002 of the Consumer Financial Protection Act of
9 2010 (12 U.S.C. 5481)), enforcement actions by the
10 Commission will be coordinated with the Bureau of
11 Consumer Financial Protection.

12 (b) ENFORCEMENT BY STATE ATTORNEYS GEN-
13 ERAL.—

14 (1) IN GENERAL.—If the chief law enforcement
15 officer of a State, or an official or agency designated
16 by a State, has reason to believe that any covered
17 entity has violated or is violating section 2 or 3 of
18 this Act, the attorney general, official, or agency of
19 the State, in addition to any authority it may have
20 to bring an action in State court under its consumer
21 protection law, may bring a civil action in any ap-
22 propriate United States district court or in any
23 other court of competent jurisdiction, including a
24 State court, to—

1 (A) enjoin further such violation by the de-
2 fendant;

3 (B) enforce compliance with such section;

4 (C) obtain civil penalties; and

5 (D) obtain damages, restitution, or other
6 compensation on behalf of residents of the
7 State.

8 (2) NOTICE AND INTERVENTION BY THE
9 FTC.—The attorney general of a State shall provide
10 prior written notice of any action under paragraph
11 (1) to the Commission and provide the Commission
12 with a copy of the complaint in the action, except in
13 any case in which such prior notice is not feasible,
14 in which case the attorney general shall serve such
15 notice immediately upon instituting such action. The
16 Commission shall have the right—

17 (A) to intervene in the action;

18 (B) upon so intervening, to be heard on all
19 matters arising therein; and

20 (C) to file petitions for appeal.

21 (3) LIMITATION ON STATE ACTION WHILE FED-
22 ERAL ACTION IS PENDING.—If the Commission has
23 instituted a civil action for violation of this Act, no
24 State attorney general, or official or agency of a
25 State, may bring an action under this subsection

1 during the pendency of that action against any de-
2 fendant named in the complaint of the Commission
3 for any violation of this Act alleged in the complaint.

4 (4) RELATIONSHIP WITH STATE-LAW CLAIMS.—

5 If the attorney general of a State has authority to
6 bring an action under State law directed at acts or
7 practices that also violate this Act, the attorney gen-
8 eral may assert the State-law claim and a claim
9 under this Act in the same civil action.

10 **SEC. 5. DEFINITIONS.**

11 In this Act:

12 (1) BREACH OF SECURITY.—The term “breach
13 of security” means unauthorized access to, acquisi-
14 tion of, or use of data containing personal informa-
15 tion.

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

18 (3) CONSUMER REPORTING AGENCY.—The term
19 “consumer reporting agency” has the meaning given
20 that term in section 603 of the Fair Credit Report-
21 ing Act (15 U.S.C. 1681a).

22 (4) COVERED ENTITY.—The term “covered en-
23 tity” means—

24 (A) any organization, corporation, trust,
25 partnership, sole proprietorship, unincorporated

1 association, or venture over which the Commis-
2 sion has authority pursuant to section 5(a)(2)
3 of the Federal Trade Commission Act (15
4 U.S.C. 45(a)(2));

5 (B) notwithstanding section 5(a)(2) of the
6 Federal Trade Commission Act (15 U.S.C.
7 45(a)(2)), common carriers subject to the Com-
8 munications Act of 1934 (47 U.S.C. 151 et
9 seq.); and

10 (C) notwithstanding sections 4 and 5(a)(2)
11 of the Federal Trade Commission Act (15
12 U.S.C. 44 and 45(a)(2)), any nonprofit organi-
13 zation, including any organization described in
14 section 501(c) of the Internal Revenue Code of
15 1986 that is exempt from taxation under sec-
16 tion 501(a) of the Internal Revenue Code of
17 1986.

18 (5) INFORMATION BROKER.—The term “infor-
19 mation broker”—

20 (A) means a commercial entity whose busi-
21 ness is to collect, assemble, or maintain per-
22 sonal information concerning individuals who
23 are not current or former customers of such en-
24 tity in order to sell such information or provide
25 access to such information to any nonaffiliated

1 third party in exchange for consideration,
2 whether such collection, assembly, or mainte-
3 nance of personal information is performed by
4 the information broker directly, or by contract
5 or subcontract with any other entity; and

6 (B) does not include a commercial entity to
7 the extent that such entity processes informa-
8 tion collected by and received from a non-
9 affiliated third party concerning individuals who
10 are current or former customers or employees
11 of the third party to enable the third party to
12 provide benefits for the employees or directly
13 transact business with the customers.

14 (6) PERSONAL INFORMATION.—

15 (A) DEFINITION.—The term “personal in-
16 formation” means any information or compila-
17 tion of information that includes any of the fol-
18 lowing:

19 (i) An individual’s first name or initial
20 and last name in combination with any 2
21 or more of the following data elements for
22 that individual:

23 (I) Home address or telephone
24 number.

25 (II) Mother’s maiden name.

1 (III) Month, day, and year of
2 birth.

3 (IV) User name or electronic
4 mail address.

5 (ii) Driver's license number, passport
6 number, military identification number,
7 alien registration number, or other similar
8 number issued on a government document
9 used to verify identity.

10 (iii) Unique account identifier, includ-
11 ing a financial account number, or credit
12 or debit card number, electronic identifica-
13 tion number, user name, or routing code.

14 (iv) Partial or complete Social Secu-
15 rity number.

16 (v) Unique biometric or genetic data
17 such as a faceprint, fingerprint, voice
18 print, a retina or iris image, or any other
19 unique physical representations.

20 (vi) Information that could be used to
21 access an individual's account, such as
22 user name and password or email address
23 and password.

24 (vii) Any security code, access code, or
25 password, or source code that could be

1 used to generate such codes or passwords,
2 in combination with either of the following
3 data elements:

4 (I) An individual's first and last
5 name or first initial and last name.

6 (II) A unique account identifier,
7 including a financial account number
8 or credit or debit card number, elec-
9 tronic identification number, user
10 name, or routing code.

11 (viii) Information generated or derived
12 from the operation or use of an electronic
13 communications device that is sufficient to
14 identify the street name and name of the
15 city or town in which the device is located.

16 (ix) Any information regarding an in-
17 dividual's medical history, mental or phys-
18 ical condition, medical treatment or diag-
19 nosis by a health care professional, or the
20 provision of health care to the individual,
21 including health information provided to a
22 website or mobile application.

23 (x) A health insurance policy number
24 or subscriber identification number and
25 any unique identifier used by a health in-

1 surer to identify the individual, or any in-
2 formation in an individual's health insur-
3 ance application and claims history, includ-
4 ing any appeals records.

5 (xi) Digitized or other electronic sig-
6 nature.

7 (xii) Nonpublic communications or
8 other user-created content such as emails,
9 photographs, or videos.

10 (xiii) Any record or information con-
11 cerning payroll, income, financial accounts,
12 mortgages, loans, lines of credit, utility
13 bills, accumulated purchases, or any other
14 information regarding financial assets, ob-
15 ligations, or spending habits.

16 (xiv) Any additional element the Com-
17 mission defines as personal information.

18 (B) MODIFIED DEFINITION BY RULE-
19 MAKING.—The Commission may, by rule pro-
20 mulgated under section 553 of title 5, United
21 States Code, modify the definition of “personal
22 information” under subparagraph (A).

23 (7) STATE.—The term “State” means each of
24 the several States, the District of Columbia, the
25 Commonwealth of Puerto Rico, Guam, American

1 Samoa, the United States Virgin Islands, the Com-
2 monwealth of the Northern Mariana Islands, any
3 other territory or possession of the United States,
4 and each federally recognized Indian tribe.

5 **SEC. 6. EFFECT ON OTHER LAWS.**

6 (a) **PREEMPTION OF STATE DATA SECURITY AND**
7 **BREACH NOTIFICATION LAWS.**—No State or political sub-
8 division thereof shall have any authority to establish or
9 continue in effect any standard or requirement that is not
10 identical to the standards and requirements established
11 under this Act for—

12 (1) information security practices for the treat-
13 ment and protection of the personal information de-
14 fined in section 5(6)(A), or as subsequently amended
15 by the Commission under section 5(6)(B), by cov-
16 ered entities, as defined in section 5(4); or

17 (2) notification to individuals of a breach of se-
18 curity of the personal information defined in section
19 5(6)(A), or as subsequently amended by the Com-
20 mission under section 5(6)(B), by covered entities,
21 as defined in section 5(4).

22 (b) **EFFECT ON STATE LAW.**—In the case of a provi-
23 sion of the law of a State that is superseded by subsection
24 (a), this Act may be enforced in the same manner and
25 to the same extent as the State law could have been en-

1 forced under State law had the provision of the law of
2 the State not been superseded.

3 (c) EFFECT ON OTHER STATE LAWS.—Except as
4 provided in subsection (a), nothing in this Act shall be
5 construed to—

6 (1) preempt or limit any provision of any law,
7 rule, regulation, requirement, standard, or other pro-
8 vision having the force and effect of law of any
9 State, including any State consumer protection law,
10 any State law relating to acts of fraud or deception,
11 and any State trespass, contract, or tort law;

12 (2) preempt or limit any provision of any law,
13 rule, regulation, requirement, standard, or other pro-
14 vision having the force and effect of law of any State
15 regarding post-data breach services, including secu-
16 rity or credit freezes, credit monitoring, identity
17 theft monitoring, and identity theft services;

18 (3) prevent or limit the attorney general of a
19 State from exercising the powers conferred upon the
20 attorney general by the laws of the State, including
21 conducting investigations, administering oaths or af-
22 firmations, or compelling the attendance of witnesses
23 or the production of documentary and other evi-
24 dence; or

1 (4) preempt or limit any provision of any law,
2 rule, regulation, requirement, standard, or other pro-
3 vision having the force and effect of law of any State
4 with respect to any person that is not a covered enti-
5 ty, as defined in section 5(4), or any information
6 that is not personal information, as defined in sec-
7 tion 5(6)(A), or as subsequently amended by the
8 Commission under section 5(6)(B).

9 (d) PRESERVATION OF AUTHORITY.—

10 (1) FEDERAL TRADE COMMISSION.—Nothing in
11 this Act may be construed in any way to limit the
12 Commission’s authority under any other provision of
13 law.

14 (2) FEDERAL COMMUNICATIONS COMMISSION.—
15 Nothing in this Act may be construed in any way to
16 limit or affect the Federal Communications Commis-
17 sion’s authority under any other provision of law.

18 (3) BUREAU OF CONSUMER FINANCIAL PROTEC-
19 TION.—Nothing in this Act may be construed in any
20 way to limit or affect the authority of the Bureau
21 of Consumer Financial Protection under any other
22 provision of law.

1 **SEC. 7. EFFECTIVE DATE.**

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

○