

110TH CONGRESS
1ST SESSION

H. R. 958

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

FEBRUARY 8, 2007

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, Mr. BURGESS, and Mr. ENGEL) introduced the following bill; which was referred to the Committee on Energy and Commerce

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,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Data Accountability
5 and Trust Act”.

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

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

4 (1) REGULATIONS.—Not later than 1 year after
5 the date of enactment of this Act, the Commission
6 shall promulgate regulations under section 553 of
7 title 5, United States Code, to require each person
8 engaged in interstate commerce that owns or pos-
9 sesses data in electronic form containing personal in-
10 formation, or contracts to have any third party enti-
11 ty maintain such data for such person, to establish
12 and implement policies and procedures regarding in-
13 formation security practices for the treatment and
14 protection of personal informtion taking into consid-
15 eration—

16 (A) the size of, and the nature, scope, and
17 complexity of the activities engaged in by, such
18 person;

19 (B) the current state of the art in adminis-
20 trative, technical, and physical safeguards for
21 protecting such information; and

22 (C) the cost of implementing such safe-
23 guards.

24 (2) REQUIREMENTS.—Such regulations shall
25 require the policies and procedures to include the
26 following:

1 (A) A security policy with respect to the
2 collection, use, sale, other dissemination, and
3 maintenance of such personal information.

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

8 (C) A process for identifying and assessing
9 any reasonably foreseeable vulnerabilities in the
10 system maintained by such person that contains
11 such electronic data, which shall include regular
12 monitoring for a breach of security of such sys-
13 tem.

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

21 (E) A process for disposing of obsolete
22 data in electronic form containing personal in-
23 formation by shredding, permanently erasing,
24 or otherwise modifying the personal information
25 contained in such data to make such personal

1 information permanently unreadable or
2 undecipherable.

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

12 (b) DESTRUCTION OF OBSOLETE PAPER RECORDS
13 CONTAINING PERSONAL INFORMATION.—

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

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

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

14 (B) such a requirement would be effective
15 in preventing identity theft, fraud, or other un-
16 lawful conduct;

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

21 (D) compliance with such a requirement
22 would be practicable.

23 In enforcing any such regulations, the Commission
24 may determine to be in compliance with such regula-
25 tions any person who is required under any other

1 Federal law to dispose of obsolete paper documents
2 and other non-electronic data containing personal in-
3 formation if such other Federal law provides equal
4 or greater protection or personal information than
5 the regulations promulgated under this subsection.

6 (c) SPECIAL REQUIREMENTS FOR INFORMATION
7 BROKERS.—

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

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

14 (2) POST-BREACH AUDIT.—For any information
15 broker required to provide notification under section
16 3, the Commission shall conduct an audit of the in-
17 formation security practices of such information
18 broker, or require the information broker to conduct
19 an independent audit of such practices (by an inde-
20 pendent auditor who has not audited such informa-
21 tion broker's security practices during the preceding
22 5 years). The Commission may conduct or require
23 additional audits for a period of 5 years following
24 the breach of security or until the Commission deter-
25 mines that the security practices of the information

1 broker are in compliance with the requirements of
2 this section and are adequate to prevent further
3 breaches of security.

4 (3) VERIFICATION OF AND INDIVIDUAL ACCESS
5 TO PERSONAL INFORMATION.—

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

14 (B) CONSUMER ACCESS TO INFORMA-
15 TION.—

16 (i) ACCESS.—Each information broker
17 shall—

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

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

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

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

24 (I) correct any inaccuracy; or

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

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

17 (iii) LIMITATIONS.—An information
18 broker may limit the access to information
19 required under subparagraph (B) in the
20 following circumstances:

21 (I) If access of the individual to
22 the information is limited by law or
23 legally recognized privilege.

24 (II) If the information is used for
25 a legitimate governmental or fraud

1 prevention purpose that would be
2 compromised by such access.

3 (iv) RULEMAKING.—The Commission
4 shall issue regulations, as necessary, under
5 section 553 of title 5, United States Code,
6 on the application of the limitations in
7 clause (iii).

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

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

1 electronic form containing personal information col-
2 lected, assembled, or maintained by such information
3 broker.

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

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

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

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

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

23 (B) PROHIBITION ON SOLICITATION TO
24 OBTAIN PERSONAL INFORMATION UNDER FALSE
25 PRETENSES.—It shall be unlawful for an infor-

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

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

18 **SEC. 3. NOTIFICATION OF INFORMATION SECURITY**
 19 **BREACH.**

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

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

5 (2) notify the Commission.

6 (b) SPECIAL NOTIFICATION REQUIREMENT FOR CER-
7 TAIN ENTITIES.—

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

18 (2) TELECOMMUNICATIONS CARRIERS, CABLE
19 OPERATORS, INFORMATION SERVICES, AND INTER-
20 ACTIVE COMPUTER SERVICES.—If a telecommuni-
21 cations carrier, cable operator, or information service
22 (as such terms are defined in section 3 of the Com-
23 munications Act of 1934 (47 U.S.C. 153)), or an
24 interactive computer service (as such term is defined
25 in section 230(f)(2) of such Act (47 U.S.C.

1 230(f)(2))), becomes aware of a breach of security
2 during the transmission of data in electronic form
3 containing personal information that is owned or
4 possessed by another person utilizing the means of
5 transmission of such telecommunications carrier,
6 cable operator, information service, or interactive
7 computer service, such telecommunications carrier,
8 cable operator, information service, or interactive
9 computer service shall be required only to notify the
10 person who initiated such transmission of such a
11 breach of security if such person can be reasonably
12 identified. Upon receiving such notification from a
13 telecommunications carrier, cable operator, informa-
14 tion service, or interactive computer service, such
15 person shall provide the notification required under
16 subsection (a).

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

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

9 (d) **METHOD AND CONTENT OF NOTIFICATION.**—

10 (1) **DIRECT NOTIFICATION.**—

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

19 (i) Written notification.

20 (ii) Email notification, if—

21 (I) the person’s primary method
22 of communication with the individual
23 is by email; or

24 (II) the individual has consented
25 to receive such notification and the

1 notification is provided in a manner
2 that is consistent with the provisions
3 permitting electronic transmission of
4 notices under section 101 of the Elec-
5 tronic Signatures in Global Commerce
6 Act (15 U.S.C. 7001).

7 (B) CONTENT OF NOTIFICATION.—Regard-
8 less of the method by which notification is pro-
9 vided to an individual under subparagraph (A),
10 such notification shall include—

11 (i) a description of the personal infor-
12 mation that was acquired by an unauthor-
13 ized person;

14 (ii) a telephone number that the indi-
15 vidual may use, at no cost to such indi-
16 vidual, to contact the person to inquire
17 about the breach of security or the infor-
18 mation the person maintained about that
19 individual;

20 (iii) notice that the individual is enti-
21 tled to receive, at no cost to such indi-
22 vidual, consumer credit reports on a quar-
23 terly basis for a period of 2 years, and in-
24 structions to the individual on requesting
25 such reports from the person;

1 (iv) the toll-free contact telephone
2 numbers and addresses for the major cred-
3 it reporting agencies; and

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

8 (2) SUBSTITUTE NOTIFICATION.—

9 (A) CIRCUMSTANCES GIVING RISE TO SUB-
10 STITUTE NOTIFICATION.—A person required to
11 provide notification to individuals under sub-
12 section (a)(1) may provide substitute notifica-
13 tion in lieu of the direct notification required by
14 paragraph (1) if—

15 (i) the person owns or possesses data
16 in electronic form containing personal in-
17 formation of fewer than 1,000 individuals;
18 and

19 (ii) such direct notification is not fea-
20 sible due to—

21 (I) excessive cost to the person
22 required to provide such notification
23 relative to the resources of such per-
24 son, as determined in accordance with

1 the regulations issued by the Commis-
2 sion under paragraph (3)(A); or

3 (II) lack of sufficient contact in-
4 formation for the individual required
5 to be notified.

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

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

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

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

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

24 (i) notice that individuals whose per-
25 sonal information is included in the breach

1 of security are entitled to receive, at no
2 cost to the individuals, consumer credit re-
3 ports on a quarterly basis for a period of
4 2 years, and instructions on requesting
5 such reports from the person; and

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

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

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

24 (B) GUIDANCE.—In addition, the Commis-
25 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.

21 (f) EXEMPTION.—

22 (1) GENERAL EXEMPTION.—A person shall be
23 exempt from the requirements under this section if,
24 following a breach of security, such person deter-

1 mines that there is no reasonable risk of identity
2 theft, fraud, or other unlawful conduct.

3 (2) PRESUMPTIONS.—

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

12 (B) ADDITIONAL METHODOLOGIES OR
13 TECHNOLOGIES.—Not later than 270 days after
14 the date of the enactment of this Act, the Com-
15 mission shall, by rule pursuant to section 553
16 of title 5, United States Code, identify any ad-
17 ditional security methodology or technology,
18 other than encryption, which renders data in
19 electronic form unreadable or indecipherable,
20 that shall, if applied to such data, establish a
21 presumption that no reasonable risk of identity
22 theft, fraud, or other unlawful conduct exists
23 following a breach of security of such data. Any
24 such presumption may be rebutted by facts
25 demonstrating that any such methodology or

1 technology has been or is reasonably likely to be
2 compromised. In promulgating such a rule, the
3 Commission shall consult with relevant indus-
4 tries, consumer organizations, and data security
5 and identity theft prevention experts and estab-
6 lished standards setting bodies.

7 (3) FTC GUIDANCE.—Not later than 1 year
8 after the date of the enactment of this Act, the
9 Commission shall issue guidance regarding the appli-
10 cation of the exemption in paragraph (1).

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

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

1 **SEC. 4. ENFORCEMENT.**

2 (a) ENFORCEMENT BY THE FEDERAL TRADE COM-
3 MISSION.—

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

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

21 (3) 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 (b) ENFORCEMENT BY STATE ATTORNEYS GEN-
2 ERAL.—

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

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

15 (B) to compel compliance with such sec-
16 tion; or

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

19 (2) CIVIL PENALTIES.—

20 (A) CALCULATION.—

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

1 plying the number of violations of such
2 section by an amount not greater than
3 \$11,000. Each day that a person is not in
4 compliance with the requirements of such
5 section shall be treated as a separate viola-
6 tion. The maximum civil penalty calculated
7 under this clause shall not exceed
8 \$5,000,000.

9 (ii) TREATMENT OF VIOLATIONS OF
10 SECTION 3.—For purposes of paragraph
11 (1)(C) with regard to a violation of section
12 3, the amount determined under this para-
13 graph is the amount calculated by multi-
14 plying the number of violations of such
15 section by an amount not greater than
16 \$11,000. Each failure to send notification
17 as required under section 3 to a resident of
18 the State shall be treated as a separate
19 violation. The maximum civil penalty cal-
20 culated under this clause shall not exceed
21 \$5,000,000.

22 (B) ADJUSTMENT FOR INFLATION.—Be-
23 ginning on the date that the Consumer Price
24 Index is first published by the Bureau of Labor
25 Statistics that is after 1 year after the date of

1 enactment of this Act, and each year thereafter,
2 the amounts specified in clauses (i) and (ii) of
3 subparagraph (A) shall be increased by the per-
4 centage increase in the Consumer Price Index
5 published on that date from the Consumer
6 Price Index published the previous year.

7 (3) INTERVENTION BY THE FTC.—

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

17 (i) to intervene in the action;

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

20 (iii) to file petitions for appeal.

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

1 this subsection during the pendency of that ac-
2 tion against any defendant named in the com-
3 plaint of the Commission for any violation of
4 this Act alleged in the complaint.

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

11 (A) conduct investigations;

12 (B) administer oaths or affirmations; or

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

16 (c) AFFIRMATIVE DEFENSE FOR A VIOLATION OF
17 SECTION 3.—It shall be an affirmative defense to an en-
18 forcement action brought under subsection (a), or a civil
19 action brought under subsection (b), based on a violation
20 of section 3, that all of the personal information contained
21 in the data in electronic form that was acquired as a result
22 of a breach of security of the defendant is public record
23 information that is lawfully made available to the general
24 public from Federal, State, or local government records
25 and was acquired by the defendant from such records.

1 **SEC. 5. DEFINITIONS.**

2 In this Act the following definitions apply:

3 (1) **BREACH OF SECURITY.**—The term “breach
4 of security” means the unauthorized acquisition of
5 data in electronic form containing personal informa-
6 tion.

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

9 (3) **DATA IN ELECTRONIC FORM.**—The term
10 “data in electronic form” means any data stored
11 electronically or digitally on any computer system or
12 other database and includes recordable tapes and
13 other mass storage devices.

14 (4) **ENCRYPTION.**—The term “encryption”
15 means the protection of data in electronic form in
16 storage or in transit using an encryption technology
17 that has been adopted by an established standards
18 setting body which renders such data indecipherable
19 in the absence of associated cryptographic keys nec-
20 essary to enable decryption of such data. Such
21 encryption must include appropriate management
22 and safeguards of such keys to protect the integrity
23 of the encryption.

24 (5) **IDENTITY THEFT.**—The term “identity
25 theft” means the unauthorized use of another per-
26 son’s personal information for the purpose of engag-

1 ing in commercial transactions under the name of
2 such other person.

3 (6) INFORMATION BROKER.—The term “infor-
4 mation broker” means a commercial entity whose
5 business is to collect, assemble, or maintain personal
6 information concerning individuals who are not cur-
7 rent or former customers of such entity in order to
8 sell such information or provide access to such infor-
9 mation to any nonaffiliated third party in exchange
10 for consideration, whether such collection, assembly,
11 or maintenance of personal information is performed
12 by the information broker directly, or by contract or
13 subcontract with any other entity.

14 (7) 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 or other
22 State identification number.

23 (iii) Financial account number, or
24 credit or debit card number, and any re-
25 quired security code, access code, or pass-

1 word that is necessary to permit access to
2 an individual's financial account.

3 (B) MODIFIED DEFINITION BY RULE-
4 MAKING.—The Commission may, by rule, mod-
5 ify the definition of “personal information”
6 under subparagraph (A) to the extent that such
7 modification is necessary to accommodate
8 changes in technology or practices, will not un-
9 reasonably impede interstate commerce, and
10 will accomplish the purposes of this Act.

11 (8) PERSON.—The term “person” has the same
12 meaning given such term in section 551(2) of title
13 5, United States Code.

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

20 (10) NON-PUBLIC INFORMATION.—The term
21 “non-public information” means information about
22 an individual that is of a private nature and neither
23 available to the general public nor obtained from a
24 public record.

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

2 (a) **PREEMPTION OF STATE INFORMATION SECURITY**
3 **LAWS.**—This Act supersedes any provision of a statute,
4 regulation, or rule of a State or political subdivision of
5 a State, with respect to those entities covered by the regu-
6 lations issued pursuant to this Act, that expressly—

7 (1) requires information security practices and
8 treatment of data in electronic form containing per-
9 sonal information similar to any of those required
10 under section 2; and

11 (2) requires notification to individuals of a
12 breach of security resulting in unauthorized acquisi-
13 tion of data in electronic form containing personal
14 information.

15 (b) **ADDITIONAL PREEMPTION.**—

16 (1) **IN GENERAL.**—No person other than the
17 Attorney General of a State may bring a civil action
18 under the laws of any State if such action is pre-
19 mised in whole or in part upon the defendant vio-
20 lating any provision of this Act.

21 (2) **PROTECTION OF CONSUMER PROTECTION**
22 **LAWS.**—This subsection shall not be construed to
23 limit the enforcement of any State consumer protec-
24 tion law by an Attorney General of a State.

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

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

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

7 (d) PRESERVATION OF FTC AUTHORITY.—Nothing
8 in this Act may be construed in any way to limit or affect
9 the Commission’s authority under any other provision of
10 law, including the authority to issue advisory opinions
11 (under part 1 of volume 16 of the Code of Federal Regula-
12 tions), policy statements, or guidance regarding this Act.

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

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

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

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

20 There is authorized to be appropriated to the Com-
21 mission \$1,000,000 for each of fiscal years 2008 through
22 2012 to carry out this Act.

○