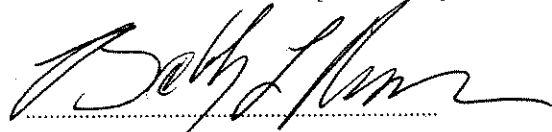


[109H4127]



(Original Signature of Member)

110TH CONGRESS
1ST SESSION

H. R. _____

To protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information, and to provide for nationwide notice in the event of a security breach.

IN THE HOUSE OF REPRESENTATIVES

Mr. RUSH (for himself, Mr. STEARNS, Ms. SCHAKOWSKY, Mr. DINGELL, Mr. BARTON of Texas, Mr. MARKEY, Mr. GORDON of Tennessee, Ms. ESHOO, Mr. STUPAK, Mr. GENE GREEN of Texas, Ms. DEGETTE, Mrs. CAPPS, Mr. DOYLE, Ms. SOLIS, Mr. GONZALEZ, Mr. INSLEE, Ms. BALDWIN, Ms. HOOLEY, Mr. BUTTERFIELD, Mr. HASTERT, Mrs. BONO, Mr. TERRY, ~~and~~ Mr. BURGESS) introduced the following bill; which was referred to the Committee on _____

and Mr. Engel *per*
A BILL

To protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information, and to provide for nationwide notice in the event of a security breach.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

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 in electronic form containing personal in-
13 formation , or contracts to have any third party en-
14 tity maintain such data for such person, to establish
15 and implement policies and procedures regarding in-
16 formation security practices for the treatment and
17 protection of personal informtion taking into consid-
18 eration—

19 (A) the size of, and the nature, scope, and
20 complexity of the activities engaged in by, such
21 person;

22 (B) the current state of the art in adminis-
23 trative, technical, and physical safeguards for
24 protecting such information; and

25 (C) the cost of implementing such safe-
26 guards.

1 (2) REQUIREMENTS.—Such regulations shall
2 require the policies and procedures to include the
3 following:

4 (A) A security policy with respect to the
5 collection, use, sale, other dissemination, and
6 maintenance of such personal information.

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

11 (C) A process for identifying and assessing
12 any reasonably foreseeable vulnerabilities in the
13 system maintained by such person that contains
14 such electronic data , which shall include reg-
15 ular monitoring for a breach of security of such
16 system.

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

24 (E) A process for disposing of obsolete
25 data in electronic form containing personal in-

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

6 (3) TREATMENT OF ENTITIES GOVERNED BY
7 OTHER LAW.—In promulgating the regulations
8 under this subsection, the Commission may deter-
9 mine to be in compliance with this subsection any
10 person who is required under any other Federal law
11 to maintain standards and safeguards for informa-
12 tion security and protection of personal information
13 that provide equal or greater protection than those
14 required under this subsection.

15 (b) DESTRUCTION OF OBSOLETE PAPER RECORDS
16 CONTAINING PERSONAL INFORMATION.—

17 (1) STUDY.—Not later than 1 year after the
18 date of enactment of this Act, the Commission shall
19 conduct a study on the practicality of requiring a
20 standard method or methods for the destruction of
21 obsolete paper documents and other non-electronic
22 data containing personal information by persons en-
23 gaged in interstate commerce who own or possess
24 such paper documents and non-electronic data. The
25 study shall consider the cost, benefit, feasibility, and

1 effect of a requirement of shredding or other perma-
2 nent destruction of such paper documents and non-
3 electronic data.

4 (2) REGULATIONS.—The Commission may pro-
5 mulgate regulations under section 553 of title 5,
6 United States Code, requiring a standard method or
7 methods for the destruction of obsolete paper docu-
8 ments and other non-electronic data containing per-
9 sonal information by persons engaged in interstate
10 commerce who own or possess such paper documents
11 and non-electronic data if the Commission finds
12 that—

13 (A) the improper disposal of obsolete paper
14 documents and other non-electronic data cre-
15 ates a reasonable risk of identity theft, fraud,
16 or other unlawful conduct;

17 (B) such a requirement would be effective
18 in preventing identity theft, fraud, or other un-
19 lawful conduct;

20 (C) the benefit in preventing identity theft,
21 fraud, or other unlawful conduct would out-
22 weigh the cost to persons subject to such a re-
23 quirement; and

24 (D) compliance with such a requirement
25 would be practicable.

1 In enforcing any such regulations, the Commission
2 may determine to be in compliance with such regula-
3 tions any person who is required under any other
4 Federal law to dispose of obsolete paper documents
5 and other non-electronic data containing personal in-
6 formation if such other Federal law provides equal
7 or greater protection of personal information than
8 the regulations promulgated under this subsection.

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

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

12 The regulations promulgated under subsection (a)
13 shall require information brokers to submit their se-
14 curity policies to the Commission in conjunction with
15 a notification of a breach of security under section
16 3 or upon request of the Commission.

17 (2) POST-BREACH AUDIT.—For any informa-
18 tion broker required to provide notification under
19 section 3, the Commission shall conduct an audit of
20 the information security practices of such informa-
21 tion broker, or require the information broker to
22 conduct an independent audit of such practices (by
23 an independent auditor who has not audited such in-
24 formation broker's security practices during the pre-
25 ceding 5 years). The Commission may conduct or re-

1 quire additional audits for a period of 5 years fol-
2 lowing the breach of security or until the Commis-
3 sion determines that the security practices of the in-
4 formation broker are in compliance with the require-
5 ments of this section and are adequate to prevent
6 further breaches of security.

7 (3) VERIFICATION OF AND INDIVIDUAL ACCESS
8 TO PERSONAL INFORMATION.—

9 (A) VERIFICATION.—Each information
10 broker shall establish reasonable procedures to
11 verify the accuracy of the personal information
12 it collects, assembles, or maintains, and any
13 other information it collects, assembles, or
14 maintains that specifically identifies an indi-
15 vidual, other than information which merely
16 identifies an individual's name or address.

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

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

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

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

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

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

1 such request is frivolous or irrelevant,
2 shall—

3 (I) correct any inaccuracy; or

4 (II)(aa) in the case of informa-
5 tion that is public record information,
6 inform the individual of the source of
7 the information, and, if reasonably
8 available, where a request for correc-
9 tion may be directed; or

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

20 (iii) LIMITATIONS.—An information
21 broker may limit the access to information
22 required under subparagraph (B) in the
23 following circumstances:

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

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

8 (iv) RULEMAKING.—The Commission
9 shall issue regulations, as necessary, under
10 section 553 of title 5, United States Code,
11 on the application of the limitations in
12 clause (iii).

13 (C) TREATMENT OF ENTITIES GOVERNED
14 BY OTHER LAW.—The Commission may pro-
15 mulgate rules (under section 553 of title 5,
16 United States Code) to determine to be in com-
17 pliance with this paragraph any person who is
18 a consumer reporting agency, as defined in sec-
19 tion 603(f) of the Fair Credit Reporting Act,
20 with respect to those products and services that
21 are subject to and in compliance with the re-
22 quirements of that Act.

23 (4) REQUIREMENT OF AUDIT LOG OF
24 ACCESSED AND TRANSMITTED INFORMATION.—Not
25 later than 1 year after the date of the enactment of

1 this Act, the Commission shall promulgate regula-
2 tions under section 553 of title 5, United States
3 Code, to require information brokers to establish
4 measures which facilitate the auditing or retracing
5 of any internal or external access to, or trans-
6 missions of, any data in electronic form containing
7 personal information collected, assembled, or main-
8 tained by such information broker.

9 (5) PROHIBITION ON PRETEXTING BY INFOR-
10 MATION BROKERS.—

11 (A) PROHIBITION ON OBTAINING PER-
12 SONAL INFORMATION BY FALSE PRETENSES.—

13 It shall be unlawful for an information broker
14 to obtain or attempt to obtain, or cause to be
15 disclosed or attempt to cause to be disclosed to
16 any person, personal information or any other
17 information relating to any person by—

18 (i) making a false, fictitious, or fraud-
19 ulent statement or representation to any
20 person; or

21 (ii) providing any document or other
22 information to any person that the infor-
23 mation broker knows or should know to be
24 forged, counterfeit, lost, stolen, or fraudu-
25 lently obtained, or to contain a false, ficti-

1 tious, or fraudulent statement or represen-
2 tation.

3 (B) PROHIBITION ON SOLICITATION TO
4 OBTAIN PERSONAL INFORMATION UNDER FALSE
5 PRETENSES.—It shall be unlawful for an infor-
6 mation broker to request a person to obtain
7 personal information or any other information
8 relating to any other person, if the information
9 broker knew or should have known that the per-
10 son to whom such a request is made will obtain
11 or attempt to obtain such information in the
12 manner described in subsection (a).

13 (d) EXEMPTION FOR TELECOMMUNICATIONS CAR-
14 RIER, CABLE OPERATOR, INFORMATION SERVICE, OR
15 INTERACTIVE COMPUTER SERVICE.—Nothing in this sec-
16 tion shall apply to any electronic communication by a third
17 party stored by a telecommunications carrier, cable oper-
18 ator, or information service, as those terms are defined
19 in section 3 of the Communications Act of 1934 (47
20 U.S.C. 153), or an interactive computer service, as such
21 term is defined in section 230(f)(2) of such Act (47 U.S.C.
22 230(f)(2)).

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 in electronic form containing personal information shall,
6 following the discovery of a breach of security of the sys-
7 tem maintained by such person that contains such data—

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

12 (2) notify the Commission.

13 (b) **SPECIAL NOTIFICATION REQUIREMENT FOR CER-**
14 **TAIN ENTITIES.**—

15 (1) **THIRD PARTY AGENTS.**—In the event of a
16 breach of security by any third party entity that has
17 been contracted to maintain or process data in elec-
18 tronic form containing personal information on be-
19 half of any other person who owns or possesses such
20 data, such third party entity shall be required only
21 to notify such person of the breach of security. Upon
22 receiving such notification from such third party,
23 such person shall provide the notification required
24 under subsection (a).

25 (2) **TELECOMMUNICATIONS CARRIERS, CABLE**
26 **OPERATORS, INFORMATION SERVICES, AND INTER-**

1 ACTIVE COMPUTER SERVICES.—If a telecommuni-
2 cations carrier, cable operator, or information service
3 (as such terms are defined in section 3 of the Com-
4 munications Act of 1934 (47 U.S.C. 153)), or an
5 interactive computer service (as such term is defined
6 in section 230(f)(2) of such Act (47 U.S.C.
7 230(f)(2))), becomes aware of a breach of security
8 during the transmission of data in electronic form
9 containing personal information that is owned or
10 possessed by another person utilizing the means of
11 transmission of such telecommunications carrier,
12 cable operator, information service, or interactive
13 computer service, such telecommunications carrier,
14 cable operator, information service, or interactive
15 computer service shall be required only to notify the
16 person who initiated such transmission of such a
17 breach of security if such person can be reasonably
18 identified. Upon receiving such notification from a
19 telecommunications carrier, cable operator, informa-
20 tion service, or interactive computer service, such
21 person shall provide the notification required under
22 subsection (a).

23 (3) BREACH OF HEALTH INFORMATION.—If the
24 Commission receives a notification of a breach of se-
25 curity and determines that information included in

1 such breach is individually identifiable health infor-
2 mation (as such term is defined in section 1171(6)
3 of the Social Security Act (42 U.S.C. 1320d(6)), the
4 Commission shall send a copy of such notification to
5 the Secretary of Health and Human Services.

6 (c) TIMELINESS OF NOTIFICATION.—All notifications
7 required under subsection (a) shall be made as promptly
8 as possible and without unreasonable delay following the
9 discovery of a breach of security of the system and con-
10 sistent with any measures necessary to determine the
11 scope of the breach, prevent further breach or unauthor-
12 ized disclosures, and reasonably restore the integrity of the
13 data system.

14 (d) METHOD AND CONTENT OF NOTIFICATION.—

15 (1) DIRECT NOTIFICATION.—

16 (A) METHOD OF NOTIFICATION.—A person
17 required to provide notification to individuals
18 under subsection (a)(1) shall be in compliance
19 with such requirement if the person provides
20 conspicuous and clearly identified notification
21 by one of the following methods (provided the
22 selected method can reasonably be expected to
23 reach the intended individual):

24 (i) Written notification.

25 (ii) Email notification, if—

1 (I) the person's primary method
2 of communication with the individual
3 is by email; or

4 (II) the individual has consented
5 to receive such notification and the
6 notification is provided in a manner
7 that is consistent with the provisions
8 permitting electronic transmission of
9 notices under section 101 of the Elec-
10 tronic Signatures in Global Commerce
11 Act (15 U.S.C. 7001).

12 (B) CONTENT OF NOTIFICATION.—Regard-
13 less of the method by which notification is pro-
14 vided to an individual under subparagraph (A),
15 such notification shall include—

16 (i) a description of the personal infor-
17 mation that was acquired by an unauthor-
18 ized person;

19 (ii) a telephone number that the indi-
20 vidual may use, at no cost to such indi-
21 vidual, to contact the person to inquire
22 about the breach of security or the infor-
23 mation the person maintained about that
24 individual;

1 (iii) notice that the individual is enti-
2 tled to receive, at no cost to such indi-
3 vidual, consumer credit reports on a quar-
4 terly basis for a period of 2 years, and in-
5 structions to the individual on requesting
6 such reports from the person;

7 (iv) the toll-free contact telephone
8 numbers and addresses for the major cred-
9 it reporting agencies; and

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

14 (2) SUBSTITUTE NOTIFICATION.—

15 (A) CIRCUMSTANCES GIVING RISE TO SUB-
16 STITUTE NOTIFICATION.—A person required to
17 provide notification to individuals under sub-
18 section (a)(1) may provide substitute notifica-
19 tion in lieu of the direct notification required by
20 paragraph (1) if—

21 (i) the person owns or possesses data
22 in electronic form containing personal in-
23 formation of fewer than 1,000 individuals;
24 and

1 (ii) such direct notification is not fea-
2 sible due to—

3 (I) excessive cost to the person
4 required to provide such notification
5 relative to the resources of such per-
6 son, as determined in accordance with
7 the regulations issued by the Commis-
8 sion under paragraph (3)(A); or

9 (II) lack of sufficient contact in-
10 formation for the individual required
11 to be notified.

12 (B) ~~CONTENT~~ ~~FORM~~ OF SUBSTITUTE NO-
13 TIFICATION.—Such substitute notification shall
14 include—

15 (i) email notification to the extent
16 that the person has email addresses of in-
17 dividuals to whom it is required to provide
18 notification under subsection (a)(1);

19 (ii) a conspicuous notice on the Inter-
20 net website of the person (if such person
21 maintains such a website); and

22 (iii) notification in print and to broad-
23 cast media, including major media in met-
24 ropolitan and rural areas where the indi-

1 viduals whose personal information was ac-
2 quired reside.

3 (C) CONTENT OF SUBSTITUTE NOTICE.—

4 Each form of substitute notice under this para-
5 graph shall include—

6 (i) notice that individuals whose per-
7 sonal information is included in the breach
8 of security are entitled to receive, at no
9 cost to the individuals, consumer credit re-
10 ports on a quarterly basis for a period of
11 2 years, and instructions on requesting
12 such reports from the person; and

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

18 (3) FEDERAL TRADE COMMISSION REGULA-
19 TIONS AND GUIDANCE.—

20 (A) REGULATIONS.—Not later than 1 year
21 after the date of enactment of this Act, the
22 Commission shall, by regulations under section
23 553 of title 5, United States Code, establish cri-
24 teria for determining the 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 cost to the person
4 required to provide such notification relative to
5 the resources of such person.

6 (B) GUIDANCE.—In addition, the Commis-
7 sion shall provide and publish general guidance
8 with respect to compliance with this section.
9 Such guidance shall include—

10 (i) a description of written or email
11 notification that complies with the require-
12 ments of paragraph (1); and

13 (ii) guidance on the content of sub-
14 stitute notification under paragraph
15 (2)(B), including the extent of notification
16 to print and broadcast media that complies
17 with the requirements of such paragraph.

18 (e) OTHER OBLIGATIONS FOLLOWING BREACH.—A
19 person required to provide notification under subsection
20 (a) shall , upon request of an individual whose personal
21 information was included in the breach of security, provide
22 or arrange for the provision of, to each such individual
23 and at no cost to such individual, consumer credit reports
24 from at least one of the major credit reporting agencies
25 beginning not later than 2 months following the discovery

1 of a breach of security and continuing on a quarterly basis
2 for a period of 2 years thereafter.

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, such person deter-
7 mines that there is no reasonable risk of identity
8 theft, fraud, or other unlawful conduct.

9 (2) PRESUMPTIONS.—

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

18 (B) ADDITIONAL METHODOLOGIES OR
19 TECHNOLOGIES.—Not later than 270 days after
20 the date of the enactment of this Act, the Com-
21 mission shall, by rule pursuant to section 553
22 of title 5, United States Code, identify any ad-
23 ditional security methodology or technology,
24 other than encryption, which renders data in
25 electronic form unreadable or indecipherable,

1 that shall, if applied to such data, establish a
2 presumption that no reasonable risk of identity
3 theft, fraud, or other unlawful conduct exists
4 following a breach of security of such data. Any
5 such presumption may be rebutted by facts
6 demonstrating that any such methodology or
7 technology has been or is reasonably likely to be
8 compromised. In promulgating such a rule, the
9 Commission shall consult with relevant indus-
10 tries, consumer organizations, and data security
11 and identity theft prevention experts and estab-
12 lished standards setting bodies.

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

17 (g) WEBSITE NOTICE OF FEDERAL TRADE COMMIS-
18 SION.—If the Commission, upon receiving notification of
19 any breach of security that is reported to the Commission
20 under subsection (a)(2), finds that notification of such a
21 breach of security via the Commission's Internet website
22 would be in the public interest or for the protection of
23 consumers, the Commission shall place such a notice in
24 a clear and conspicuous location on its Internet website.

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

8 **SEC. 4. ENFORCEMENT.**

9 (a) ENFORCEMENT BY THE FEDERAL TRADE COM-
10 MISSION.—

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

18 (2) POWERS OF COMMISSION.—The Commis-
19 sion shall enforce this Act in the same manner, by
20 the same means, and with the same jurisdiction,
21 powers, and duties as though all applicable terms
22 and provisions of the Federal Trade Commission Act
23 (15 U.S.C. 41 et seq.) were incorporated into and
24 made a part of this Act. Any person who violates
25 such regulations shall be subject to the penalties and

1 entitled to the privileges and immunities provided in
2 that Act.

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

8 (b) ENFORCEMENT BY STATE ATTORNEYS GEN-
9 ERAL.—

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

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

22 (B) to compel compliance with such sec-
23 tion; or

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

1 (2) CIVIL PENALTIES.—

2 (A) CALCULATION.—

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

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

1 violation. The maximum civil penalty cal-
2 culated under this clause shall not exceed
3 \$5,000,000.

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

14 (3) INTERVENTION BY THE FTC.—

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

24 (i) to intervene in the action;

1 (ii) upon so intervening, to be heard

2 on all matters arising therein; and

3 (iii) to file petitions for appeal.

4 (B) LIMITATION ON STATE ACTION WHILE
5 FEDERAL ACTION IS PENDING.—If the Commis-
6 sion has instituted a civil action for violation of
7 this Act, no State attorney general, or official
8 or agency of a State, may bring an action under
9 this subsection during the pendency of that ac-
10 tion against any defendant named in the com-
11 plaint of the Commission for any violation of
12 this Act alleged in the complaint.

13 (4) CONSTRUCTION.—For purposes of bringing
14 any civil action under paragraph (1), nothing in this
15 Act shall be construed to prevent an attorney gen-
16 eral of a State from exercising the powers conferred
17 on the attorney general by the laws of that State
18 to—

19 (A) conduct investigations;

20 (B) administer oaths or affirmations; or

21 (C) compel the attendance of witnesses or
22 the production of documentary and other evi-
23 dence.

24 (c) AFFIRMATIVE DEFENSE FOR A VIOLATION OF
25 SECTION 3.—It shall be an affirmative defense to an en-

1 enforcement action brought under subsection (a), or a civil
2 action brought under subsection (b), based on a violation
3 of section 3, that all of the personal information contained
4 in the data in electronic form that was acquired as a result
5 of a breach of security of the defendant is public record
6 information that is lawfully made available to the general
7 public from Federal, State, or local government records
8 and was acquired by the defendant from such records.

9 **SEC. 5. DEFINITIONS.**

10 In this Act the following definitions apply:

11 (1) **BREACH OF SECURITY.**—The term “breach
12 of security” means the unauthorized acquisition of
13 data in electronic form containing personal informa-
14 tion.

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

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

22 (4) **ENCRYPTION.**—The term “encryption”
23 means the protection of data in electronic form in
24 storage or in transit using an encryption technology
25 that has been adopted by an established standards

1 setting body which renders such data indecipherable
2 in the absence of associated cryptographic keys nec-
3 essary to enable decryption of such data. Such
4 encryption must include appropriate management
5 and safeguards of such keys to protect the integrity
6 of the encryption.

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

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

23 (7) PERSONAL INFORMATION.—

24 (A) DEFINITION.—The term “personal in-
25 formation” means an individual’s first name or

1 initial and last name, or address, or phone
2 number, in combination with any 1 or more of
3 the following data elements for that individual:

4 (i) Social Security number.

5 (ii) Driver's license number or other
6 State identification number.

7 (iii) Financial account number, or
8 credit or debit card number, and any re-
9 quired security code, access code, or pass-
10 word that is necessary to permit access to
11 an individual's financial account.

12 (B) MODIFIED DEFINITION BY RULE-
13 MAKING.—The Commission may, by rule, mod-
14 ify the definition of “personal information”
15 under subparagraph (A) to the extent that such
16 modification is necessary to accommodate
17 changes in technology or practices, will not un-
18 reasonably impede interstate commerce, and
19 will accomplish the purposes of this Act.

20 (8) PERSON.—The term “person” has the same
21 meaning given such term in section 551(2) of title
22 5, United States Code.

23 (9) PUBLIC RECORD INFORMATION.—The term
24 “public record information” means information
25 about an individual which has been obtained origi-

1 nally from records of a Federal, State, or local gov-
2 ernment entity that are available for public inspec-
3 tion.

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

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

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

15 (1) requires information security practices and
16 treatment of data in electronic form containing per-
17 sonal information similar to any of those required
18 under section 2; and

19 (2) requires notification to individuals of a
20 breach of security resulting in unauthorized acquisi-
21 tion of data in electronic form containing personal
22 information.

23 (b) ADDITIONAL PREEMPTION.—

24 (1) IN GENERAL.—No person other than the
25 Attorney General of a State may bring a civil action

1 under the laws of any State if such action is pre-
2 mised in whole or in part upon the defendant vio-
3 lating any provision of this Act.

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

8 (c) PROTECTION OF CERTAIN STATE LAWS.—This
9 Act shall not be construed to preempt the applicability
10 of—

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

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

14 (d) PRESERVATION OF FTC AUTHORITY.—Nothing
15 in this Act may be construed in any way to limit or affect
16 the Commission's authority under any other provision of
17 law, including the authority to issue advisory opinions
18 (under part 1 of volume 16 of the Code of Federal Regula-
19 tions), policy statements, or guidance regarding this Act.

20 **SEC. 7. EFFECTIVE DATE AND SUNSET.**

21 (a) EFFECTIVE DATE.—This Act shall take effect 1
22 year after the date of enactment of this Act.

23 (b) SUNSET.—This Act shall cease to be in effect on
24 the date that is 10 years from the date of enactment of
25 this Act.

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

2 There is authorized to be appropriated to the Com-
3 mission \$1,000,000 for each of fiscal years 2008 through
4 2012 to carry out this Act.