

115TH CONGRESS  
2D SESSION

# H. R. 5388

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

MARCH 22, 2018

Mr. RUSH 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 “Data Accountability  
5       and Trust Act”.

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

2 (a) GENERAL SECURITY POLICIES AND PROCE-  
3 DURES.—

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 policies and proce-  
9 dures regarding information security practices for  
10 the treatment and protection of personal information  
11 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 and procedures to include the  
24 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 vulner-  
16 abilities identified in the process required by  
17 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' key controls, sys-  
23 tems, and procedures.

24 (E) A process for disposing of data con-  
25 taining personal information by shredding, per-

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

5           (F) A process for overseeing persons to  
6           whom personal information is disclosed, or who  
7           have access to 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           (3) TREATMENT OF ENTITIES GOVERNED BY  
17           OTHER FEDERAL LAW.—Any covered entity who is  
18           in compliance with any other Federal law that re-  
19           quires such covered entity to maintain standards  
20           and safeguards for information security and protec-  
21           tion of personal information that, taken as a whole  
22           and as the Commission shall determine in the rule-  
23           making required under this subsection, provide pro-  
24           tections substantially similar to, or greater than,

1       those required under this subsection, shall be  
2       deemed to be in compliance with this subsection.

3       (b) SPECIAL REQUIREMENTS FOR INFORMATION  
4       BROKERS.—

5               (1) SUBMISSION OF POLICIES TO THE FTC.—

6       The regulations promulgated under subsection (a)  
7       shall require each information broker to submit its  
8       security policies to the Commission in conjunction  
9       with a notification of a breach of security under sec-  
10      tion 3 or upon request of the Commission.

11              (2) POST-BREACH AUDIT.—For any information  
12      broker required to provide notification under section  
13      3, the Commission may conduct audits of the infor-  
14      mation security practices of such information broker,  
15      or require the information broker to conduct inde-  
16      pendent audits of such practices (by an independent  
17      auditor who has not audited such information bro-  
18      ker's security practices during the preceding 5  
19      years).

20              (3) ACCURACY OF AND INDIVIDUAL ACCESS TO  
21      PERSONAL INFORMATION.—

22                      (A) ACCURACY.—

23                              (i) IN GENERAL.—Each information  
24                      broker shall establish reasonable proce-  
25                      dures to assure the maximum possible ac-

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

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

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

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

1 (B) CONSUMER ACCESS TO INFORMA-  
2 TION.—Each information broker shall—

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

17 (ii) place a conspicuous notice on the  
18 Internet website of the information broker  
19 (if the information broker maintains such  
20 a website) instructing individuals how to  
21 request access to the information required  
22 to be provided under clause (i), and, as ap-  
23 plicable, how to express a preference with  
24 respect to the use of personal information

1           for marketing purposes under subpara-  
2           graph (D).

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

11                   (i) correct any inaccuracy; or

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

14                   (I) public record information, in-  
15                   form the individual of the source of  
16                   the information, and, if reasonably  
17                   available, where a request for correc-  
18                   tion may be directed and, if the indi-  
19                   vidual provides proof that the public  
20                   record has been corrected or that the  
21                   information broker was reporting the  
22                   information incorrectly, correct the in-  
23                   accuracy in the information broker’s  
24                   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) and is not required  
6 to provide notice to individuals as required  
7 under subparagraph (B)(ii) in the following cir-  
8 cumstances:

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

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

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

20 (F) RULEMAKING.—Not later than 1 year  
21 after the date of enactment of this Act, the  
22 Commission shall promulgate regulations under  
23 section 553 of title 5, United States Code, to  
24 carry out this paragraph and to facilitate the  
25 purposes of this Act. In addition, the Commis-

1           sion shall issue regulations, as necessary, under  
2           section 553 of title 5, United States Code, on  
3           the scope of the application of the limitations in  
4           subparagraph (E), including any additional cir-  
5           cumstances in which an information broker may  
6           limit access to information under such clause  
7           that the Commission determines to be appro-  
8           priate.

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

18          (4) REQUIREMENT OF AUDIT LOG OF ACCESSED  
19          AND TRANSMITTED INFORMATION.—Not later than  
20          1 year after the date of enactment of this Act, the  
21          Commission shall promulgate regulations under sec-  
22          tion 553 of title 5, United States Code, to require  
23          information brokers to establish measures which fa-  
24          cilitate the auditing or retracing of any internal or  
25          external access to, or transmissions of, any data con-

1       taining personal information collected, assembled, or  
2       maintained by such information broker.

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

5               (A) PROHIBITION ON OBTAINING PER-  
6       SONAL INFORMATION BY FALSE PRETENSES.—

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

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

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

22              (B) PROHIBITION ON SOLICITATION TO  
23      OBTAIN PERSONAL INFORMATION UNDER FALSE  
24      PRETENSES.—It shall be unlawful for an infor-  
25      mation broker to request a person to obtain

1           personal information or any other information  
2           relating to any other person, if the information  
3           broker knew or should have known that the per-  
4           son to whom such a request is made will obtain  
5           or attempt to obtain such information in the  
6           manner described in subparagraph (A).

7 **SEC. 3. NOTIFICATION OF INFORMATION SECURITY**  
8 **BREACH.**

9       (a) INDIVIDUAL NOTIFICATION.—

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

17           (2) TIMELINESS OF NOTIFICATION.—

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

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

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

20 (ii) NATIONAL SECURITY.—If a Fed-  
21 eral national security agency or homeland  
22 security agency determines that the notifi-  
23 cation required under this section would  
24 threaten national or homeland security,  
25 such notification may be delayed for a pe-

1           riod of time which the national security  
2           agency or homeland security agency deter-  
3           mines is reasonably necessary and requests  
4           in writing. A Federal national security  
5           agency or homeland security agency may  
6           revoke such delay or extend the period of  
7           time set forth in the original request made  
8           under this paragraph by a subsequent  
9           written request if further delay is nec-  
10          essary.

11       (b) COORDINATION OF NOTIFICATION WITH CREDIT  
12   REPORTING AGENCIES.—If a covered entity is required to  
13   provide notification to more than 5,000 individuals under  
14   subsection (a)(1), the covered entity shall also notify the  
15   major consumer reporting agencies that compile and  
16   maintain files on consumers on a nationwide basis, of the  
17   timing and distribution of the notifications. Such notifica-  
18   tion shall be given to the credit reporting agencies without  
19   unreasonable delay and, if such notification will not delay  
20   notification to the affected individuals, prior to the dis-  
21   tribution of notifications to the affected individuals.

22       (c) METHOD AND CONTENT OF NOTIFICATION.—

23           (1) GENERAL NOTIFICATION.—A covered entity  
24       required to provide notification to individuals under  
25       subsection (a)(1) shall be in compliance with such

1 requirement if the covered entity provides con-  
2 spicuous and clearly identified notification by one of  
3 the following methods (provided the selected method  
4 can reasonably be expected to reach the intended in-  
5 dividual):

6 (A) Written notification to the last known  
7 home mailing address of the individual in the  
8 records of the covered entity.

9 (B) Notification by email or other elec-  
10 tronic means, if—

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

14 (ii) the individual has consented to re-  
15 ceive such notification and the notification  
16 is provided in a manner that is consistent  
17 with the provisions permitting electronic  
18 transmission of notifications under section  
19 101 of the Electronic Signatures in Global  
20 Commerce Act (15 U.S.C. 7001).

21 (2) WEBSITE NOTIFICATION.—The covered en-  
22 tity shall also provide conspicuous notification on the  
23 Internet website of the covered entity (if such cov-  
24 ered entity maintains such a website) for a period of  
25 not less than 90 days.

1           (3) MEDIA NOTIFICATION.—If the number of  
2 residents of a State whose personal information was,  
3 or is reasonably believed to have been acquired or  
4 accessed by an unauthorized person, or used for an  
5 unauthorized purpose exceeds 5,000, the covered en-  
6 tity shall also provide notification in print and to  
7 broadcast media, including major media in metro-  
8 politan and rural areas where the individuals whose  
9 personal information was, or is reasonably believed  
10 to have been, acquired or accessed by an unauthor-  
11 ized person, or used for an unauthorized purpose,  
12 reside.

13           (4) CONTENT OF NOTIFICATION.—

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

18                   (i) a description of the personal infor-  
19 mation that was, or is reasonably believed  
20 to have been, acquired or accessed by an  
21 unauthorized person, or used for an unau-  
22 thorized purpose;

23                   (ii) a telephone number that the indi-  
24 vidual may use, at no cost to such indi-  
25 vidual, to contact the covered entity, or

1 agent of the covered entity, to inquire  
2 about the breach of security or the infor-  
3 mation the covered entity maintained  
4 about that individual;

5 (iii) notification that the individual is  
6 entitled to receive, at no cost to such indi-  
7 vidual, consumer credit reports on a quar-  
8 terly basis for a period of 5 years, or credit  
9 monitoring or other service that enables  
10 consumers to detect the misuse of their  
11 personal information for a period of 5  
12 years, and instructions to the individual on  
13 requesting such reports or service from the  
14 covered entity;

15 (iv) the toll-free contact telephone  
16 numbers and addresses for the major cred-  
17 it reporting agencies; and

18 (v) a toll-free telephone number and  
19 Internet website address for the Commis-  
20 sion whereby the individual may obtain in-  
21 formation regarding identity theft.

22 (B) DIRECT BUSINESS RELATIONSHIP.—

23 Regardless of whether the covered entity or a  
24 designated third party provides notification  
25 under this subsection, such notification shall

1 identify the covered entity that has a direct  
2 business relationship with the individual.

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

8 (A) establish criteria for determining cir-  
9 cumstances under which substitute notification  
10 may be provided in lieu of direct notification re-  
11 quired by paragraph (1), including criteria for  
12 determining if notification under paragraph (1)  
13 is not feasible due to excessive costs to the cov-  
14 ered entity required to provided such notifica-  
15 tion relative to the resources of such covered  
16 entity; and

17 (B) establish the form and content of sub-  
18 stitute notification.

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

24 (1) the Commission;

25 (2) the Federal Bureau of Investigation;

1 (3) the Secret Service;

2 (4) for common carriers, the Federal Commu-  
3 nications Commission;

4 (5) the Consumer Financial Protection Bureau;  
5 and

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

11 (e) OTHER OBLIGATIONS FOLLOWING BREACH.—

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

18 (A) consumer credit reports from the  
19 major credit reporting agencies beginning not  
20 later than 60 days following the individual's re-  
21 quest and continuing on a quarterly basis for a  
22 period of 5 years thereafter; or

23 (B) a credit monitoring or other service  
24 that enables consumers to detect the misuse of  
25 their personal information, beginning not later

1           than 60 days following the individual's request  
2           and continuing for a period of 5 years.

3           (2) RULEMAKING.—As part of the Commis-  
4           sion's rulemaking described in subsection (c)(5), the  
5           Commission shall determine the circumstances under  
6           which a covered entity required to provide notifica-  
7           tion under subsection (a) shall provide or arrange  
8           for the provision of free consumer credit reports or  
9           credit monitoring or other service to affected individ-  
10          uals.

11          (f) WEBSITE NOTIFICATION OF FEDERAL TRADE  
12          COMMISSION.—If the Commission, upon receiving notifi-  
13          cation of any breach of security that is reported to the  
14          Commission under subsection (d)(1), finds that notifica-  
15          tion of such a breach of security via the Commission's  
16          Internet website would be in the public interest or for the  
17          protection of consumers, the Commission shall place such  
18          a notification in a clear and conspicuous location on its  
19          Internet website.

20          (g) WEBSITE NOTIFICATION OF STATE ATTORNEYS  
21          GENERAL.—If a State attorney general, upon receiving  
22          notification of any breach of security that is reported to  
23          the Commission under subsection (d)(5), finds that notifi-  
24          cation of such a breach of security through the State at-  
25          torney general's Internet website would be in the public

1 interest or for the protection of consumers, the State at-  
2 torney general shall place such a notification in a clear  
3 and conspicuous location on its Internet website.

4 (h) FTC STUDY ON NOTIFICATION IN LANGUAGES  
5 IN ADDITION TO ENGLISH.—Not later than 1 year after  
6 the date of enactment of this Act, the Commission shall  
7 conduct a study on the practicality and cost effectiveness  
8 of requiring the notification required by subsection (c)(1)  
9 to be provided in a language in addition to English to indi-  
10 viduals known to speak only such other language.

11 (i) EDUCATION AND OUTREACH FOR SMALL BUSI-  
12 NESSES.—The Commission shall conduct education and  
13 outreach for small business concerns on data security  
14 practices and how to prevent hacking and other unauthor-  
15 ized access to, acquisition of, or use of data maintained  
16 by such small business concerns.

17 (j) WEBSITE ON DATA SECURITY BEST PRAC-  
18 TICES.—The Commission shall establish and maintain an  
19 Internet website containing non-binding best practices for  
20 businesses regarding data security and how to prevent  
21 hacking and other unauthorized access to, acquisition of,  
22 or use of data maintained by such businesses.

23 (k) GENERAL RULEMAKING AUTHORITY.—

24 (1) IN GENERAL.—The Commission may pro-  
25 mulgate regulations necessary under section 553 of

1 title 5, United States Code, to effectively enforce the  
2 requirements of this section.

3 (2) LIMITATION.—In promulgating rules under  
4 this Act, the Commission shall not require the de-  
5 ployment or use of any specific products or tech-  
6 nologies, including any specific computer software or  
7 hardware.

8 (l) TREATMENT OF PERSONS GOVERNED BY OTHER  
9 LAW.—A covered entity who is in compliance with any  
10 other Federal law that requires such covered entity to pro-  
11 vide notification to individuals following a breach of secu-  
12 rity, shall be deemed to be in compliance with this section  
13 with respect to activities and information covered under  
14 such Federal law.

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

16 (a) ENFORCEMENT BY THE FEDERAL TRADE COM-  
17 MISSION.—

18 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-  
19 TICES.—A violation of section 2 or 3 shall be treated  
20 as an unfair and deceptive act or practice in viola-  
21 tion of a regulation under section 18(a)(1)(B) of the  
22 Federal Trade Commission Act (15 U.S.C.  
23 57a(a)(1)(B)) regarding unfair or deceptive acts or  
24 practices and shall be subject to enforcement by the  
25 Commission under that Act with respect to any cov-

1       ered entity. All of the functions and powers of the  
2       Commission under the Federal Trade Commission  
3       Act are available to the Commission to enforce com-  
4       pliance by any person with the requirements imposed  
5       under this title, irrespective of whether that person  
6       is engaged in commerce or meets any other jurisdic-  
7       tional tests under the Federal Trade Commission  
8       Act.

9               (2) COORDINATION WITH FEDERAL COMMU-  
10       NICATIONS COMMISSION.—Where enforcement re-  
11       lates to entities subject to the authority of the Fed-  
12       eral Communications Commission, enforcement ac-  
13       tions by the Commission will be coordinated with the  
14       Federal Communications Commission.

15              (3) COORDINATION WITH CONSUMER FINANCIAL  
16       PROTECTION BUREAU.—Where enforcement relates  
17       to financial information or information associated  
18       with the provision of financial products or services,  
19       enforcement actions by the Commission will be co-  
20       ordinated with the Consumer Financial Protection  
21       Bureau.

22       (b) ENFORCEMENT BY STATE ATTORNEYS GEN-  
23       ERAL.—

24              (1) IN GENERAL.—If the chief law enforcement  
25       officer of a State, or an official or agency designated

1 by a State, has reason to believe that any covered  
2 entity has violated or is violating section 2 or 3 of  
3 this Act, the attorney general, official, or agency of  
4 the State, in addition to any authority it may have  
5 to bring an action in State court under its consumer  
6 protection law, may bring a civil action in any ap-  
7 propriate United States district court or in any  
8 other court of competent jurisdiction, including a  
9 State court, to—

10 (A) enjoin further such violation by the de-  
11 fendant;

12 (B) enforce compliance with this such sec-  
13 tion;

14 (C) obtain civil penalties in the amount de-  
15 termined under paragraph (2); and

16 (D) obtain damages, restitution, or other  
17 compensation on behalf of residents of the  
18 State.

19 (2) CIVIL PENALTIES.—

20 (A) CALCULATION.—

21 (i) TREATMENT OF VIOLATIONS OF  
22 SECTION 2.—For purposes of paragraph  
23 (1)(C) with regard to a violation of section  
24 2, the amount determined under this para-  
25 graph is the amount calculated by multi-

1           plying the number of days that a covered  
2           entity is not in compliance with such sec-  
3           tion by an amount to be determined by the  
4           Commission. Such amount determined by  
5           the Commission shall be adjusted as de-  
6           scribed in the Federal Civil Penalties Infla-  
7           tion Adjustment Act of 1990 (Public Law  
8           101-410; 28 U.S.C. 2461 note).

9           (ii) TREATMENT OF VIOLATIONS OF  
10          SECTION 3.—For purposes of paragraph  
11          (1)(C) with regard to a violation of section  
12          3, the amount determined under this para-  
13          graph is the amount calculated by multi-  
14          plying the number of violations of such  
15          section by an amount to be determined by  
16          the Commission. Each failure to send noti-  
17          fication as required under section 3 to a  
18          citizen or resident of the United States  
19          shall be treated as a separate violation.

20          (B) ADJUSTMENT FOR INFLATION.—Be-  
21          ginning on the date that the Consumer Price  
22          Index is first published by the Bureau of Labor  
23          Statistics that is after 1 year after the date of  
24          enactment of this Act, and each year thereafter,  
25          the amounts specified in clauses (i) and (ii) of

1           subparagraph (A) shall be increased by the per-  
2           centage increase in the Consumer Price Index  
3           published on that date from the Consumer  
4           Price Index published the previous year.

5           (3) NOTICE AND INTERVENTION BY THE  
6       FTC.—

7           (A) The attorney general of a State shall  
8           provide prior written notice of any action under  
9           paragraph (1) to the Commission and provide  
10          the Commission with a copy of the complaint in  
11          the action, except in any case in which such  
12          prior notice is not feasible, in which case the at-  
13          torney general shall serve such notice imme-  
14          diately upon instituting such action. The Com-  
15          mission shall have the right—

16               (i) to intervene in the action;

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

19               (iii) to file petitions for appeal.

20          (B) LIMITATION ON STATE ACTION WHILE  
21          FEDERAL ACTION IS PENDING.—If the Commis-  
22          sion has instituted a civil action for violation of  
23          this Act, no State attorney general, or official  
24          or agency of a State, may bring an action under  
25          this subsection during the pendency of that ac-

1           tion against any defendant named in the com-  
2           plaint of the Commission for any violation of  
3           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, sale of, or use of data containing personal  
15           information.

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

18           (3) COVERED ENTITY.—The term “covered en-  
19           tity” means—

20                   (A) any organization, corporation, trust,  
21                   partnership, sole proprietorship, unincorporated  
22                   association, or venture over which the Commis-  
23                   sion has authority pursuant to section 5(a)(2)  
24                   of the Federal Trade Commission Act (15  
25                   U.S.C. 45(a)(2));

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

(C) notwithstanding sections 4 and 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 44 and 45(a)(2)), any non-profit organization, including any organization described in section 501(c) of the Internal Revenue Code of 1986 that is exempt from taxation under section 501(a) of the Internal Revenue Code of 1986.

(4) PERSONAL INFORMATION.—

(A) DEFINITION.—The term “personal information” means any information or compilation of information that includes any of the following:

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

(I) Home address or telephone number.

(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 fingerprint, voice print, a retina  
18 or iris image, or any other unique physical  
19 representations.

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

24 (vii) Any two or more of the following  
25 data elements:

1 (I) An individual's first and last  
2 name or first initial and last name.

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

8 (III) Any security code, access  
9 code, or password, or source code that  
10 could be used to generate such codes  
11 or passwords.

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

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

24 (x) A health insurance policy number  
25 or subscriber identification number and

any unique identifier used by a health insurer to identify the individual, or any information in an individual's health insurance application and claims history, including any appeals records.

(xi) Digitized or other electronic signature.

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

(xiii) Any record or information concerning payroll, income, financial accounts, mortgages, loans, lines of credit, utility bills, accumulated purchases, or any other information regarding financial assets, obligations, or spending habits.

(xiv) Any additional element the Commission defines as personal information.

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

(5) STATE.—The term “State” means each of the several States, the District of Columbia, the

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

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

7 (a) EFFECT ON STATE DATA SECURITY AND  
8 BREACH NOTIFICATION LAWS.—This Act supersedes any  
9 provision of a statute or regulation of a State or political  
10 subdivision of a State, with respect to a covered entity,  
11 that expressly—

12 (1) requires information security practices for  
13 the treatment and protection of personal information  
14 similar to any of those required under section 2; or

15 (2) requires notification to individuals of a  
16 breach of security of personal information.

17 (b) EFFECT ON OTHER STATE LAWS.—Nothing in  
18 this Act shall be construed to—

19 (1) preempt or limit any provision of any law,  
20 rule, regulation, requirement, standard, or other pro-  
21 vision having the force and effect of law of any  
22 State, including any State consumer protection law,  
23 any State law relating to acts of fraud or deception,  
24 and any State trespass, contract, or tort law;

1           (2) prevent or limit the attorney general of a  
2       State from exercising the powers conferred upon the  
3       attorney general by the laws of the State, including  
4       conducting investigations, administering oaths or af-  
5       firmations, or compelling the attendance of witnesses  
6       or the production of documentary and other evi-  
7       dence; or

8           (3) preempt or limit any provision of any law,  
9       rule, regulation, requirement, standard, or other pro-  
10      vision having the force and effect of law of any State  
11      with respect to any person that is not a covered enti-  
12      ty.

13      (c) PRESERVATION OF AUTHORITY.—

14           (1) FEDERAL TRADE COMMISSION.—Nothing in  
15      this Act may be construed in any way to limit the  
16      Commission’s authority under any other provision of  
17      law.

18           (2) FEDERAL COMMUNICATIONS COMMISSION.—  
19      Nothing in this Act may be construed in any way to  
20      limit or affect the Federal Communication Commis-  
21      sion’s authority under any other provision of law.

22           (3) CONSUMER FINANCIAL PROTECTION BU-  
23      REAU.—Nothing in this Act may be construed in  
24      any way to limit or affect the Consumer Financial

1       Protection Bureau's authority under any other pro-  
2       vision of law.

3   **SEC. 7. EFFECTIVE DATE.**

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

