

116TH CONGRESS  
1ST SESSION

# H. R. 1282

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

FEBRUARY 14, 2019

Mr. RUSH (for himself, Ms. BLUNT ROCHESTER, and Ms. CLARKE of New York) 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, that require each cov-  
8 ered entity to establish and implement policies and  
9 procedures regarding information security practices  
10 for the treatment and protection of personal infor-  
11 mation 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.—The regulations required  
23 pursuant to paragraph (1) shall include a require-  
24 ment that the policies and procedures include the  
25 following:

1 (A) A written security policy with respect  
2 to the collection, use, sale, other dissemination,  
3 and maintenance of the 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 vulnerability in any  
10 system maintained by the covered entity that  
11 contains such data, including regular moni-  
12 toring for a breach of security of any such sys-  
13 tem.

14 (D) A process for—

15 (i) taking preventive and corrective  
16 action to mitigate against any vulnerability  
17 identified in the process required by sub-  
18 paragraph (C), which may include imple-  
19 menting any changes to security practices  
20 and the architecture, installation, or imple-  
21 mentation of network or operating soft-  
22 ware; and

23 (ii) regularly testing or otherwise  
24 monitoring the effectiveness of the key con-

1 trols, systems, and procedures of the safe-  
2 guards.

3 (E) A process for disposing of data con-  
4 taining personal information by shredding, per-  
5 manently erasing, or otherwise modifying the  
6 personal information contained in such data to  
7 make such personal information permanently  
8 unreadable or undecipherable.

9 (F) A process for overseeing persons to  
10 whom personal information is disclosed, or who  
11 have access to internet-connected devices, by—

12 (i) taking reasonable steps to select  
13 and retain persons that are capable of  
14 maintaining appropriate safeguards for the  
15 personal information or internet-connected  
16 devices at issue; and

17 (ii) requiring all such persons to im-  
18 plement and maintain such safeguards.

19 (3) TREATMENT OF ENTITIES GOVERNED BY  
20 OTHER FEDERAL LAW.—Any covered entity who is  
21 in compliance with any other Federal law that re-  
22 quires the covered entity to maintain standards and  
23 safeguards for information security and protection of  
24 personal information that, taken as a whole and as  
25 the Commission shall determine in the rulemaking

1 required under this subsection, provide protections  
2 substantially similar to, or greater than, those re-  
3 quired under this subsection, shall be deemed to be  
4 in compliance with this subsection.

5 (b) SPECIAL REQUIREMENTS FOR INFORMATION  
6 BROKERS.—

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

8 The regulations promulgated pursuant to subsection  
9 (a) shall include a requirement for an information  
10 broker to submit each security policy of the broker  
11 to the Commission in conjunction with a notification  
12 of a breach of security under section 3 or upon re-  
13 quest of the Commission.

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

23 (3) ACCURACY OF AND INDIVIDUAL ACCESS TO  
24 PERSONAL INFORMATION.—The regulations promul-

1 gated pursuant to subsection (a) shall include a re-  
2 quirement for the following:

3 (A) ACCURACY.—

4 (i) IN GENERAL.—Each information  
5 broker to establish reasonable procedures  
6 to assure the maximum possible accuracy  
7 of the personal information the informa-  
8 tion broker collects, assembles, or main-  
9 tains, and any other information the infor-  
10 mation broker collects, assembles, or main-  
11 tains that specifically identifies an indi-  
12 vidual, other than information which mere-  
13 ly identifies an individual's name or ad-  
14 dress.

15 (ii) LIMITED EXCEPTION FOR FRAUD  
16 DATABASES.—The requirement in clause  
17 (i) shall not prevent the collection or main-  
18 tenance of information that may be inac-  
19 curate with respect to a particular indi-  
20 vidual when that information is being col-  
21 lected or maintained solely—

22 (I) for the purpose of indicating  
23 whether there may be a discrepancy  
24 or irregularity in the personal infor-

1                   mation that is associated with an indi-  
2                   vidual; and

3                   (II) to help identify, or authen-  
4                   ticate the identity of, an individual, or  
5                   to protect against or investigate fraud  
6                   or other unlawful conduct.

7                   (B) CONSUMER ACCESS TO INFORMA-  
8                   TION.—Each information broker to—

9                   (i) provide to each individual whose  
10                  personal information the information  
11                  broker maintains (at the individual's re-  
12                  quest at least once per year, at no cost to  
13                  the individual, and after verifying the iden-  
14                  tity of the individual), a means for the in-  
15                  dividual to review any personal information  
16                  regarding such individual maintained by  
17                  the information broker and any other in-  
18                  formation maintained by the information  
19                  broker that specifically identifies the indi-  
20                  vidual, other than information which mere-  
21                  ly identifies an individual's name or ad-  
22                  dress; and

23                  (ii) place a conspicuous notice on the  
24                  internet website of the information broker  
25                  (if the information broker maintains such

1 a website) instructing individuals how to  
2 request access to the information required  
3 to be provided under clause (i), and, as ap-  
4 plicable, how to express a preference with  
5 respect to the use of personal information  
6 for marketing purposes.

7 (C) DISPUTED INFORMATION.—

8 (i) IN GENERAL.—Whenever an indi-  
9 vidual whose information the information  
10 broker maintains makes a written request  
11 disputing the accuracy of the information,  
12 the information broker, after verifying the  
13 identity of the individual making such re-  
14 quest and unless there are reasonable  
15 grounds to believe such request is frivolous  
16 or irrelevant, to—

17 (I) correct any inaccuracy; or

18 (II) in the case of information  
19 that is—

20 (aa) public record informa-  
21 tion, inform the individual of the  
22 source of the information, and, if  
23 reasonably available, where a re-  
24 quest for correction may be di-  
25 rected and, if the individual pro-

vides proof that the public record has been corrected or that the information broker was reporting the information incorrectly, correct the inaccuracy in the information broker's records; or

(bb) nonpublic information, note the information that is disputed, including the individual's statement disputing such information, and take reasonable steps to independently verify such information under the procedures outlined in subparagraph (A) if such information can be independently verified.

(ii) STRUCTURE FOR DISPUTE PROCESS.—A basic structure for the dispute process described in clause (i) which shall be in writing, require an online option for the submission of a dispute, and provide an electronic receipt acknowledging the submission.

(D) LIMITATIONS.—A provision, including the scope of the application, that allows an in-

1           formation broker to limit the access to informa-  
2           tion required under subparagraph (B)(i) and is  
3           not required to provide notice to individuals as  
4           required under subparagraph (B)(ii) in the fol-  
5           lowing circumstances:

6                   (i) If access of the individual to the  
7                   information is limited by law or legally rec-  
8                   ognized privilege.

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

13                  (iii) If the information consists of in-  
14                  formation already made available to the  
15                  public, unless that record has been in-  
16                  cluded in a report about an individual  
17                  shared with a third party.

18                  (iv) Any other circumstance in which  
19                  an information broker may limit access to  
20                  information that the Commission deter-  
21                  mines to be appropriate.

22           (E) FCRA REGULATED PERSONS.—A pro-  
23           vision that any information broker that is en-  
24           gaged in activities subject to the Fair Credit  
25           Reporting Act and who is in compliance with

1 sections 609, 610, and 611 of such Act (15  
2 U.S.C. 1681g; 1681h; 1681i) with respect to in-  
3 formation subject to such Act is deemed to be  
4 in compliance with this paragraph with respect  
5 to such information.

6 (F) REQUIREMENT OF AUDIT LOG OF  
7 ACCESSED AND TRANSMITTED INFORMATION.—

8 Each information broker to establish measures  
9 which facilitate the auditing or retracing of any  
10 internal or external access to, or transmissions  
11 of, any data containing personal information  
12 collected, assembled, or maintained by such in-  
13 formation broker.

14 (4) PROHIBITION ON PRETEXTING BY INFOR-  
15 MATION BROKERS.—The regulations promulgated  
16 pursuant to subsection (a) shall include a prohibition  
17 on the following:

18 (A) PROHIBITION ON OBTAINING PER-  
19 SONAL INFORMATION BY FALSE PRETENSES.—

20 An information broker to obtain, attempt to ob-  
21 tain, cause to be disclosed, or attempt to cause  
22 to be disclosed to any person, personal informa-  
23 tion or any other information relating to any  
24 person by—

1 (i) making a false, fictitious, or fraud-  
 2 ulent statement or representation to any  
 3 person; or

4 (ii) providing any document or other  
 5 information to any person that the infor-  
 6 mation broker knows or should know—

7 (I) to be forged, counterfeit, lost,  
 8 stolen, or fraudulently obtained; or

9 (II) to contain a false, fictitious,  
 10 or fraudulent statement or representa-  
 11 tion.

12 (B) PROHIBITION ON SOLICITATION TO  
 13 OBTAIN PERSONAL INFORMATION UNDER FALSE  
 14 PRETENSES.—An information broker to request  
 15 a person to obtain personal information or any  
 16 other information relating to any other person,  
 17 if the information broker knew or should have  
 18 known that the person to whom such a request  
 19 is made will obtain or attempt to obtain such  
 20 information in the manner described in sub-  
 21 paragraph (A).

22 **SEC. 3. NOTIFICATION OF INFORMATION SECURITY**  
 23 **BREACH.**

24 (a) INDIVIDUAL NOTIFICATION.—Not later than 1  
 25 year after the date of enactment of this Act, the Commis-

1 sion shall promulgate regulations under section 553 of  
2 title 5, United States Code, that require the following:

3 (1) IN GENERAL.—Each covered entity to, fol-  
4 lowing the discovery of a breach of security, notify  
5 each individual who is a citizen or resident of the  
6 United States whose personal information was, or is  
7 reasonably believed to have been, acquired or  
8 accessed by an unauthorized person, or used for an  
9 unauthorized purpose.

10 (2) TIMELINESS OF NOTIFICATION.—

11 (A) IN GENERAL.—Unless subject to a  
12 delay authorized under subparagraph (B), a no-  
13 tification required under paragraph (1) shall be  
14 made as expeditiously as practicable and with-  
15 out unreasonable delay, but not later than 30  
16 days following the discovery of a breach of secu-  
17 rity.

18 (B) DELAY OF NOTIFICATION AUTHORIZED  
19 FOR LAW ENFORCEMENT OR NATIONAL SECU-  
20 RITY PURPOSES.—

21 (i) LAW ENFORCEMENT.—If a Fed-  
22 eral or State law enforcement agency, in-  
23 cluding an attorney general of a State, de-  
24 termines that the notification required  
25 under this section would impede a civil or

1 criminal investigation, such notification  
2 shall be delayed upon the written request  
3 of the law enforcement agency for 30 days  
4 or such lesser period of time which the law  
5 enforcement agency determines is reason-  
6 ably necessary and requests in writing.  
7 Such law enforcement agency may, by a  
8 subsequent written request, revoke such  
9 delay or extend the period of time set forth  
10 in the original request made under this  
11 clause if further delay is necessary.

12 (ii) NATIONAL SECURITY.—If a Fed-  
13 eral national security agency or homeland  
14 security agency determines that the notifi-  
15 cation required under this section would  
16 threaten national or homeland security,  
17 such notification may be delayed for a pe-  
18 riod of time which the national security  
19 agency or homeland security agency deter-  
20 mines is reasonably necessary and requests  
21 in writing. A Federal national security  
22 agency or homeland security agency may  
23 revoke such delay or extend the period of  
24 time set forth in the original request made

1 under this clause by a subsequent written  
2 request if further delay is necessary.

3 (3) COORDINATION OF NOTIFICATION WITH  
4 CREDIT REPORTING AGENCIES.—If a covered entity  
5 is required to provide notification to more than  
6 5,000 individuals under paragraph (1), the covered  
7 entity shall also notify the major consumer reporting  
8 agencies that compile and maintain files on con-  
9 sumers on a nationwide basis, of the timing and dis-  
10 tribution of the notifications. Such notification shall  
11 be given to the credit reporting agencies without un-  
12 reasonable delay and, if such notification will not  
13 delay notification to the affected individuals, prior to  
14 the distribution of notifications to the affected indi-  
15 viduals.

16 (4) METHOD AND CONTENT OF NOTIFICA-  
17 TION.—

18 (A) GENERAL NOTIFICATION.—A covered  
19 entity required to provide notification to indi-  
20 viduals under paragraph (1) shall be in compli-  
21 ance with such requirement if the covered entity  
22 provides conspicuous and clearly identified noti-  
23 fication by one of the following methods (pro-  
24 vided the selected method can reasonably be ex-  
25 pected to reach the intended individual):

1 (i) Written notification to the last  
2 known home mailing address of the indi-  
3 vidual in the records of the covered entity.

4 (ii) Notification by email or other  
5 electronic means, if—

6 (I) the covered entity's primary  
7 method of communication with the in-  
8 dividual is by email or such other elec-  
9 tronic means; or

10 (II) the individual has consented  
11 to receive such notification and the  
12 notification is provided in a manner  
13 that is consistent with the provisions  
14 permitting electronic transmission of  
15 notifications under section 101 of the  
16 Electronic Signatures in Global Com-  
17 merce Act (15 U.S.C. 7001).

18 (B) WEBSITE NOTIFICATION.—The cov-  
19 ered entity shall also provide conspicuous notifi-  
20 cation on the internet website of the covered en-  
21 tity (if such covered entity maintains such a  
22 website) for a period of not less than 90 days.

23 (C) MEDIA NOTIFICATION.—If the number  
24 of residents of a State whose personal informa-  
25 tion was, or is reasonably believed to have been

1           acquired or accessed by an unauthorized per-  
2           son, or used for an unauthorized purpose ex-  
3           ceeds 5,000, the covered entity shall also pro-  
4           vide notification in print and to broadcast  
5           media, including major media in metropolitan  
6           and rural areas where the individuals whose  
7           personal information was, or is reasonably be-  
8           lieved to have been, acquired or accessed by an  
9           unauthorized person, or used for an unauthor-  
10          ized purpose, reside.

11                   (D) CONTENT OF NOTIFICATION.—

12                   (i) IN GENERAL.—Any notification  
13                   provided under subparagraph (A), (B), or  
14                   (C) shall include—

15                   (I) a description of the personal  
16                   information that was, or is reasonably  
17                   believed to have been, acquired or  
18                   accessed by an unauthorized person,  
19                   or used for an unauthorized purpose;

20                   (II) a telephone number that the  
21                   individual may use, at no cost to such  
22                   individual, to contact the covered enti-  
23                   ty, or agent of the covered entity, to  
24                   inquire about the breach of security or

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

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

14 (IV) the toll-free contact tele-  
15 phone numbers and addresses for the  
16 major credit reporting agencies; and

17 (V) a toll-free telephone number  
18 and internet website address for the  
19 Commission whereby the individual  
20 may obtain information regarding  
21 identity theft.

22 (ii) DIRECT BUSINESS RELATION-  
23 SHIP.—Any notification provided under  
24 this subsection shall identify the covered

entity that has a direct business relationship with the individual.

(E) SUBSTITUTE NOTIFICATION.—Criteria for determining circumstances under which substitute notification may be provided in lieu of direct notification required by subparagraph (A), including criteria for determining if notification under subparagraph (A) is not feasible due to excessive costs to the covered entity required to provide such notification relative to the resources of such covered entity and the form and content of substitute notification.

(5) NOTIFICATION FOR LAW ENFORCEMENT AND OTHER PURPOSES.—A covered entity to, as expeditiously as practicable and without unreasonable delay, but not later than 7 days following the discovery of a breach of security, provide notification of the breach to—

(A) the Commission;

(B) the Federal Bureau of Investigation;

(C) the Secret Service;

(D) for common carriers, the Federal Communications Commission;

(E) for entities that provide a consumer financial product or service (as defined in section

1 1002 of the Consumer Financial Protection Act  
2 of 2010 (12 U.S.C. 5481)), the Consumer Fi-  
3 nancial Protection Bureau; and

4 (F) the attorney general of each State in  
5 which the personal information of a resident or  
6 residents of the State was, or is reasonably be-  
7 lieved to have been, acquired or accessed by an  
8 unauthorized person, or used for an unauthor-  
9 ized purpose.

10 (6) OTHER OBLIGATIONS FOLLOWING  
11 BREACH.—

12 (A) IN GENERAL.—A covered entity re-  
13 quired to provide notification under subsection  
14 (a) to, upon request of an individual whose per-  
15 sonal information was included in the breach of  
16 security, provide or arrange for the provision of,  
17 to each such individual and at no cost to such  
18 individual—

19 (i) consumer credit reports from the  
20 major credit reporting agencies beginning  
21 not later than 60 days following the indi-  
22 vidual's request and continuing on a quar-  
23 terly basis for a period of 10 years there-  
24 after; or

1 (ii) a credit monitoring or other serv-  
2 ice that enables consumers to detect the  
3 misuse of their personal information, be-  
4 ginning not later than 60 days following  
5 the individual's request and continuing for  
6 a period of 10 years.

7 (B) RULEMAKING.—The circumstances  
8 under which a covered entity required to pro-  
9 vide notification under paragraph (1) shall pro-  
10 vide or arrange for the provision of free con-  
11 sumer credit reports or credit monitoring or  
12 other service to affected individuals.

13 (b) WEBSITE NOTIFICATION.—

14 (1) FEDERAL TRADE COMMISSION.—If the  
15 Commission, upon receiving notification of any  
16 breach of security that is reported to the Commis-  
17 sion under subsection (a)(5)(A), finds that notifica-  
18 tion of such a breach of security through the website  
19 of the Commission would be in the public interest or  
20 for the protection of consumers, the Commission  
21 shall place such a notification in a clear and con-  
22 spicuous location on the website.

23 (2) OTHER FEDERAL AGENCY.—If another Fed-  
24 eral agency (such as the Federal Communications  
25 Commission, the Consumer Financial Protection Bu-

1       reau, or the Department of Justice) receives notice  
2       of a breach of security from a covered entity and  
3       finds that notification of such a breach of security  
4       through the website of the Commission would be in  
5       the public interest or for the protection of con-  
6       sumers, that Federal agency shall place such a noti-  
7       fication in a clear and conspicuous location on the  
8       website of that agency.

9       (c) WEBSITE NOTIFICATION OF STATE ATTORNEYS  
10      GENERAL.—If a State attorney general, upon receiving  
11      notification of any breach of security that is reported to  
12      the Commission under subsection (d)(5), finds that notifi-  
13      cation of such a breach of security through the State at-  
14      torney general’s internet website would be in the public  
15      interest or for the protection of consumers, the State at-  
16      torney general shall place such a notification in a clear  
17      and conspicuous location on its internet website.

18      (d) FTC STUDY ON NOTIFICATION IN LANGUAGES  
19      IN ADDITION TO ENGLISH.—Not later than 1 year after  
20      the date of enactment of this Act, the Commission shall  
21      conduct a study on the practicality and cost effectiveness  
22      of requiring the notification required by subsection (c)(1)  
23      to be provided in a language in addition to English to indi-  
24      viduals known to speak only such other language.

1       (e) EDUCATION AND OUTREACH FOR SMALL BUSI-  
2 NESSES.—The Commission shall conduct education and  
3 outreach for small business concerns on data security  
4 practices and how to prevent hacking and other unauthor-  
5 ized access to, acquisition of, or use of data maintained  
6 by such small business concerns.

7       (f) WEBSITE ON DATA SECURITY BEST PRAC-  
8 TICES.—The Commission shall establish and maintain an  
9 internet website containing non-binding best practices for  
10 businesses regarding data security and how to prevent  
11 hacking and other unauthorized access to, acquisition of,  
12 or use of data maintained by such businesses.

13       (g) GENERAL RULEMAKING AUTHORITY.—

14           (1) IN GENERAL.—The Commission may pro-  
15 mulgate regulations necessary under section 553 of  
16 title 5, United States Code, to effectively enforce the  
17 requirements of this section.

18           (2) LIMITATION.—In promulgating rules under  
19 this Act, the Commission shall not require the de-  
20 ployment or use of any specific product or tech-  
21 nology, including any specific computer software or  
22 hardware.

23       (h) TREATMENT OF PERSONS GOVERNED BY OTHER  
24 LAW.—A covered entity who is in compliance with any  
25 other Federal law that requires such covered entity to pro-

1 vide notification to individuals following a breach of secu-  
2 rity, shall be deemed to be in compliance with this section  
3 with respect to activities and information covered under  
4 such Federal law.

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

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

8 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-  
9 TICES.—A violation of a regulation promulgated  
10 under section 2 or 3 shall be treated as an unfair  
11 and deceptive act or practice in violation of a regula-  
12 tion under section 18(a)(1)(B) of the Federal Trade  
13 Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding  
14 unfair or deceptive acts or practices and shall be  
15 subject to enforcement by the Commission under  
16 that Act with respect to any covered entity. All of  
17 the functions and powers of the Commission under  
18 the Federal Trade Commission Act are available to  
19 the Commission to enforce compliance by any person  
20 with the requirements imposed under this Act.

21 (2) COORDINATION WITH FEDERAL COMMU-  
22 NICATIONS COMMISSION.—In the case of enforce-  
23 ment under this Act that relates to entities subject  
24 to the authority of the Federal Communications  
25 Commission, enforcement actions by the Commission

1 shall be coordinated with the Federal Communica-  
2 tions Commission.

3 (3) COORDINATION WITH CONSUMER FINANCIAL  
4 PROTECTION BUREAU.—In the case of enforcement  
5 under this Act that relates to entities that provide  
6 a consumer financial product or service (as defined  
7 in section 1002 of the Consumer Financial Protec-  
8 tion Act of 2010 (12 U.S.C. 5481)), enforcement ac-  
9 tions by the Commission shall be coordinated with  
10 the Consumer Financial Protection Bureau.

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

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

24 (A) enjoin further such violation by the de-  
25 fendant;

1 (B) enforce compliance with section 2 or 3,  
2 as applicable;

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

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

8 (2) CIVIL PENALTIES.—

9 (A) CALCULATION.—

10 (i) TREATMENT OF VIOLATIONS OF  
11 SECTION 2.—For purposes of paragraph  
12 (1)(C) with regard to a violation of section  
13 2, the amount determined under this para-  
14 graph is the amount calculated by multi-  
15 plying the number of days that a covered  
16 entity is not in compliance with such sec-  
17 tion by an amount to be determined by the  
18 Commission. Such amount determined by  
19 the Commission shall be adjusted as de-  
20 scribed in the Federal Civil Penalties Infla-  
21 tion Adjustment Act of 1990 (Public Law  
22 101–410; 28 U.S.C. 2461 note).

23 (ii) TREATMENT OF VIOLATIONS OF  
24 SECTION 3.—For purposes of paragraph  
25 (1)(C) with regard to a violation of section

1           3, the amount determined under this para-  
2           graph is the amount calculated by multi-  
3           plying the number of violations of such  
4           section by an amount to be determined by  
5           the Commission. Each failure to send noti-  
6           fication as required under section 3 to a  
7           citizen or resident of the United States  
8           shall be treated as a separate violation.

9           (B) ADJUSTMENT FOR INFLATION.—Be-  
10          ginning on the date that the Consumer Price  
11          Index is first published by the Bureau of Labor  
12          Statistics that is after 1 year after the date of  
13          enactment of this Act, and each year thereafter,  
14          the amounts specified in clauses (i) and (ii) of  
15          subparagraph (A) shall be increased by the per-  
16          centage increase in the Consumer Price Index  
17          published on that date from the Consumer  
18          Price Index published the previous year.

19          (3) NOTICE AND INTERVENTION BY THE  
20          FTC.—

21          (A) IN GENERAL.—The attorney general of  
22          a State shall provide prior written notice of any  
23          action under paragraph (1) to the Commission  
24          and provide the Commission with a copy of the  
25          complaint in the action, except in any case in

1           which such prior notice is not feasible, in which  
 2           case the attorney general shall serve such notice  
 3           immediately upon instituting such action. The  
 4           Commission shall have the right—

5                     (i) to intervene in the action;

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

8                     (iii) to file petitions for appeal.

9           (B) LIMITATION ON STATE ACTION WHILE  
 10          FEDERAL ACTION IS PENDING.—If the Commis-  
 11          sion has instituted a civil action for a violation  
 12          of this Act, no State attorney general, or offi-  
 13          cial or agency of a State, may bring an action  
 14          under this subsection during the pendency of  
 15          that action against any defendant named in the  
 16          complaint of the Commission for any violation  
 17          of this Act alleged in the complaint.

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

19          If the attorney general of a State has authority to  
 20          bring an action under State law directed at acts or  
 21          practices that also violate this Act, the attorney gen-  
 22          eral may assert the State-law claim and a claim  
 23          under this Act in the same civil action.

24   **SEC. 5. DEFINITIONS.**

25          In this Act:

1           (1) BREACH OF SECURITY.—The term “breach  
2       of security” means unauthorized access to, acquisi-  
3       tion of, sale of, release of, or use of data containing  
4       personal information.

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

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

9                (A) any person, partnership, or corporation  
10           over which the Commission has authority pur-  
11           suant to section 5(a)(2) of the Federal Trade  
12           Commission Act (15 U.S.C. 45(a)(2));

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

18               (C) notwithstanding sections 4 and 5(a)(2)  
19           of the Federal Trade Commission Act (15  
20           U.S.C. 44 and 45(a)(2)), any nonprofit organi-  
21           zation.

22           (4) NONPROFIT ORGANIZATION.—The term  
23       “nonprofit organization” means an organization de-  
24       scribed in section 501(c) of the Internal Revenue

1 Code of 1986 that is exempt from taxation under  
2 section 501(a) of such Code.

3 (5) INFORMATION BROKER.—The term “infor-  
4 mation broker” means any individual, person, part-  
5 nership, or corporation that collects personal infor-  
6 mation, sells personal information, or profits from  
7 personal information in any way.

8 (6) PERSONAL INFORMATION.—

9 (A) DEFINITION.—The term “personal in-  
10 formation” means any information or compila-  
11 tion of information that includes any of the fol-  
12 lowing:

13 (i) An individual’s first name or initial  
14 and last name in combination with any of  
15 the following data elements for that indi-  
16 vidual:

17 (I) Home address or telephone  
18 number.

19 (II) Mother’s maiden name.

20 (III) Month, day, and year of  
21 birth.

22 (IV) User name or electronic  
23 mail address.

24 (ii) Driver’s license number, passport  
25 number, military identification number,

1 alien registration number, or other similar  
2 number issued on a government document  
3 used to verify identity.

4 (iii) Unique account identifier (includ-  
5 ing a financial account number or credit or  
6 debit card number), electronic identifica-  
7 tion number, user name, or routing code.

8 (iv) Partial or complete Social Secu-  
9 rity number.

10 (v) Unique biometric or genetic data  
11 such as a fingerprint, voice print, retina or  
12 iris image, facial recognition data, or any  
13 other unique physical representation.

14 (vi) Information that could be used to  
15 access an individual's account, such as  
16 user name and password or e-mail address  
17 and password.

18 (vii) Any security code, access code,  
19 password, or source code that could be  
20 used to generate such codes or passwords,  
21 in combination with either of the following  
22 data elements:

23 (I) An individual's first and last  
24 name or first initial and last name.

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

6 (viii) Information generated or derived  
7 from the operation or use of an electronic  
8 communications device that is sufficient to  
9 identify the street name and name of the  
10 city or town in which the device is located.

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

18 (x) A health insurance policy number  
19 or subscriber identification number and  
20 any unique identifier used by a health in-  
21 surer to identify the individual or any in-  
22 formation in an individual's health insur-  
23 ance application and claims history, includ-  
24 ing any appeals records.

1 (xi) Digitized or other electronic sig-  
2 nature.

3 (xii) Nonpublic communication such  
4 as a text, SMS, MMS, RCS, and other  
5 electronic message or other user-created  
6 content such as an email, photograph, or  
7 video.

8 (xiii) Any record or information con-  
9 cerning payroll, income, financial account,  
10 mortgage, loan, line of credit, utility bill,  
11 accumulated purchase, or any other infor-  
12 mation regarding a financial asset, obliga-  
13 tion, or spending habit.

14 (xiv) Any additional element the Com-  
15 mission defines as personal information in  
16 accordance with subparagraph (B).

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

22 (7) SMALL BUSINESS CONCERN.—The term  
23 “small business concern” has the meaning given  
24 that term in section 3 of the Small Business Act (15  
25 U.S.C. 632).

1           (8) STATE.—The term “State” means each of  
2       the several States, the District of Columbia, the  
3       Commonwealth of Puerto Rico, Guam, American  
4       Samoa, the United States Virgin Islands, the Com-  
5       monwealth of the Northern Mariana Islands, any  
6       other territory or possession of the United States,  
7       and each federally recognized Indian Tribe.

8   **SEC. 6. EFFECT ON OTHER LAWS.**

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

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

17           (2) requires notification to individuals of a  
18       breach of security of personal information.

19       (b) EFFECT ON OTHER STATE LAWS.—Except as  
20   provided in subsection (a), nothing in this Act shall be  
21   construed to—

22           (1) preempt or limit any provision of any law,  
23       rule, regulation, requirement, standard, or other pro-  
24       vision having the force and effect of law of any  
25       State, including any State consumer protection law,

1 any State law relating to acts of fraud or deception,  
2 and any State trespass, contract, or tort law;

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

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

15 (c) PRESERVATION OF AUTHORITY.—Nothing in this  
16 Act may be construed in any way to limit or affect the  
17 authority of the Commission, the Federal Communication  
18 Commission, or the Consumer Financial Protection Bu-  
19 reau under any other provision of law.

20 **SEC. 7. EFFECTIVE DATE.**

21 This Act shall take effect 90 days after the date of  
22 enactment of this Act.

○