

**AMENDMENT IN THE NATURE OF A SUBSTITUTE**  
**TO H.R. 3997**  
**OFFERED BY MR. STEARNS**

**[Amendment to the Committee Print showing the amendment  
to H.R. 3997 adopted by the Committee on Financial Services]**

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 (DATA)”.

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 enti-  
14 ty maintain such data for such person, to establish  
15 and implement policies and procedures regarding in-  
16 formation security practices for the treatment and



1 protection of personal information taking into  
2 consideration—

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

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

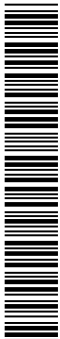
9 (C) the cost of implementing such safe-  
10 guards.

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

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

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

21 (C) A process for identifying and assessing  
22 any reasonably foreseeable vulnerabilities in the  
23 system maintained by such person that contains  
24 such electronic data, which shall include regular



1 monitoring for a breach of security of such sys-  
2 tem.

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

10 (E) A process for disposing of obsolete  
11 data in electronic form containing personal in-  
12 formation by shredding, permanently erasing,  
13 or otherwise modifying the personal information  
14 contained in such data to make such personal  
15 information permanently unreadable or  
16 undecipherable.

17 (3) TREATMENT OF ENTITIES GOVERNED BY  
18 OTHER LAW.—In promulgating the regulations  
19 under this subsection, the Commission may deter-  
20 mine to be in compliance with this subsection any  
21 person who is required under any other Federal law  
22 to maintain standards and safeguards for informa-  
23 tion security and protection of personal information  
24 that provide equal or greater protection than those  
25 required under this subsection.

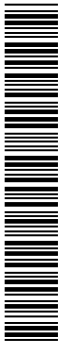


1 (b) DESTRUCTION OF OBSOLETE PAPER RECORDS  
2 CONTAINING PERSONAL INFORMATION.—

3 (1) STUDY.—Not later than 1 year after the  
4 date of enactment of this Act, the Commission shall  
5 conduct a study on the practicality of requiring a  
6 standard method or methods for the destruction of  
7 obsolete paper documents and other non-electronic  
8 data containing personal information by persons en-  
9 gaged in interstate commerce who own or possess  
10 such paper documents and non-electronic data. The  
11 study shall consider the cost, benefit, feasibility, and  
12 effect of a requirement of shredding or other perma-  
13 nent destruction of such paper documents and non-  
14 electronic data.

15 (2) REGULATIONS.—The Commission may pro-  
16 mulgate regulations under section 553 of title 5,  
17 United States Code, requiring a standard method or  
18 methods for the destruction of obsolete paper docu-  
19 ments and other non-electronic data containing per-  
20 sonal information by persons engaged in interstate  
21 commerce who own or possess such paper documents  
22 and non-electronic data if the Commission finds  
23 that—

24 (A) the improper disposal of obsolete paper  
25 documents and other non-electronic data cre-



1           ates a reasonable risk of identity theft, fraud,  
2           or other unlawful conduct;

3           (B) such a requirement would be effective  
4           in preventing identity theft, fraud, or other un-  
5           lawful conduct;

6           (C) the benefit in preventing identity theft,  
7           fraud, or other unlawful conduct would out-  
8           weigh the cost to persons subject to such a re-  
9           quirement; and

10          (D) compliance with such a requirement  
11          would be practicable.

12          In enforcing any such regulations, the Commission  
13          may determine to be in compliance with such regula-  
14          tions any person who is required under any other  
15          Federal law to dispose of obsolete paper documents  
16          and other non-electronic data containing personal in-  
17          formation if such other Federal law provides equal  
18          or greater protection or personal information than  
19          the regulations promulgated under this subsection.

20          (c) 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 their se-  
25          curity 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 shall 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) VERIFICATION OF AND INDIVIDUAL ACCESS  
19 TO PERSONAL INFORMATION.—

20 (A) VERIFICATION.—Each information  
21 broker shall establish reasonable procedures to  
22 verify the accuracy of the personal information  
23 it collects, assembles, or maintains, and any  
24 other information it collects, assembles, or  
25 maintains that specifically identifies an indi-



1           vidual, other than information which merely  
2           identifies an individual's name or address.

3                   (B) CONSUMER ACCESS TO INFORMA-  
4           TION.—

5                   (i) ACCESS.—Each information broker  
6           shall—

7                   (I) provide to each individual  
8           whose personal information it main-  
9           tains, at the individual's request at  
10          least 1 time per year and at no cost  
11          to the individual, and after verifying  
12          the identity of such individual, a  
13          means for the individual to review any  
14          personal information regarding such  
15          individual maintained by the informa-  
16          tion broker and any other information  
17          maintained by the information broker  
18          that specifically identifies such indi-  
19          vidual, other than information which  
20          merely identifies an individual's name  
21          or address; and

22                   (II) place a conspicuous notice on  
23          its Internet website (if the informa-  
24          tion broker maintains such a website)  
25          instructing individuals how to request



1 access to the information required to  
2 be provided under subclause (I).

3 (ii) DISPUTED INFORMATION.—When-  
4 ever an individual whose information the  
5 information broker maintains makes a  
6 written request disputing the accuracy of  
7 any such information, the information  
8 broker, after verifying the identity of the  
9 individual making such request and unless  
10 there are reasonable grounds to believe  
11 such request is frivolous or irrelevant,  
12 shall—

13 (I) correct any inaccuracy; or

14 (II)(aa) in the case of informa-  
15 tion that is public record information,  
16 inform the individual of the source of  
17 the information, and, if reasonably  
18 available, where a request for correc-  
19 tion may be directed; or

20 (bb) in the case of information  
21 that is non-public information, note  
22 the information that is disputed, in-  
23 cluding the individual’s statement dis-  
24 puting such information, and take  
25 reasonable steps to independently ver-





1           ify such information under the proce-  
2           dures outlined in subparagraph (A) if  
3           such information can be independently  
4           verified.

5           (iii) LIMITATIONS.—An information  
6           broker may limit the access to information  
7           required under subparagraph (B) in the  
8           following circumstances:

9                   (I) If access of the individual to  
10                  the information is limited by law or  
11                  legally recognized privilege.

12                  (II) If the information is used for  
13                  a legitimate governmental or fraud  
14                  prevention purpose that would be  
15                  compromised by such access.

16           (iv) RULEMAKING.—The Commission  
17           shall issue regulations, as necessary, under  
18           section 553 of title 5, United States Code,  
19           on the application of the limitations in  
20           clause (iii).

21           (C) TREATMENT OF ENTITIES GOVERNED  
22           BY OTHER LAW.—The Commission may pro-  
23           mulgate rules (under section 553 of title 5,  
24           United States Code) to determine to be in com-  
25           pliance with this paragraph any person who is



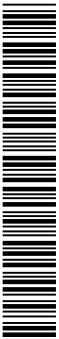
1 a consumer reporting agency, as defined in sec-  
2 tion 603(f) of the Fair Credit Reporting Act,  
3 with respect to those products and services that  
4 are subject to and in compliance with the re-  
5 quirements of that Act.

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

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

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

21 It shall be unlawful for an information broker  
22 to obtain or attempt to obtain, or cause to be  
23 disclosed or attempt to cause to be disclosed to  
24 any person, personal information or any other  
25 information relating to any person by—

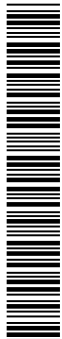


1 (i) making a false, fictitious, or fraud-  
2 ulent statement or representation to any  
3 person; or

4 (ii) providing any document or other  
5 information to any person that the infor-  
6 mation broker knows or should know to be  
7 forged, counterfeit, lost, stolen, or fraudu-  
8 lently obtained, or to contain a false, ficti-  
9 tious, or fraudulent statement or represen-  
10 tation.

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

21 (d) EXEMPTION FOR TELECOMMUNICATIONS CAR-  
22 RIER, CABLE OPERATOR, INFORMATION SERVICE, OR  
23 INTERACTIVE COMPUTER SERVICE.—Nothing in this sec-  
24 tion shall apply to any electronic communication by a third  
25 party stored by a telecommunications carrier, cable oper-



1 ator, or information service, as those terms are defined  
2 in section 3 of the Communications Act of 1934 (47  
3 U.S.C. 153), or an interactive computer service, as such  
4 term is defined in section 230(f)(2) of such Act (47 U.S.C.  
5 230(f)(2)).

6 **SEC. 3. NOTIFICATION OF INFORMATION SECURITY**  
7 **BREACH.**

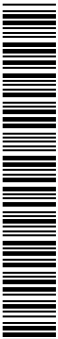
8 (a) NATIONWIDE NOTIFICATION.—Any person en-  
9 gaged in interstate commerce that owns or possesses data  
10 in electronic form containing personal information shall,  
11 following the discovery of a breach of security of the sys-  
12 tem maintained by such person that contains such data—

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

17 (2) notify the Commission.

18 (b) SPECIAL NOTIFICATION REQUIREMENT FOR CER-  
19 TAIN ENTITIES.—

20 (1) THIRD PARTY AGENTS.—In the event of a  
21 breach of security by any third party entity that has  
22 been contracted to maintain or process data in elec-  
23 tronic form containing personal information on be-  
24 half of any other person who owns or possesses such  
25 data, such third party entity shall be required only



1 to notify such person of the breach of security. Upon  
2 receiving such notification from such third party,  
3 such person shall provide the notification required  
4 under subsection (a).

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



1       tion service, or interactive computer service, such  
2       person shall provide the notification required under  
3       subsection (a).

4               (3) BREACH OF HEALTH INFORMATION.—If the  
5       Commission receives a notification of a breach of se-  
6       curity and determines that information included in  
7       such breach is individually identifiable health infor-  
8       mation (as such term is defined in section 1171(6)  
9       of the Social Security Act (42 U.S.C. 1320d(6)), the  
10      Commission shall send a copy of such notification to  
11      the Secretary of Health and Human Services.

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

20              (d) METHOD AND CONTENT OF NOTIFICATION.—

21                      (1) DIRECT NOTIFICATION.—

22                              (A) METHOD OF NOTIFICATION.—A person  
23                      required to provide notification to individuals  
24                      under subsection (a)(1) shall be in compliance  
25                      with such requirement if the person provides



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

5 (i) Written notification.

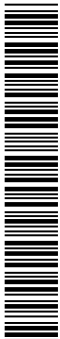
6 (ii) Email notification, if—

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

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

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

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

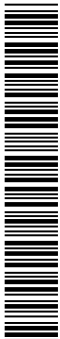
7 (iii) notice that the individual is enti-  
8 tled to receive, at no cost to such indi-  
9 vidual, consumer credit reports on a quar-  
10 terly basis for a period of 2 years, and in-  
11 structions to the individual on requesting  
12 such reports from the person;

13 (iv) the toll-free contact telephone  
14 numbers and addresses for the major cred-  
15 it reporting agencies; and

16 (v) a toll-free telephone number and  
17 Internet website address for the Commis-  
18 sion whereby the individual may obtain in-  
19 formation regarding identity theft.

20 (2) SUBSTITUTE NOTIFICATION.—

21 (A) CIRCUMSTANCES GIVING RISE TO SUB-  
22 STITUTE NOTIFICATION.—A person required to  
23 provide notification to individuals under sub-  
24 section (a)(1) may provide substitute notifica-





1           tion in lieu of the direct notification required by  
2           paragraph (1) if—

3                   (i) the person owns or possesses data  
4                   in electronic form containing personal in-  
5                   formation of fewer than 1,000 individuals;  
6                   and

7                   (ii) such direct notification is not fea-  
8                   sible due to—

9                           (I) excessive cost to the person  
10                           required to provide such notification  
11                           relative to the resources of such per-  
12                           son, as determined in accordance with  
13                           the regulations issued by the Commis-  
14                           sion under paragraph (3)(A); or

15                           (II) lack of sufficient contact in-  
16                           formation for the individual required  
17                           to be notified.

18                   (B) FORM OF SUBSTITUTE NOTICE.—Such  
19                   substitute notification shall include—

20                           (i) email notification to the extent  
21                           that the person has email addresses of in-  
22                           dividuals to whom it is required to provide  
23                           notification under subsection (a)(1);



1 (ii) a conspicuous notice on the Inter-  
 2 net website of the person (if such person  
 3 maintains such a website); and

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

9 (C) CONTENT OF SUBSTITUTE NOTICE.—

10 Each form of substitute notice under this para-  
 11 graph shall include—

12 (i) notice that individuals whose per-  
 13 sonal information is included in the breach  
 14 of security are entitled to receive, at no  
 15 cost to the individuals, consumer credit re-  
 16 ports on a quarterly basis for a period of  
 17 2 years, and instructions on requesting  
 18 such reports from the person; and

19 (ii) a telephone number by which an  
 20 individual can, at no cost to such indi-  
 21 vidual, learn whether that individual's per-  
 22 sonal information is included in the breach  
 23 of security.

24 (3) FEDERAL TRADE COMMISSION REGULA-  
 25 TIONS AND GUIDANCE.—



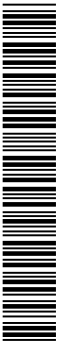
1 (A) REGULATIONS.—Not later than 1 year  
2 after the date of enactment of this Act, the  
3 Commission shall, by regulations under section  
4 553 of title 5, United States Code, establish cri-  
5 teria for determining the circumstances under  
6 which substitute notification may be provided  
7 under paragraph (2), including criteria for de-  
8 termining if notification under paragraph (1) is  
9 not feasible due to excessive cost to the person  
10 required to provide such notification relative to  
11 the resources of such person.

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

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

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

24 (e) OTHER OBLIGATIONS FOLLOWING BREACH.—A  
25 person required to provide notification under subsection



1 (a) shall, upon request of an individual whose personal in-  
2 formation was included in the breach of security, provide  
3 or arrange for the provision of, to each such individual  
4 and at no cost to such individual, consumer credit reports  
5 from at least one of the major credit reporting agencies  
6 beginning not later than 2 months following the discovery  
7 of a breach of security and continuing on a quarterly basis  
8 for a period of 2 years thereafter.

9 (f) EXEMPTION.—

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

15 (2) PRESUMPTIONS.—

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

24 (B) ADDITIONAL METHODOLOGIES OR  
25 TECHNOLOGIES.—Not later than 270 days after



1 the date of the enactment of this Act, the Com-  
2 mission shall, by rule pursuant to section 553  
3 of title 5, United States Code, identify any ad-  
4 ditional security methodology or technology,  
5 other than encryption, which renders data in  
6 electronic form unreadable or indecipherable,  
7 that shall, if applied to such data, establish a  
8 presumption that no reasonable risk of identity  
9 theft, fraud, or other unlawful conduct exists  
10 following a breach of security of such data. Any  
11 such presumption may be rebutted by facts  
12 demonstrating that any such methodology or  
13 technology has been or is reasonably likely to be  
14 compromised. In promulgating such a rule, the  
15 Commission shall consult with relevant indus-  
16 tries, consumer organizations, and data security  
17 and identity theft prevention experts and estab-  
18 lished standards setting bodies.

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

23 (g) WEBSITE NOTICE OF FEDERAL TRADE COMMIS-  
24 SION.—If the Commission, upon receiving notification of  
25 any breach of security that is reported to the Commission



1 under subsection (a)(2), finds that notification of such a  
2 breach of security via the Commission's Internet website  
3 would be in the public interest or for the protection of  
4 consumers, the Commission shall place such a notice in  
5 a clear and conspicuous location on its Internet website.

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

13 **SEC. 4. ENFORCEMENT.**

14 (a) ENFORCEMENT BY THE FEDERAL TRADE COM-  
15 MISSION.—

16 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-  
17 TICES.—A violation of section 2 or 3 shall be treated  
18 as an unfair and deceptive act or practice in viola-  
19 tion of a regulation under section 18(a)(1)(B) of the  
20 Federal Trade Commission Act (15 U.S.C.  
21 57a(a)(1)(B)) regarding unfair or deceptive acts or  
22 practices.

23 (2) POWERS OF COMMISSION.—The Commis-  
24 sion shall enforce this Act in the same manner, by  
25 the same means, and with the same jurisdiction,



1 powers, and duties as though all applicable terms  
2 and provisions of the Federal Trade Commission Act  
3 (15 U.S.C. 41 et seq.) were incorporated into and  
4 made a part of this Act. Any person who violates  
5 such regulations shall be subject to the penalties and  
6 entitled to the privileges and immunities provided in  
7 that Act.

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

13 (b) ENFORCEMENT BY STATE ATTORNEYS GEN-  
14 ERAL.—

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



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

3 (B) to compel compliance with such sec-  
4 tion; or

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

7 (2) CIVIL PENALTIES.—

8 (A) CALCULATION.—

9 (i) TREATMENT OF VIOLATIONS OF  
10 SECTION 2.—For purposes of paragraph  
11 (1)(C) with regard to a violation of section  
12 2, 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 day that a person is not in  
17 compliance with the requirements of such  
18 section shall be treated as a separate viola-  
19 tion. The maximum civil penalty calculated  
20 under this clause shall not exceed  
21 \$5,000,000.

22 (ii) TREATMENT OF VIOLATIONS OF  
23 SECTION 3.—For purposes of paragraph  
24 (1)(C) with regard to a violation of section  
25 3, the amount determined under this para-





1 graph is the amount calculated by multi-  
2 plying the number of violations of such  
3 section by an amount not greater than  
4 \$11,000. Each failure to send notification  
5 as required under section 3 to a resident of  
6 the State shall be treated as a separate  
7 violation. The maximum civil penalty cal-  
8 culated under this clause shall not exceed  
9 \$5,000,000.

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

20 (3) INTERVENTION BY THE FTC.—

21 (A) NOTICE AND INTERVENTION.—The  
22 State shall provide prior written notice of any  
23 action under paragraph (1) to the Commission  
24 and provide the Commission with a copy of its  
25 complaint, except in any case in which such



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

5 (i) to intervene in the action;

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

8 (iii) to file petitions for appeal.

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

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

24 (A) conduct investigations;

25 (B) administer oaths or affirmations; or



1 (C) compel the attendance of witnesses or  
2 the production of documentary and other evi-  
3 dence.

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

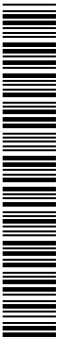
14 **SEC. 5. DEFINITIONS.**

15 In this Act the following definitions apply:

16 (1) BREACH OF SECURITY.—The term “breach  
17 of security” means the unauthorized acquisition of  
18 data in electronic form containing personal informa-  
19 tion.

20 (2) COMMISSION.—The term “Commission”  
21 means the Federal Trade Commission.

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



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

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

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

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



1 or maintenance of personal information is performed  
2 by the information broker directly, or by contract or  
3 subcontract with any other entity.

4 (7) PERSONAL INFORMATION.—

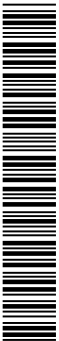
5 (A) DEFINITION.—The term “personal in-  
6 formation” means an individual’s first name or  
7 initial and last name, or address, or phone  
8 number, in combination with any 1 or more of  
9 the following data elements for that individual:

10 (i) Social Security number.

11 (ii) Driver’s license number or other  
12 State identification number.

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

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



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

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

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

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

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

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



1 (b) ADDITIONAL PREEMPTION.—

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

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

11 (c) PROTECTION OF CERTAIN STATE LAWS.—This  
12 Act shall not be construed to preempt the applicability  
13 of—

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

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

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

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

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



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

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

5 There is authorized to be appropriated to the Com-  
6 mission \$1,000,000 for each of fiscal years 2006 through  
7 2010 to carry out this Act.

Amend the title so as to read “To protect consumers  
by requiring reasonable security policies and procedures  
to protect computerized data containing personal infor-  
mation, and to provide for nationwide notice in the event  
of a security breach.”.

