

**AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 2221
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 obsolete
9 data in electronic form containing personal in-
10 formation by shredding, permanently erasing,
11 or otherwise modifying the personal information
12 contained in such data to make such personal
13 information permanently unreadable or
14 undecipherable.

15 (F) A standard method or methods for the
16 destruction of obsolete paper documents and
17 other non-electronic data containing personal
18 information by persons engaged in interstate
19 commerce who own or possess such paper docu-
20 ments and non-electronic data if the Commis-
21 sion finds that—

22 (i) the improper disposal of obsolete
23 paper documents and other non-electronic
24 data creates a reasonable risk of identity
25 theft, fraud, or other unlawful conduct;

1 (ii) such a requirement would be ef-
2 fective in preventing identity theft, fraud,
3 or other unlawful conduct;

4 (iii) the benefit in preventing identity
5 theft, fraud, or other unlawful conduct
6 would outweigh the cost to persons subject
7 to such a requirement; and

8 (iv) compliance with such a require-
9 ment would be practicable.

10 (3) TREATMENT OF ENTITIES GOVERNED BY
11 OTHER LAW.—In promulgating the regulations
12 under this subsection, the Commission shall deter-
13 mine to be in compliance with this subsection any
14 person who is in compliance with any other Federal
15 law that requires such person to maintain standards
16 and safeguards for information security and protec-
17 tion of personal information that, taken as a whole,
18 provide protections substantially similar to, or great-
19 er than, those required under this subsection.

20 (b) SPECIAL REQUIREMENTS FOR INFORMATION
21 BROKERS.—

22 (1) SUBMISSION OF POLICIES TO THE FTC.—
23 The regulations promulgated under subsection (a)
24 shall require information brokers to submit its secu-
25 rity policies to the Commission in conjunction with

1 a notification of a breach of security under section
2 3 or upon request of the Commission.

3 (2) POST-BREACH AUDIT.—For any information
4 broker required to provide notification under section
5 3, the Commission may conduct an audit of the in-
6 formation security practices of such information
7 broker, or require the information broker to conduct
8 an independent audit of such practices (by an inde-
9 pendent auditor who has not audited such informa-
10 tion broker's security practices during the preceding
11 5 years). The Commission may conduct or require
12 additional audits for a period of 5 years following
13 the breach of security or until the Commission deter-
14 mines that the security practices of the information
15 broker are in compliance with the requirements of
16 this section and are adequate to prevent further
17 breaches of security.

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

20 (A) ACCURACY.—

21 (i) IN GENERAL.—Each information
22 broker shall establish reasonable proce-
23 dures to assure the maximum possible ac-
24 curacy of the personal information it col-
25 lects, assembles, or maintains, and any

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

6 (ii) LIMITED EXCEPTION FOR FRAUD
7 DATABASES.—The requirement in clause
8 (i) shall not prevent the maintenance of in-
9 formation that may be inaccurate with re-
10 spect to a particular individual, but that is
11 associated with identity theft or other un-
12 lawful conduct, so long as such information
13 is flagged or otherwise identified as inac-
14 curate information to be used for fraud de-
15 tection or investigation purposes.

16 (B) CONSUMER ACCESS TO INFORMA-
17 TION.—

18 (i) ACCESS.—Each information broker
19 shall—

20 (I) provide to each individual
21 whose personal information it main-
22 tains, at the individual's request at
23 least 1 time per year and at no cost
24 to the individual, and after verifying
25 the identity of such individual, a

1 means for the individual to review any
2 personal information regarding such
3 individual maintained by the informa-
4 tion broker and any other information
5 maintained by the information broker
6 that specifically identifies such indi-
7 vidual, other than information which
8 merely identifies an individual's name
9 or address; and

10 (II) place a conspicuous notice on
11 its Internet website (if the informa-
12 tion broker maintains such a website)
13 instructing individuals how to request
14 access to the information required to
15 be provided under subclause (I).

16 (ii) DISPUTED INFORMATION.—When-
17 ever an individual whose information the
18 information broker maintains makes a
19 written request disputing the accuracy of
20 any such information, the information
21 broker, after verifying the identity of the
22 individual making such request and unless
23 there are reasonable grounds to believe
24 such request is frivolous or irrelevant,
25 shall—

1 (I) correct any inaccuracy; or

2 (II)(aa) in the case of informa-
3 tion that is public record information,
4 inform the individual of the source of
5 the information, and, if reasonably
6 available, where a request for correc-
7 tion may be directed and, if the indi-
8 vidual provides proof that the public
9 record has been corrected or that the
10 information broker was reporting the
11 information incorrectly, correct the in-
12 accuracy in the information broker's
13 records; or

14 (bb) in the case of information
15 that is non-public information, note
16 the information that is disputed, in-
17 cluding the individual's statement dis-
18 puting such information, and take
19 reasonable steps to independently
20 verify such information under the pro-
21 cedures outlined in subparagraph (A)
22 if such information can be independ-
23 ently verified.

24 (iii) LIMITATIONS.—An information
25 broker may limit the access to information

1 required under subparagraph (B) in the
2 following circumstances:

3 (I) If access of the individual to
4 the information is limited by law or
5 legally recognized privilege.

6 (II) If the information is used for
7 a legitimate governmental or fraud
8 prevention purpose that would be
9 compromised by such access.

10 (III) If the information consists
11 of a published media record, unless
12 that record has been included in a re-
13 port about an individual shared with a
14 third party.

15 (iv) RULEMAKING.—Not later than 1
16 year after the date of the enactment of this
17 Act, the Commission shall promulgate reg-
18 ulations under section 553 of title 5,
19 United States Code, to carry out this para-
20 graph and to facilitate the purposes of this
21 Act. In addition, the Commission shall
22 issue regulations, as necessary, under sec-
23 tion 553 of title 5, United States Code,
24 on—

1 (I) the scope of the application of
2 the limitations in clause (iii); and

3 (II) any additional circumstances
4 in which an information broker may
5 limit access to information under
6 clause (iii), that the Commission de-
7 termines would be appropriate.

8 (C) FCRA REGULATED PERSONS.—Any in-
9 formation broker who is determined to be in
10 compliance with the Fair Credit Reporting Act
11 and its implementing regulations shall be con-
12 sidered to be in compliance with this paragraph
13 with respect to the activities that are regulated
14 by such Act.

15 (4) REQUIREMENT OF AUDIT LOG OF ACCESSED
16 AND TRANSMITTED INFORMATION.—Not later than
17 1 year after the date of the enactment of this Act,
18 the Commission shall promulgate regulations under
19 section 553 of title 5, United States Code, to require
20 information brokers to establish measures which fa-
21 cilitate the auditing or retracing of any internal or
22 external access to, or transmissions of, any data con-
23 taining personal information collected, assembled, or
24 maintained by such information broker.

1 (5) PROHIBITION ON PRETEXTING BY INFOR-
2 MATION BROKERS.—

3 (A) PROHIBITION ON OBTAINING PER-
4 SONAL INFORMATION BY FALSE PRETENSES.—

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

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

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

20 (B) PROHIBITION ON SOLICITATION TO
21 OBTAIN PERSONAL INFORMATION UNDER FALSE
22 PRETENSES.—It shall be unlawful for an infor-
23 mation broker to request a person to obtain
24 personal information or any other information
25 relating to any other person, if the information

1 broker knew or should have known that the per-
2 son to whom such a request is made will obtain
3 or attempt to obtain such information in the
4 manner described in subsection (a).

5 (c) EXEMPTION FOR TELECOMMUNICATIONS CAR-
6 RIER, CABLE OPERATOR, INFORMATION SERVICE, OR
7 INTERACTIVE COMPUTER SERVICE.—Nothing in this sec-
8 tion shall apply to any electronic communication by a third
9 party stored by a telecommunications carrier, cable oper-
10 ator, or information service, as those terms are defined
11 in section 3 of the Communications Act of 1934 (47
12 U.S.C. 153), or an interactive computer service, as such
13 term is defined in section 230(f)(2) of such Act (47 U.S.C.
14 230(f)(2)).

15 **SEC. 3. NOTIFICATION OF INFORMATION SECURITY**
16 **BREACH.**

17 (a) NATIONWIDE NOTIFICATION.—Any person en-
18 gaged in interstate commerce that owns or possesses data
19 in electronic form containing personal information shall,
20 following the discovery of a breach of security of the sys-
21 tem maintained by such person that contains such data—

22 (1) notify each individual who is a citizen or
23 resident of the United States whose personal infor-
24 mation was acquired by an unauthorized person as
25 a result of such a breach of security; and

1 (2) notify the Commission.

2 (b) SPECIAL NOTIFICATION REQUIREMENTS.—

3 (1) THIRD PARTY AGENTS.—In the event of a
4 breach of security by any third party entity that has
5 been contracted to maintain or process data in elec-
6 tronic form containing personal information on be-
7 half of any other person who owns or possesses such
8 data, such third party entity shall be required to no-
9 tify such person of the breach of security. Upon re-
10 ceiving such notification from such third party, such
11 person shall provide the notification required under
12 subsection (a).

13 (2) TELECOMMUNICATIONS CARRIERS, CABLE
14 OPERATORS, INFORMATION SERVICES, AND INTER-
15 ACTIVE COMPUTER SERVICES.—If a telecommuni-
16 cations carrier, cable operator, or information service
17 (as such terms are defined in section 3 of the Com-
18 munications Act of 1934 (47 U.S.C. 153)), or an
19 interactive computer service (as such term is defined
20 in section 230(f)(2) of such Act (47 U.S.C.
21 230(f)(2))), becomes aware of a breach of security
22 during the transmission of data in electronic form
23 containing personal information that is owned or
24 possessed by another person utilizing the means of
25 transmission of such telecommunications carrier,

1 cable operator, information service, or interactive
2 computer service, such telecommunications carrier,
3 cable operator, information service, or interactive
4 computer service shall be required only to notify the
5 person who initiated such transmission of such a
6 breach of security if such person can be reasonably
7 identified. Upon receiving such notification from a
8 telecommunications carrier, cable operator, informa-
9 tion service, or interactive computer service, such
10 person shall provide the notification required under
11 subsection (a).

12 (3) BREACH OF HEALTH INFORMATION.— If
13 the Commission receives a notification of a breach of
14 security and determines that information included in
15 such breach is individually identifiable health infor-
16 mation (as such term is defined in section 1171(6)
17 of the Social Security Act (42 U.S.C. 1320d(6)), the
18 Commission shall send a copy of such notification to
19 the Secretary of Health and Human Services.

20 (4) COORDINATION OF NOTIFICATION WITH
21 CREDIT REPORTING AGENCIES.—If a person is re-
22 quired to provide notification to more than 5,000 in-
23 dividuals under subsection (a)(1), the person shall
24 also notify the major credit reporting agencies that
25 compile and maintain files on consumers on a na-

1 tionwide basis, of the timing and distribution of the
2 notices. Such notice shall be given to the credit re-
3 porting agencies without unreasonable delay and, if
4 it will not delay notice to the affected individuals,
5 prior to the distribution of notices to the affected in-
6 dividuals.

7 (c) TIMELINESS OF NOTIFICATION.—

8 (1) IN GENERAL.—All notifications required
9 under subsection (a) shall be made as promptly as
10 possible and without unreasonable delay following
11 the discovery of a breach of security of the system
12 and consistent with any measures necessary to de-
13 termine the scope of the breach, prevent further
14 breach or unauthorized disclosures, and reasonably
15 restore the integrity of the data system.

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

19 (A) LAW ENFORCEMENT.—If a Federal,
20 State, or local law enforcement agency deter-
21 mines that the notification required under this
22 section would impede a civil or criminal inves-
23 tigation, such notification shall be delayed upon
24 the written request of the law enforcement
25 agency for 30 days or such lesser period of time

1 which the law enforcement agency determines is
2 reasonably necessary and requests in writing. A
3 law enforcement agency may, by a subsequent
4 written request, revoke such delay or extend the
5 period 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 extend the pe-
18 riod of time set forth in the original request
19 made under this paragraph by a subsequent
20 written request if further delay is necessary.

21 (d) METHOD AND CONTENT OF NOTIFICATION.—

22 (1) DIRECT NOTIFICATION.—

23 (A) METHOD OF NOTIFICATION.—A person
24 required to provide notification to individuals
25 under subsection (a)(1) shall be in compliance

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

6 (i) Written notification.

7 (ii) Email notification, if—

8 (I) the person's primary method
9 of communication with the individual
10 is by email; or

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

19 (B) CONTENT OF NOTIFICATION.—Regard-
20 less of the method by which notification is pro-
21 vided to an individual under subparagraph (A),
22 such notification shall include—

23 (i) a description of the personal infor-
24 mation that was acquired by an unauthor-
25 ized person;

1 (ii) a telephone number that the indi-
2 vidual may use, at no cost to such indi-
3 vidual, to contact the person to inquire
4 about the breach of security or the infor-
5 mation the person maintained about that
6 individual;

7 (iii) notice that the individual is enti-
8 tled to receive, at no cost to such indi-
9 vidual, consumer credit reports on a quar-
10 terly basis for a period of 2 years, and in-
11 structions to the individual on requesting
12 such reports from the person, except when
13 the only information which has been the
14 subject of the security breach is the indi-
15 vidual's first name or initial and last
16 name, or address, or phone number, in
17 combination with a credit or debit card
18 number, and any required security code;

19 (iv) the toll-free contact telephone
20 numbers and addresses for the major cred-
21 it reporting agencies; and

22 (v) a toll-free telephone number and
23 Internet website address for the Commis-
24 sion whereby the individual may obtain in-
25 formation regarding identity theft.

1 (2) SUBSTITUTE NOTIFICATION.—

2 (A) CIRCUMSTANCES GIVING RISE TO SUB-
3 STITUTE NOTIFICATION.—A person required to
4 provide notification to individuals under sub-
5 section (a)(1) may provide substitute notifica-
6 tion in lieu of the direct notification required by
7 paragraph (1) if—

8 (i) the person owns or possesses data
9 in electronic form containing personal in-
10 formation of fewer than 1,000 individuals;
11 and

12 (ii) such direct notification is not fea-
13 sible due to—

14 (I) excessive cost to the person
15 required to provide such notification
16 relative to the resources of such per-
17 son, as determined in accordance with
18 the regulations issued by the Commis-
19 sion under paragraph (3)(A); or

20 (II) lack of sufficient contact in-
21 formation for the individual required
22 to be notified.

23 (B) FORM OF SUBSTITUTE NOTIFICA-
24 TION.—Such substitute notification shall in-
25 clude—

1 (i) email notification to the extent
2 that the person has email addresses of in-
3 dividuals to whom it is required to provide
4 notification under subsection (a)(1);

5 (ii) a conspicuous notice on the Inter-
6 net website of the person (if such person
7 maintains such a website); and

8 (iii) notification in print and to broad-
9 cast media, including major media in met-
10 ropolitan and rural areas where the indi-
11 viduals whose personal information was ac-
12 quired reside.

13 (C) CONTENT OF SUBSTITUTE NOTICE.—
14 Each form of substitute notice under this para-
15 graph shall include—

16 (i) notice that individuals whose per-
17 sonal information is included in the breach
18 of security are entitled to receive, at no
19 cost to the individuals, consumer credit re-
20 ports on a quarterly basis for a period of
21 2 years, and instructions on requesting
22 such reports from the person, except when
23 the only information which has been the
24 subject of the security breach is the indi-
25 vidual's first name or initial and last

1 name, or address, or phone number, in
2 combination with a credit or debit card
3 number, and any required security code;
4 and

5 (ii) a telephone number by which an
6 individual can, at no cost to such indi-
7 vidual, learn whether that individual's per-
8 sonal information is included in the breach
9 of security.

10 (3) FEDERAL TRADE COMMISSION REGULA-
11 TIONS AND GUIDANCE.—

12 (A) REGULATIONS.—Not later than 1 year
13 after the date of enactment of this Act, the
14 Commission shall, by regulations under section
15 553 of title 5, United States Code, establish cri-
16 teria for determining the circumstances under
17 which substitute notification may be provided
18 under paragraph (2), including criteria for de-
19 termining if notification under paragraph (1) is
20 not feasible due to excessive cost to the person
21 required to provide such notification relative to
22 the resources of such person.

23 (B) GUIDANCE.—In addition, the Commis-
24 sion shall provide and publish general guidance

1 with respect to compliance with this section.

2 Such guidance shall include—

3 (i) a description of written or email
4 notification that complies with the require-
5 ments of paragraph (1); and

6 (ii) guidance on the content of sub-
7 stitute notification under paragraph
8 (2)(B), including the extent of notification
9 to print and broadcast media that complies
10 with the requirements of such paragraph.

11 (e) OTHER OBLIGATIONS FOLLOWING BREACH.—A
12 person required to provide notification under subsection
13 (a) shall, upon request of an individual whose personal in-
14 formation was included in the breach of security, provide
15 or arrange for the provision of, to each such individual
16 and at no cost to such individual, consumer credit reports
17 from at least one of the major credit reporting agencies
18 beginning not later than 2 months following the discovery
19 of a breach of security and continuing on a quarterly basis
20 for a period of 2 years thereafter, except when the only
21 information which has been the subject of the security
22 breach is the individual's first name or initial and last
23 name, or address, or phone number, in combination with
24 a credit or debit card number, and any required security
25 code. As part of the Commission's rulemaking described

1 in subsection (d)(3), the Commission shall determine the
2 circumstances under which a person required to provide
3 notification under subsection (a)(1) shall provide or ar-
4 range for the provision of free consumer credit reports to
5 affected individuals.

6 (f) EXEMPTION.—

7 (1) GENERAL EXEMPTION.—A person shall be
8 exempt from the requirements under this section if,
9 following a breach of security, such person deter-
10 mines that there is no reasonable risk of identity
11 theft, fraud, or other unlawful conduct.

12 (2) PRESUMPTIONS.—

13 (A) ENCRYPTION.—The encryption of data
14 in electronic form shall establish a presumption
15 that no reasonable risk of identity theft, fraud,
16 or other unlawful conduct exists following a
17 breach of security of such data. Any such pre-
18 sumption may be rebutted by facts dem-
19 onstrating that the encryption has been or is
20 reasonably likely to be compromised.

21 (B) ADDITIONAL METHODOLOGIES OR
22 TECHNOLOGIES.—Not later than 270 days after
23 the date of the enactment of this Act, the Com-
24 mission shall, by rule pursuant to section 553
25 of title 5, United States Code, identify any ad-

1 ditional security methodology or technology,
2 other than encryption, which renders data in
3 electronic form unusable, unreadable, or indeci-
4 pherable, that shall, if applied to such data, es-
5 tablish a presumption that no reasonable risk of
6 identity theft, fraud, or other unlawful conduct
7 exists following a breach of security of such
8 data. Any such presumption may be rebutted by
9 facts demonstrating that any such methodology
10 or technology has been or is reasonably likely to
11 be compromised. In promulgating such a rule,
12 the Commission shall consult with relevant in-
13 dustries, consumer organizations, and data se-
14 curity and identity theft prevention experts and
15 established standards setting bodies.

16 (3) FTC GUIDANCE.—Not later than 1 year
17 after the date of the enactment of this Act, the
18 Commission shall issue guidance regarding the appli-
19 cation of the exemption in paragraph (1).

20 (g) WEBSITE NOTICE OF FEDERAL TRADE COMMIS-
21 SION.—If the Commission, upon receiving notification of
22 any breach of security that is reported to the Commission
23 under subsection (a)(2), finds that notification of such a
24 breach of security via the Commission’s Internet website
25 would be in the public interest or for the protection of

1 consumers, the Commission shall place such a notice in
2 a clear and conspicuous location on its Internet website.

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

10 **SEC. 4. ENFORCEMENT.**

11 (a) ENFORCEMENT BY THE FEDERAL TRADE COM-
12 MISSION.—

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

20 (2) POWERS OF COMMISSION.—The Commis-
21 sion shall enforce this Act in the same manner, by
22 the same means, and with the same jurisdiction,
23 powers, and duties as though all applicable terms
24 and provisions of the Federal Trade Commission Act
25 (15 U.S.C. 41 et seq.) were incorporated into and

1 made a part of this Act. Any person who violates
2 such regulations shall be subject to the penalties and
3 entitled to the privileges and immunities provided in
4 that Act.

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

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

12 (1) CIVIL ACTION.—In any case in which the
13 attorney general of a State, or an official or agency
14 of a State, has reason to believe that an interest of
15 the residents of that State has been or is threatened
16 or adversely affected by any person who violates sec-
17 tion 2 or 3 of this Act, the attorney general, official,
18 or agency of the State, as *parens patriae*, may bring
19 a civil action on behalf of the residents of the State
20 in a district court of the United States of appro-
21 priate jurisdiction—

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

24 (B) to compel compliance with such sec-
25 tion; or

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

3 (2) CIVIL PENALTIES.—

4 (A) CALCULATION.—

5 (i) TREATMENT OF VIOLATIONS OF
6 SECTION 2.—For purposes of paragraph
7 (1)(C) with regard to a violation of section
8 2, the amount determined under this para-
9 graph is the amount calculated by multi-
10 plying the number of violations of such
11 section by an amount not greater than
12 \$11,000. Each day that a person is not in
13 compliance with the requirements of such
14 section shall be treated as a separate viola-
15 tion. The maximum civil penalty calculated
16 under this clause shall not exceed
17 \$5,000,000.

18 (ii) TREATMENT OF VIOLATIONS OF
19 SECTION 3.—For purposes of paragraph
20 (1)(C) with regard to a violation of section
21 3, the amount determined under this para-
22 graph is the amount calculated by multi-
23 plying the number of violations of such
24 section by an amount not greater than
25 \$11,000. Each failure to send notification

1 as required under section 3 to a resident of
2 the State shall be treated as a separate
3 violation. The maximum civil penalty cal-
4 culated under this clause shall not exceed
5 \$5,000,000.

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

16 (3) INTERVENTION BY THE FTC.—

17 (A) NOTICE AND INTERVENTION.—The
18 State shall provide prior written notice of any
19 action under paragraph (1) to the Commission
20 and provide the Commission with a copy of its
21 complaint, except in any case in which such
22 prior notice is not feasible, in which case the
23 State shall serve such notice immediately upon
24 instituting such action. The Commission shall
25 have the right—

1 (i) to intervene in the action;

2 (ii) upon so intervening, to be heard

3 on all matters arising therein; and

4 (iii) to file petitions for appeal.

5 (B) LIMITATION ON STATE ACTION WHILE

6 FEDERAL ACTION IS PENDING.—If the Commis-

7 sion has instituted a civil action for violation of

8 this Act, no State attorney general, or official

9 or agency of a State, may bring an action under

10 this subsection during the pendency of that ac-

11 tion against any defendant named in the com-

12 plaint of the Commission for any violation of

13 this Act alleged in the complaint.

14 (4) CONSTRUCTION.—For purposes of bringing

15 any civil action under paragraph (1), nothing in this

16 Act shall be construed to prevent an attorney gen-

17 eral of a State from exercising the powers conferred

18 on the attorney general by the laws of that State

19 to—

20 (A) conduct investigations;

21 (B) administer oaths or affirmations; or

22 (C) compel the attendance of witnesses or

23 the production of documentary and other evi-

24 dence.

1 (c) AFFIRMATIVE DEFENSE FOR A VIOLATION OF
2 SECTION 3.—It shall be an affirmative defense to an en-
3 forcement action brought under subsection (a), or a civil
4 action brought under subsection (b), based on a violation
5 of section 3, that all of the personal information contained
6 in the data in electronic form that was acquired as a result
7 of a breach of security of the defendant is public record
8 information that is lawfully made available to the general
9 public from Federal, State, or local government records
10 and was acquired by the defendant from such records.

11 **SEC. 5. DEFINITIONS.**

12 In this Act the following definitions apply:

13 (1) BREACH OF SECURITY.—The term “breach
14 of security” means unauthorized access to or acqui-
15 sition of data in electronic form containing personal
16 information.

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

19 (3) DATA IN ELECTRONIC FORM.—The term
20 “data in electronic form” means any data stored
21 electronically or digitally on any computer system or
22 other database and includes recordable tapes and
23 other mass storage devices.

24 (4) ENCRYPTION.—The term “encryption”
25 means the protection of data in electronic form in

1 storage or in transit using an encryption technology
2 that has been adopted by an established standards
3 setting body which renders such data indecipherable
4 in the absence of associated cryptographic keys nec-
5 essary to enable decryption of such data. Such
6 encryption must include appropriate management
7 and safeguards of such keys to protect the integrity
8 of the encryption.

9 (5) IDENTITY THEFT.—The term “identity
10 theft” means the unauthorized use of another per-
11 son’s personal information for the purpose of engag-
12 ing in commercial transactions under the name of
13 such other person.

14 (6) INFORMATION BROKER.—The term “infor-
15 mation broker” means a commercial entity whose
16 business is to collect, assemble, or maintain personal
17 information concerning individuals who are not cur-
18 rent or former customers of such entity in order to
19 sell such information or provide access to such infor-
20 mation to any nonaffiliated third party in exchange
21 for consideration, whether such collection, assembly,
22 or maintenance of personal information is performed
23 by the information broker directly, or by contract or
24 subcontract with any other entity.

25 (7) PERSONAL INFORMATION.—

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

6 (i) Social Security number.

7 (ii) Driver’s license number, passport
8 number, military identification number, or
9 other similar number issued on a govern-
10 ment document used to verify identity.

11 (iii) Financial account number, or
12 credit or debit card number, and any re-
13 quired security code, access code, or pass-
14 word that is necessary to permit access to
15 an individual’s financial account.

16 (B) MODIFIED DEFINITION BY RULE-
17 MAKING.—The Commission may, by rule, mod-
18 ify the definition of “personal information”
19 under subparagraph (A)—

20 (i) for the purpose of section 2 to the
21 extent that such modification will not un-
22 reasonably impede interstate commerce,
23 and will accomplish the purposes of this
24 Act; or

1 (ii) for the purpose of section 3, to the
2 extent that such modification is necessary
3 to accommodate changes in technology or
4 practices, will not unreasonably impede
5 interstate commerce, and will accomplish
6 the purposes of this Act.

7 (8) PUBLIC RECORD INFORMATION.—The term
8 “public record information” means information
9 about an individual which has been obtained origi-
10 nally from records of a Federal, State, or local gov-
11 ernment entity that are available for public inspec-
12 tion.

13 (9) NON-PUBLIC INFORMATION.—The term
14 “non-public information” means information about
15 an individual that is of a private nature and neither
16 available to the general public nor obtained from a
17 public record.

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

19 (a) PREEMPTION OF STATE INFORMATION SECURITY
20 LAWS.—This Act supersedes any provision of a statute,
21 regulation, or rule of a State or political subdivision of
22 a State, with respect to those entities covered by the regu-
23 lations issued pursuant to this Act, that expressly—

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

4 (2) requires notification to individuals of a
5 breach of security resulting in unauthorized access
6 to or acquisition of data in electronic form con-
7 taining personal information.

8 (b) ADDITIONAL PREEMPTION.—

9 (1) IN GENERAL.—No person other than the
10 Attorney General of a State may bring a civil action
11 under the laws of any State if such action is pre-
12 mised in whole or in part upon the defendant vio-
13 lating any provision of this Act.

14 (2) PROTECTION OF CONSUMER PROTECTION
15 LAWS.—This subsection shall not be construed to
16 limit the enforcement of any State consumer protec-
17 tion law by an Attorney General of a State.

18 (c) PROTECTION OF CERTAIN STATE LAWS.—This
19 Act shall not be construed to preempt the applicability
20 of—

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

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

24 (d) PRESERVATION OF FTC AUTHORITY.—Nothing
25 in this Act may be construed in any way to limit or affect

1 the Commission’s authority under any other provision of
2 law, including the authority to issue advisory opinions
3 (under part 1 of volume 16 of the Code of Federal Regula-
4 tions), policy statements, or guidance regarding this Act.

5 **SEC. 7. EFFECTIVE DATE.**

6 This Act shall take effect 1 year after the date of
7 enactment of this Act.

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

9 There is authorized to be appropriated to the Com-
10 mission \$1,000,000 for each of fiscal years 2010 through
11 2015 to carry out this Act.

Amend the title so as to read: “A bill to protect con-
sumers by requiring reasonable security policies and pro-
cedures to protect data containing personal information,
and to provide for nationwide notice in the event of a se-
curity breach.”.

