

**AMENDMENT IN THE NATURE OF A SUBSTITUTE  
OFFERED BY MR. RUSH**

Strike all after the enacting clause and insert the  
following:

**1 SECTION 1. SHORT TITLE.**

2       This Act may be cited as the “Data Accountability  
3 and Trust Act”.

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

5       (a) GENERAL SECURITY POLICIES AND PROCE-  
6 DURES.—

7           (1) REGULATIONS.—Not later than 1 year after  
8 the date of enactment of this Act, the Commission  
9 shall promulgate regulations under section 553 of  
10 title 5, United States Code, to require each person  
11 engaged in interstate commerce that owns or pos-  
12 sesses data containing personal information, or con-  
13 tracts to have any third party entity maintain such  
14 data for such person, to establish and implement  
15 policies and procedures regarding information secu-  
16 rity practices for the treatment and protection of  
17 personal information taking into consideration—

1 (A) the size of, and the nature, scope, and  
2 complexity of the activities engaged in by, such  
3 person;

4 (B) the current state of the art in adminis-  
5 trative, technical, and physical safeguards for  
6 protecting such information; and

7 (C) the cost of implementing such safe-  
8 guards.

9 (2) REQUIREMENTS.—Such regulations shall  
10 require the policies and procedures to include the  
11 following:

12 (A) A security policy with respect to the  
13 collection, use, sale, other dissemination, and  
14 maintenance of such personal information.

15 (B) The identification of an officer or  
16 other individual as the point of contact with re-  
17 sponsibility for the management of information  
18 security.

19 (C) A process for identifying and assessing  
20 any reasonably foreseeable vulnerabilities in the  
21 system or systems maintained by such person  
22 that contains such data, which shall include  
23 regular monitoring for a breach of security of  
24 such system or systems.

1 (D) A process for taking preventive and  
2 corrective action to mitigate against any  
3 vulnerabilities identified in the process required  
4 by subparagraph (C), which may include imple-  
5 menting any changes to security practices and  
6 the architecture, installation, or implementation  
7 of network or operating software.

8 (E) A process for disposing of data in elec-  
9 tronic form containing personal information by  
10 shredding, permanently erasing, or otherwise  
11 modifying the personal information contained in  
12 such data to make such personal information  
13 permanently unreadable or undecipherable.

14 (F) A standard method or methods for the  
15 destruction of paper documents and other non-  
16 electronic data containing personal information.

17 (3) TREATMENT OF ENTITIES GOVERNED BY  
18 OTHER LAW.—Any person who is in compliance with  
19 any other Federal law that requires such person to  
20 maintain standards and safeguards for information  
21 security and protection of personal information that,  
22 taken as a whole and as the Commission shall deter-  
23 mine in the rulemaking required under paragraph  
24 (1), provide protections substantially similar to, or  
25 greater than, those required under this subsection,

1 shall be deemed to be in compliance with this sub-  
2 section.

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 curacy of the personal information it col-  
2 lects, assembles, or maintains, and any  
3 other information it collects, assembles, or  
4 maintains that specifically identifies an in-  
5 dividual, other than information which  
6 merely identifies an individual's name or  
7 address.

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

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

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

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

1 (i) provide to each individual whose  
2 personal information it maintains, at the  
3 individual's request at least 1 time per  
4 year and at no cost to the individual, and  
5 after verifying the identity of such indi-  
6 vidual, a means for the individual to review  
7 any personal information regarding such  
8 individual maintained by the information  
9 broker and any other information main-  
10 tained by the information broker that spe-  
11 cifically identifies such individual, other  
12 than information which merely identifies  
13 an individual's name or address; and

14 (ii) place a conspicuous notice on its  
15 Internet website (if the information broker  
16 maintains such a website) instructing indi-  
17 viduals how to request access to the infor-  
18 mation required to be provided under  
19 clause (i), and, as applicable, how to ex-  
20 press a preference with respect to the use  
21 of personal information for marketing pur-  
22 poses under subparagraph (D).

23 (C) DISPUTED INFORMATION.—Whenever  
24 an individual whose information the information  
25 broker maintains makes a written request dis-

1           puting the accuracy of any such information,  
2           the information broker, after verifying the iden-  
3           tity of the individual making such request and  
4           unless there are reasonable grounds to believe  
5           such request is frivolous or irrelevant, shall—

6                           (i) correct any inaccuracy; or

7                           (ii)(I) in the case of information that  
8                           is public record information, inform the in-  
9                           dividual of the source of the information,  
10                           and, if reasonably available, where a re-  
11                           quest for correction may be directed and,  
12                           if the individual provides proof that the  
13                           public record has been corrected or that  
14                           the information broker was reporting the  
15                           information incorrectly, correct the inaccu-  
16                           racy in the information broker's records; or

17                           (II) in the case of information that is  
18                           non-public information, note the informa-  
19                           tion that is disputed, including the individ-  
20                           ual's statement disputing such informa-  
21                           tion, and take reasonable steps to inde-  
22                           pendently verify such information under  
23                           the procedures outlined in subparagraph  
24                           (A) if such information can be independ-  
25                           ently verified.

1           (D) ALTERNATIVE PROCEDURE FOR CER-  
2 TAIN MARKETING INFORMATION.—In accord-  
3 ance with regulations issued under clause (v),  
4 an information broker that maintains any infor-  
5 mation described in clause (i) which is used,  
6 shared, or sold by such information broker for  
7 marketing purposes, may, in lieu of complying  
8 with the access and dispute requirements set  
9 forth in clauses (i) and (ii), provide each indi-  
10 vidual whose information it maintains with a  
11 reasonable means of expressing a preference not  
12 to have his or her information used for such  
13 purposes. If the individual expresses such a  
14 preference, the information broker may not use,  
15 share, or sell the individual's information for  
16 marketing purposes.

17           (E) LIMITATIONS.—An information broker  
18 may limit the access to information required  
19 under subparagraph (B)(i) and is not required  
20 to provide notice to individuals as required  
21 under subparagraph (B)(ii) in the following cir-  
22 cumstances:

23                   (i) If access of the individual to the  
24 information is limited by law or legally rec-  
25 ognized privilege.

1 (ii) If the information is used for a le-  
2 gitimate governmental or fraud prevention  
3 purpose that would be compromised by  
4 such access.

5 (iii) If the information consists of a  
6 published media record, unless that record  
7 has been included in a report about an in-  
8 dividual shared with a third party.

9 (F) RULEMAKING.—Not later than 1 year  
10 after the date of the enactment of this Act, the  
11 Commission shall promulgate regulations under  
12 section 553 of title 5, United States Code, to  
13 carry out this paragraph and to facilitate the  
14 purposes of this Act. In addition, the Commis-  
15 sion shall issue regulations, as necessary, under  
16 section 553 of title 5, United States Code, on  
17 the scope of the application of the limitations in  
18 clause (iv), including any additional cir-  
19 cumstances in which an information broker may  
20 limit access to information under such clause  
21 that the Commission determines to be appro-  
22 priate.

23 (G) FCRA REGULATED PERSONS.—Any  
24 information broker who is engaged in activities  
25 subject to the Fair Credit Reporting Act and

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

7           (4) REQUIREMENT OF AUDIT LOG OF ACCESSED  
8           AND TRANSMITTED INFORMATION.—Not later than  
9           1 year after the date of the enactment of this Act,  
10          the Commission shall promulgate regulations under  
11          section 553 of title 5, United States Code, to require  
12          information brokers to establish measures which fa-  
13          cilitate the auditing or retracing of any internal or  
14          external access to, or transmissions of, any data con-  
15          taining personal information collected, assembled, or  
16          maintained by such information broker.

17          (5) PROHIBITION ON PRETEXTING BY INFOR-  
18          MATION BROKERS.—

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

21                 It shall be unlawful for an information broker  
22                 to obtain or attempt to obtain, or cause to be  
23                 disclosed or attempt to cause to be disclosed to  
24                 any person, personal information or any other  
25                 information relating to any 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 to be  
7 forged, counterfeit, lost, stolen, or fraudu-  
8 lently obtained, or to contain a false, ficti-  
9 tious, or fraudulent statement or represen-  
10 tation.

11 (B) PROHIBITION ON SOLICITATION TO  
12 OBTAIN PERSONAL INFORMATION UNDER FALSE  
13 PRETENSES.—It shall be unlawful for an infor-  
14 mation broker to request a person to obtain  
15 personal information or any other information  
16 relating to any other person, if the information  
17 broker knew or should have known that the per-  
18 son to whom such a request is made will obtain  
19 or attempt to obtain such information in the  
20 manner described in subparagraph (A).

21 (c) EXEMPTION FOR CERTAIN SERVICE PRO-  
22 VIDERS.—Nothing in this section shall apply to a service  
23 provider for any electronic communication by a third party  
24 that is transmitted, routed, or stored in intermediate or  
25 transient storage by such service provider.

1 **SEC. 3. NOTIFICATION OF INFORMATION SECURITY**  
2 **BREACH.**

3 (a) **NATIONWIDE NOTIFICATION.**—Any person en-  
4 gaged in interstate commerce that owns or possesses data  
5 containing personal information shall, following the dis-  
6 covery of a breach of security of the system maintained  
7 by such person that contains such data, notify—

8 (1) each individual who is a citizen or resident  
9 of the United States whose personal information was  
10 acquired or accessed or there was a reasonable basis  
11 to conclude personal information was acquired or  
12 accessed as a result of such a breach of security;

13 (2) the Commission;

14 (3) the Federal Bureau of Investigation and  
15 United States Secret Service; and

16 (4) the Attorney General of each State in which  
17 any affected individual resides.

18 (b) **SPECIAL NOTIFICATION REQUIREMENTS.**—

19 (1) **THIRD PARTY AGENTS.**—In the event of a  
20 breach of security by any third party entity that has  
21 been contracted to maintain or process data con-  
22 taining personal information on behalf of any other  
23 person who owns or possesses such data, such third  
24 party entity shall be required to notify such person  
25 of the breach of security. Upon receiving such notifi-

1 cation from such third party, such person shall pro-  
2 vide the notification required under subsection (a).

3 (2) SERVICE PROVIDERS.—If a service provider  
4 becomes aware of a breach of security of data con-  
5 taining personal information that is owned or pos-  
6 sessed by another person that connects to or uses a  
7 system or network provided by the service provider  
8 for the purpose of transmitting, routing, or pro-  
9 viding intermediate or transient storage of such  
10 data, such service provider shall be required to no-  
11 tify of such a breach of security only the person who  
12 initiated such connection, transmission, routing, or  
13 storage if such person can be reasonably identified.  
14 Upon receiving such notification from a service pro-  
15 vider, such person shall provide the notification re-  
16 quired under subsection (a).

17 (3) COORDINATION OF NOTIFICATION WITH  
18 CONSUMER REPORTING AGENCIES.—If a person is  
19 required to provide notification to more than 5,000  
20 individuals under subsection (a)(1), the person shall  
21 also notify the major consumer reporting agencies of  
22 the timing and distribution of the notices. Such no-  
23 tice shall be given to the consumer reporting agen-  
24 cies without unreasonable delay and, if it will not

1 delay notice to the affected individuals, prior to the  
2 distribution of notices to the affected individuals.

3 (c) TIMELINESS OF NOTIFICATION.—

4 (1) IN GENERAL.—Unless subject to a delay au-  
5 thorized under paragraph (2), a notification required  
6 under subsection (a) shall be made not later than 30  
7 days following the discovery of a breach of security,  
8 unless the person providing notice can show that  
9 providing notice within such a timeframe is not fea-  
10 sible due to extraordinary circumstances necessary  
11 to prevent further breach or unauthorized disclo-  
12 sures, and reasonably restore the integrity of the  
13 data system, in which case such notification shall be  
14 made as promptly as possible.

15 (2) DELAY OF NOTIFICATION AUTHORIZED FOR  
16 LAW ENFORCEMENT OR NATIONAL SECURITY PUR-  
17 POSES.—

18 (A) LAW ENFORCEMENT.—If a Federal or  
19 State law enforcement agency, including an at-  
20 torney general of a State, determines that the  
21 notification required under this section would  
22 impede a civil or criminal investigation, such  
23 notification shall be delayed upon the written  
24 request of the law enforcement agency for 30  
25 days or such lesser period of time which the law

1 enforcement agency determines is reasonably  
2 necessary and requests in writing. Such a law  
3 enforcement agency may, by a subsequent writ-  
4 ten request, revoke such delay or extend the pe-  
5 riod of time set forth in the original request  
6 made under this paragraph if further delay is  
7 necessary.

8 (B) NATIONAL SECURITY.—If a Federal  
9 national security agency or homeland security  
10 agency determines that the notification required  
11 under this section would threaten national or  
12 homeland security, such notification may be de-  
13 layed for a period of time which the national se-  
14 curity agency or homeland security agency de-  
15 termines is reasonably necessary and requests  
16 in writing. A Federal national security agency  
17 or homeland security agency may revoke such  
18 delay or extend the period of time set forth in  
19 the original request made under this paragraph  
20 by a subsequent written request if further delay  
21 is necessary.

22 (d) METHOD AND CONTENT OF NOTIFICATION.—

23 (1) DIRECT NOTIFICATION.—

24 (A) METHOD OF NOTIFICATION.—A person  
25 required to provide notification to individuals

1 under subsection (a)(1) shall be in compliance  
2 with such requirement if the person provides  
3 conspicuous and clearly identified notification  
4 by one of the following methods (provided the  
5 selected method can reasonably be expected to  
6 reach the intended individual):

7 (i) Written notification.

8 (ii) Notification by email or other  
9 electronic means, if—

10 (I) the person's primary method  
11 of communication with the individual  
12 is by email or such other electronic  
13 means; or

14 (II) the individual has consented  
15 to receive such notification and the  
16 notification is provided in a manner  
17 that is consistent with the provisions  
18 permitting electronic transmission of  
19 notices under section 101 of the Elec-  
20 tronic Signatures in Global and Na-  
21 tional Commerce Act (15 U.S.C.  
22 7001).

23 (B) CONTENT OF NOTIFICATION.—Regard-  
24 less of the method by which notification is pro-

1           vided to an individual under subparagraph (A),  
2           such notification shall include—

3                   (i) a description of the personal infor-  
4                   mation that was acquired or accessed by  
5                   an unauthorized person;

6                   (ii) a telephone number that the indi-  
7                   vidual may use, at no cost to such indi-  
8                   vidual, to contact the person to inquire  
9                   about the breach of security or the infor-  
10                  mation the person maintained about that  
11                  individual;

12                  (iii) notice that the individual is enti-  
13                  tled to receive, at no cost to such indi-  
14                  vidual, consumer credit reports on a quar-  
15                  terly basis for a period of 2 years, or credit  
16                  monitoring or other service that enables  
17                  consumers to detect the misuse of their  
18                  personal information for a period of 2  
19                  years, and instructions to the individual on  
20                  requesting such reports or service from the  
21                  person, except when the only information  
22                  which has been the subject of the security  
23                  breach is the individual's first name or ini-  
24                  tial and last name, or address, or phone  
25                  number, in combination with a credit or

1 debit card number, and any required secu-  
2 rity code;

3 (iv) the toll-free contact telephone  
4 numbers and addresses for the major con-  
5 sumer reporting agencies; and

6 (v) a toll-free telephone number and  
7 Internet website address for the Commis-  
8 sion whereby the individual may obtain in-  
9 formation regarding identity theft.

10 (2) SUBSTITUTE NOTIFICATION.—

11 (A) CIRCUMSTANCES GIVING RISE TO SUB-  
12 STITUTE NOTIFICATION.—A person required to  
13 provide notification to individuals under sub-  
14 section (a)(1) may provide substitute notifica-  
15 tion in lieu of the direct notification required by  
16 paragraph (1) if the person owns or possesses  
17 data containing personal information of fewer  
18 than 1,000 individuals and such direct notifica-  
19 tion is not feasible due to—

20 (i) excessive cost to the person re-  
21 quired to provide such notification relative  
22 to the resources of such person, as deter-  
23 mined in accordance with the regulations  
24 issued by the Commission under paragraph  
25 (3)(A); or

1 (ii) lack of sufficient contact informa-  
2 tion for the individual required to be noti-  
3 fied.

4 (B) FORM OF SUBSTITUTE NOTIFICA-  
5 TION.—Such substitute notification shall in-  
6 clude—

7 (i) email notification to the extent  
8 that the person has email addresses of in-  
9 dividuals to whom it is required to provide  
10 notification under subsection (a)(1);

11 (ii) a conspicuous notice on the Inter-  
12 net website of the person (if such person  
13 maintains such a website); and

14 (iii) notification in print and to broad-  
15 cast media, including major media in met-  
16 ropolitan and rural areas where the indi-  
17 viduals whose personal information was ac-  
18 quired reside.

19 (C) CONTENT OF SUBSTITUTE NOTICE.—  
20 Each form of substitute notice under this para-  
21 graph shall include—

22 (i) notice that individuals whose per-  
23 sonal information is included in the breach  
24 of security are entitled to receive, at no  
25 cost to the individuals, consumer credit re-

1                   ports on a quarterly basis for a period of  
2                   2 years, or credit monitoring or other serv-  
3                   ice that enables consumers to detect the  
4                   misuse of their personal information for a  
5                   period of 2 years, and instructions on re-  
6                   questing such reports or service from the  
7                   person, except when the only information  
8                   which has been the subject of the security  
9                   breach is the individual's first name or ini-  
10                  tial and last name, or address, or phone  
11                  number, in combination with a credit or  
12                  debit card number, and any required secu-  
13                  rity code; and

14                         (ii) a telephone number by which an  
15                         individual can, at no cost to such indi-  
16                         vidual, learn whether that individual's per-  
17                         sonal information is included in the breach  
18                         of security.

19                   (3) REGULATIONS AND GUIDANCE.—

20                         (A) REGULATIONS.—Not later than 1 year  
21                         after the date of enactment of this Act, the  
22                         Commission shall, by regulation under section  
23                         553 of title 5, United States Code, establish cri-  
24                         teria for determining circumstances under  
25                         which substitute notification may be provided

1 under paragraph (2), including criteria for de-  
2 termining if notification under paragraph (1) is  
3 not feasible due to excessive costs to the person  
4 required to provide such notification relative to  
5 the resources of such person. Such regulations  
6 may also identify other circumstances where  
7 substitute notification would be appropriate for  
8 any person, including circumstances under  
9 which the cost of providing notification exceeds  
10 the benefits to consumers.

11 (B) GUIDANCE.—In addition, the Commis-  
12 sion shall provide and publish general guidance  
13 with respect to compliance with this subsection.  
14 Such guidance shall include—

15 (i) a description of written or email  
16 notification that complies with the require-  
17 ments of paragraph (1); and

18 (ii) guidance on the content of sub-  
19 stitute notification under paragraph (2),  
20 including the extent of notification to print  
21 and broadcast media that complies with  
22 the requirements of such paragraph.

23 (e) OTHER OBLIGATIONS FOLLOWING BREACH.—

24 (1) IN GENERAL.—A person required to provide  
25 notification under subsection (a) shall, upon request

1 of an individual whose personal information was in-  
2 cluded in the breach of security, provide or arrange  
3 for the provision of, to each such individual and at  
4 no cost to such individual—

5 (A) consumer credit reports from at least  
6 one of the major consumer reporting agencies  
7 beginning not later than 30 days following the  
8 individual's request and continuing on a quar-  
9 terly basis for a period of 2 years thereafter; or

10 (B) a credit monitoring or other service  
11 that enables consumers to detect the misuse of  
12 their personal information, beginning not later  
13 than 30 days following the individual's request  
14 and continuing for a period of 2 years.

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

21 (3) RULEMAKING.—As part of the Commis-  
22 sion's rulemaking described in subsection (d)(3), the  
23 Commission shall determine the circumstances under  
24 which a person required to provide notification  
25 under subsection (a)(1) shall provide or arrange for

1 the provision of free consumer credit reports or cred-  
2 it monitoring or other service to affected individuals.

3 (f) EXEMPTION.—

4 (1) GENERAL EXEMPTION.—A person shall be  
5 exempt from the requirements under this section if,  
6 following a breach of security, and consultation with  
7 the Commission, it is determined that the affected  
8 data is unusable, unreadable, or indecipherable.

9 (2) PRESUMPTION.—

10 (A) IN GENERAL.—If the data containing  
11 personal information is rendered unusable,  
12 unreadable, or indecipherable through  
13 encryption or other security technology or meth-  
14 odology (if the method of encryption or such  
15 other technology or methodology is generally ac-  
16 cepted by experts in the information security  
17 field), there shall be a presumption that no rea-  
18 sonable risk of identity theft, fraud, or other  
19 unlawful conduct exists following a breach of  
20 security of such data. Any such presumption  
21 may be rebutted by facts demonstrating that  
22 the encryption or other security technologies or  
23 methodologies in a specific case, have been or  
24 are reasonably likely to be compromised.

1           (B)     METHODOLOGIES     OR     TECH-  
2           NOLOGIES.—Not later than 1 year after the  
3           date of the enactment of this Act and bian-  
4           nually thereafter, the Commission shall issue  
5           rules (pursuant to section 553 of title 5, United  
6           States Code) or guidance to identify security  
7           methodologies or technologies which render data  
8           unusable, unreadable, or indecipherable, that  
9           shall, if applied to such data, establish a pre-  
10          sumption that no reasonable risk of identity  
11          theft, fraud, or other unlawful conduct exists  
12          following a breach of security of such data. Any  
13          such presumption may be rebutted by facts  
14          demonstrating that any such methodology or  
15          technology in a specific case has been or is rea-  
16          sonably likely to be compromised. In issuing  
17          such rules or guidance, the Commission shall  
18          consult with relevant industries, consumer orga-  
19          nizations, and data security and identity theft  
20          prevention experts and established standards  
21          setting bodies.

22          (3) FTC GUIDANCE.—Not later than 1 year  
23          after the date of the enactment of this Act the Com-  
24          mission shall issue guidance regarding the applica-  
25          tion of the exemption in paragraph (1).

1 (g) WEBSITE NOTICE OF FEDERAL TRADE COMMIS-  
2 SION.—If the Commission, upon receiving notification of  
3 any breach of security that is reported to the Commission  
4 under subsection (a)(2), finds that notification of such a  
5 breach of security via the Commission’s Internet website  
6 would be in the public interest or for the protection of  
7 consumers, the Commission shall place such a notice in  
8 a clear and conspicuous location on its Internet website.

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

16 (i) GENERAL RULEMAKING AUTHORITY.—

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

21 (2) LIMITATION.—In promulgating rules under  
22 this Act, the Commission shall not require the de-  
23 ployment or use of any specific products or tech-  
24 nologies, including any specific computer software or  
25 hardware.

1 (j) TREATMENT OF PERSONS GOVERNED BY OTHER  
2 LAW.—A person who is in compliance with any other Fed-  
3 eral law that requires such person to provide notification  
4 to individuals following a breach of security, and that,  
5 taken as a whole, provides protections substantially similar  
6 to, or greater than, those required under this section, as  
7 the Commission shall determine by rule (under section  
8 553 of title 5, United States Code), shall be deemed to  
9 be in compliance with this section.

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

11 (a) GENERAL APPLICATION.—The requirements of  
12 sections 2 and 3 shall apply to—

13 (1) those persons, partnerships, or corporations  
14 over which the Commission has authority pursuant  
15 to section 5(a)(2) of the Federal Trade Commission  
16 Act (15 U.S.C. 45(a)(2));

17 (2) notwithstanding section 5(a)(2) of the Fed-  
18 eral Trade Commission Act (15 U.S.C. 45(a)(2)),  
19 common carriers subject to the Communications Act  
20 of 1934 (47 U.S.C. 151 et seq.); and

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

1       taxation under section 501(a) of the Internal Rev-  
2       enue Code of 1986.

3       (b) ENFORCEMENT BY THE FEDERAL TRADE COM-  
4       MISSION.—

5           (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-  
6       TICES.—A violation of section 2 or 3 shall be treated  
7       as an unfair and deceptive act or practice in viola-  
8       tion of a regulation under section 18(a)(1)(B) of the  
9       Federal Trade Commission Act (15 U.S.C.  
10      57a(a)(1)(B)) regarding unfair or deceptive acts or  
11      practices.

12          (2) POWERS OF COMMISSION.—The Commis-  
13      sion shall enforce this Act in the same manner, by  
14      the same means, and with the same jurisdiction,  
15      powers, and duties as though all applicable terms  
16      and provisions of the Federal Trade Commission Act  
17      (15 U.S.C. 41 et seq.) were incorporated into and  
18      made a part of this Act. Any person who violates  
19      such regulations shall be subject to the penalties and  
20      entitled to the privileges and immunities provided in  
21      that Act.

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

24          (1) CIVIL ACTION.—In any case in which the  
25      attorney general of a State, or an official or agency

1 of a State, has reason to believe that an interest of  
2 the residents of that State has been or is threatened  
3 or adversely affected by any person who violates sec-  
4 tion 2 or 3 of this Act, the attorney general, official,  
5 or agency of the State, as *parens patriae*, may bring  
6 a civil action on behalf of the residents of the State  
7 in a district court of the United States of appro-  
8 priate jurisdiction—

9 (A) to enjoin further violation of such sec-  
10 tion by the defendant;

11 (B) to compel compliance with such sec-  
12 tion; or

13 (C) to obtain civil penalties in the amount  
14 determined under paragraph (2).

15 (2) CIVIL PENALTIES.—

16 (A) CALCULATION.—

17 (i) TREATMENT OF VIOLATIONS OF  
18 SECTION 2.—For purposes of paragraph  
19 (1)(C) with regard to a violation of section  
20 2, the amount determined under this para-  
21 graph is the amount calculated by multi-  
22 plying the number of days that a person is  
23 not in compliance with such section by an  
24 amount not greater than \$11,000.

1 (ii) TREATMENT OF VIOLATIONS OF  
2 SECTION 3.—For purposes of paragraph  
3 (1)(C) with regard to a violation of section  
4 3, the amount determined under this para-  
5 graph is the amount calculated by multi-  
6 plying the number of violations of such  
7 section by an amount not greater than  
8 \$11,000. Each failure to send notification  
9 as required under section 3 to a resident of  
10 the State shall be treated as a separate  
11 violation.

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

22 (C) MAXIMUM TOTAL LIABILITY.—Not-  
23 withstanding the number of actions which may  
24 be brought against a person under this sub-  
25 section, the maximum civil penalty for which

1 any person may be liable under this subsection  
2 shall not exceed—

3 (i) \$5,000,000 for each violation of  
4 section 2; and

5 (ii) \$5,000,000 for all violations of  
6 section 3 resulting from a single breach of  
7 security.

8 (3) INTERVENTION BY THE FTC.—

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

18 (i) to intervene in the action;

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

21 (iii) to file petitions for appeal.

22 (B) LIMITATION ON STATE ACTION WHILE  
23 FEDERAL ACTION IS PENDING.—If the Commis-  
24 sion has instituted a civil action for violation of  
25 this Act, no State attorney general, or official

1 or agency of a State, may bring an action under  
2 this subsection during the pendency of that ac-  
3 tion against any defendant named in the com-  
4 plaint of the Commission for any violation of  
5 this Act alleged in the complaint.

6 (4) CONSTRUCTION.—For purposes of bringing  
7 any civil action under paragraph (1), nothing in this  
8 Act shall be construed to prevent an attorney gen-  
9 eral of a State from exercising the powers conferred  
10 on the attorney general by the laws of that State  
11 to—

12 (A) conduct investigations;

13 (B) administer oaths or affirmations; or

14 (C) compel the attendance of witnesses or  
15 the production of documentary and other evi-  
16 dence.

17 (d) AFFIRMATIVE DEFENSE FOR A VIOLATION OF  
18 SECTION 3.—

19 (1) IN GENERAL.—It shall be an affirmative de-  
20 fense to an enforcement action brought under sub-  
21 section (b), or a civil action brought under sub-  
22 section (c), based on a violation of section 3, that all  
23 of the personal information contained in the data  
24 that was acquired or accessed as a result of a breach  
25 of security of the defendant is public record informa-

1           tion that is lawfully made available to the general  
2           public from Federal, State, or local government  
3           records and was acquired by the defendant from  
4           such records.

5           (2) NO EFFECT ON OTHER REQUIREMENTS.—  
6           Nothing in this subsection shall be construed to ex-  
7           empt any person from the requirement to notify the  
8           Commission of a breach of security as required  
9           under section 3(a).

10 **SEC. 5. DEFINITIONS.**

11           In this Act, the following definitions apply:

12           (1) BREACH OF SECURITY.—The term “breach  
13           of security” means the unauthorized acquisition of  
14           data containing personal information.

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

17           (3) CONSUMER REPORTING AGENCY.—The term  
18           “consumer reporting agency” has the meaning given  
19           the term “consumer reporting agency that compiles  
20           and maintains files on consumers on a nationwide  
21           basis” in section 603(p) of the Fair Credit Report-  
22           ing Act (15 U.S.C. 1681a(p)).

23           (4) DATA IN ELECTRONIC FORM.—The term  
24           “data in electronic form” means any data stored  
25           electronically or digitally on any computer system or

1 other database and includes recordable tapes and  
2 other mass storage devices.

3 (5) ENCRYPTION.—The term “encryption”  
4 means the protection of data in electronic form in  
5 storage or in transit using an encryption technology  
6 that has been adopted by an established standards  
7 setting body which renders such data indecipherable  
8 in the absence of associated cryptographic keys nec-  
9 essary to enable decryption of such data. Such  
10 encryption must include appropriate management  
11 and safeguards of such keys to protect the integrity  
12 of the encryption.

13 (6) IDENTITY THEFT.—The term “identity  
14 theft” means the unauthorized use of another per-  
15 son’s personal information for the purpose of engag-  
16 ing in commercial transactions under the name of  
17 such other person.

18 (7) 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 such third party to enable such third party  
12 to (1) provide benefits for its employees or (2)  
13 directly transact business with its customers.

14 (8) PERSONAL INFORMATION.—

15 (A) DEFINITION.—The term “personal in-  
16 formation” means an individual’s first name or  
17 initial and last name, or address, or phone  
18 number, in combination with any 1 or more of  
19 the following data elements for that individual:

20 (i) Social Security number.

21 (ii) Driver’s license number, passport  
22 number, military identification number, or  
23 other similar number issued on a govern-  
24 ment document used to verify identity.

1 (iii) Financial account number, or  
2 credit or debit card number, and any re-  
3 quired security code, access code, or pass-  
4 word that is necessary to permit access to  
5 an individual's financial account.

6 (iv) Unique biometric data such as  
7 fingerprint, voice print, a retina or iris  
8 image, or any other unique physical rep-  
9 resentation.

10 (v) Health insurance number in com-  
11 bination with the individual's first and last  
12 name, first initial and last name, or other  
13 unique identifier.

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

18 (vii) The individual's month, day, and  
19 year of birth or mother's maiden name

20 (viii) The individual's precise  
21 geolocation;

22 (ix) Information that relates to the in-  
23 dividual's past, present, or future physical  
24 or mental health or condition, or to the

1 provision of health care to the individual  
2 (other than health insurance number);

3 (x) The individual's non-public com-  
4 munications or other user-created content  
5 such as e-mails, photographs, or videos.

6 (xi) Any additional element the Com-  
7 mission defines as personal information.

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

13 (i) for the purpose of section 2 to the  
14 extent that such modification will not un-  
15 reasonably impede interstate commerce,  
16 and will accomplish the purposes of this  
17 Act; or

18 (ii) for the purpose of section 3, to the  
19 extent that such modification is necessary  
20 to accommodate changes in technology or  
21 practices, will not unreasonably impede  
22 interstate commerce, and will accomplish  
23 the purposes of this Act.

24 (9) PUBLIC RECORD INFORMATION.—The term  
25 “public record information” means information

1 about an individual which has been obtained origi-  
2 nally from records of a Federal, State, or local gov-  
3 ernment entity that are available for public inspec-  
4 tion.

5 (10) NON-PUBLIC INFORMATION.—The term  
6 “non-public information” means information about  
7 an individual that is of a private nature and neither  
8 available to the general public nor obtained from a  
9 public record.

10 (11) SERVICE PROVIDER.—The term “service  
11 provider” means an entity that provides to a user  
12 transmission, routing, intermediate and transient  
13 storage, or connections to its system or network, for  
14 electronic communications, between or among points  
15 specified by such user of material of the user’s  
16 choosing, without modification to the content of the  
17 material as sent or received. Any such entity shall  
18 be treated as a service provider under this Act only  
19 to the extent that it is engaged in the provision of  
20 such transmission, routing, intermediate and tran-  
21 sient storage or connections.

22 (12) STATE.—The term “State” means any of  
23 the several States, the District of Columbia, Amer-  
24 ican Samoa, Guam, the Commonwealth of the  
25 Northern Mariana Islands, the Commonwealth of

1 Puerto Rico, the United States Virgin Islands, any  
2 other territory or possession of the United States,  
3 and each federally recognized Indian tribe.

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

5 (a) **PREEMPTION OF STATE INFORMATION SECURITY**  
6 **LAWS.**—This Act supersedes any provision of a statute or  
7 regulation of a State or political subdivision of a State,  
8 with respect to those entities covered by the regulations  
9 issued pursuant to this Act, that expressly—

10 (1) requires information security practices and  
11 treatment of data containing personal information  
12 similar to any of those required under section 2; or

13 (2) requires notification to individuals of a  
14 breach of security resulting in unauthorized access  
15 to or acquisition of data in electronic form con-  
16 taining personal information.

17 (b) **ADDITIONAL PREEMPTION.**—

18 (1) **IN GENERAL.**—No person other than a per-  
19 son specified in section 4(c) may bring a civil action  
20 under the laws of any State if such action is pre-  
21 mised in whole or in part upon the defendant vio-  
22 lating any provision of this Act.

23 (2) **PROTECTION OF CONSUMER PROTECTION**  
24 **LAWS.**—This subsection shall not be construed to

1       limit the enforcement of any State consumer protec-  
2       tion law by an attorney general of a State.

3       (c) PROTECTION OF CERTAIN STATE LAWS.—This  
4 Act shall not be construed to preempt the applicability  
5 of—

6           (1) State trespass, contract, or tort law; or

7           (2) other State laws to the extent that those  
8 laws relate to acts of fraud.

9       (d) PRESERVATION OF FTC AUTHORITY.—Nothing  
10 in this Act may be construed in any way to limit the Com-  
11 mission's authority under any other provision of law.

12 **SEC. 7. EFFECTIVE DATE.**

13       This Act shall take effect 1 year after the date of  
14 enactment of this Act.

15 **SEC. 8. AUTHORIZATION OF APPROPRIATIONS.**

16       There is authorized to be appropriated to the Com-  
17 mission \$1,000,000 for each of fiscal years 2015 through  
18 2020 to carry out this Act.

