

112TH CONGRESS  
1ST SESSION

# H. R. 2577

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

---

## IN THE HOUSE OF REPRESENTATIVES

JULY 18, 2011

Mrs. BONO MACK 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 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 “Secure and Fortify  
5       Electronic Data Act” or the “SAFE Data Act”.

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

7       (a) GENERAL SECURITY POLICIES AND PROCE-

8       DURES.—

1           (1) REGULATIONS.—Not later than 1 year after  
2 the date of enactment of this Act, the Commission  
3 shall promulgate regulations under section 553 of  
4 title 5, United States Code, to require any person  
5 engaged in interstate commerce that owns or pos-  
6 sesses data containing personal information related  
7 to that commercial activity, including an information  
8 broker and any third party that has contracted with  
9 such person to maintain or process such data on be-  
10 half of such person, to establish and implement rea-  
11 sonable policies and procedures regarding informa-  
12 tion security practices for the treatment and protec-  
13 tion of personal information, taking into consider-  
14 ation—

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

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

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

23           (2) DATA SECURITY REQUIREMENTS.—Such  
24 regulations shall, taking into consideration the quan-  
25 tity, type, nature, and sensitivity of the personal in-

1       formation, require the policies and procedures to in-  
2       clude the following:

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

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

10              (C) A process for identifying and assessing  
11              any reasonably foreseeable vulnerabilities in  
12              each system maintained by such person that  
13              contains such data, which shall include regular  
14              monitoring to detect a breach of security of  
15              each such system.

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

23              (E) A process for disposing of data in elec-  
24              tronic form containing personal information by  
25              shredding, permanently erasing, or otherwise

1           modifying the personal information contained in  
2           such data to make such personal information  
3           permanently unreadable or indecipherable.

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

7           (b) DATA MINIMIZATION REQUIREMENTS.—A person  
8           subject to the requirements under subsection (a) shall es-  
9           tablish a plan and procedures for minimizing the amount  
10          of personal information maintained by such person. Such  
11          plan and procedures shall provide for the retention of such  
12          personal information only as reasonably needed for the  
13          business purposes of such person or as necessary to com-  
14          ply with any legal obligation.

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

20       **SEC. 3. NOTIFICATION AND OTHER REQUIREMENTS IN THE**  
21                               **EVENT OF A BREACH OF SECURITY.**

22          (a) REQUIREMENTS IN THE EVENT OF A BREACH OF  
23          SECURITY.—Any person engaged in interstate commerce  
24          that owns or possesses data in electronic form containing  
25          personal information related to that commercial activity,

1 following the discovery of a breach of security of any sys-  
2 tem maintained by such person that contains such data,  
3 shall, without unreasonable delay—

4 (1) notify appropriate Federal law enforcement  
5 officials of the breach of security, unless such person  
6 determines that the breach involved no unlawful ac-  
7 tivity;

8 (2) take such steps necessary to prevent further  
9 breach or unauthorized disclosures;

10 (3) identify affected individuals whose personal  
11 information may have been acquired or accessed;  
12 and

13 (4) not later than 48 hours after identifying af-  
14 fected individuals under paragraph (3), unless the  
15 person makes a reasonable determination that the  
16 breach of security presents no reasonable risk of  
17 identity theft, fraud, or other unlawful conduct af-  
18 fecting such individuals, notify—

19 (A) the Commission; and

20 (B) as promptly as possible, subject to  
21 subsection (c), each individual who is a citizen  
22 or resident of the United States whose personal  
23 information is known to have been acquired or  
24 accessed as a result of such a breach of secu-  
25 rity.

1 (b) SPECIAL NOTIFICATION REQUIREMENTS.—

2 (1) THIRD PARTY AGENTS.—In the event of a  
3 breach of security of any third party entity that has  
4 contracted with a person to maintain or process data  
5 in electronic form containing personal information  
6 on behalf of such person, such third party entity  
7 shall—

8 (A) take the actions required under para-  
9 graphs (1) and (2) of subsection (a); and

10 (B) notify as promptly as possible such  
11 person of the breach of security.

12 Upon receiving notification from the third party en-  
13 tity under subparagraph (B), such person shall take  
14 the actions required under paragraphs (3) and (4)  
15 of subsection (a).

16 (2) SERVICE PROVIDERS.—If a service provider  
17 becomes aware of a breach of security of data in  
18 electronic form containing personal information that  
19 is owned or possessed by another person engaged in  
20 interstate commerce that connects to or uses a sys-  
21 tem or network provided by the service provider for  
22 the purpose of transmitting, routing, or providing in-  
23 termediate or transient storage of such data in con-  
24 nection with that commercial activity, such service  
25 provider shall—

1 (A) take the actions required under para-  
2 graphs (1) and (2) of subsection (a); and

3 (B) notify only the person who initiated  
4 such connection, transmission, routing, or stor-  
5 age, of the breach of security, if such person  
6 can be reasonably identified.

7 Upon receiving such notification from a service pro-  
8 vider, such person shall take the action required  
9 under paragraphs (3) and (4) of subsection (a).

10 (3) COORDINATION OF NOTIFICATION WITH  
11 CREDIT REPORTING AGENCIES.—If a person is re-  
12 quired to provide notification to more than 5,000 in-  
13 dividuals under subsection (a)(4)(B), the person  
14 shall also notify the major credit reporting agencies  
15 that compile and maintain files on consumers on a  
16 nationwide basis of the timing and distribution of  
17 the notices. Such notice shall be given to the credit  
18 reporting agencies without unreasonable delay and,  
19 if it will not delay notice to the affected individuals,  
20 prior to the distribution of notices to the affected in-  
21 dividuals.

22 (c) TIMING AND DELAY OF NOTIFICATION AUTHOR-  
23 IZED FOR LAW ENFORCEMENT OR NATIONAL SECURITY  
24 PURPOSES.—

1           (1) DEADLINE FOR COMMENCING NOTIFICA-  
2           TION.—Except as provided under paragraph (2) or  
3           (3), a person required to provide notification to indi-  
4           viduals of a breach of security pursuant to sub-  
5           section (a)(4)(B) shall begin to notify such individ-  
6           uals not later than 45 days after discovery of such  
7           breach.

8           (2) LAW ENFORCEMENT.—If a Federal law en-  
9           forcement agency determines that the notification  
10          required under subsection (a)(4)(B) would impede a  
11          civil or criminal investigation, such notification shall  
12          be delayed upon the request of the law enforcement  
13          agency for 30 days or such lesser period of time that  
14          the law enforcement agency determines is reasonably  
15          necessary. The law enforcement agency shall follow  
16          up such a request in writing. A law enforcement  
17          agency may, by a subsequent written request, revoke  
18          such delay or extend the period of time set forth in  
19          the original request made under this paragraph if  
20          further delay is necessary.

21          (3) NATIONAL SECURITY.—If a Federal na-  
22          tional security agency or homeland security agency  
23          determines that the notification required under sub-  
24          section (a)(4)(B) would threaten national or home-  
25          land security, such notification may be delayed for



1 a period of time that the national security agency or  
2 homeland security agency determines is reasonably  
3 necessary. The national security agency or homeland  
4 security agency shall follow up such a request in  
5 writing. A Federal national security agency or home-  
6 land security agency may revoke such delay or ex-  
7 tend the period of time set forth in the original re-  
8 quest made under this paragraph by a subsequent  
9 written request if further delay is necessary.

10 (d) METHOD AND CONTENT OF NOTIFICATION.—

11 (1) DIRECT NOTIFICATION.—

12 (A) METHOD OF NOTIFICATION.—A person  
13 required to provide notification to individuals  
14 under subsection (a)(4)(B) shall be in compli-  
15 ance with such requirement if the person pro-  
16 vides a conspicuous and clearly identified notifi-  
17 cation by one of the following methods (pro-  
18 vided the selected method can reasonably be ex-  
19 pected to reach the intended individual):

20 (i) Written notification.

21 (ii) Notification by email or other  
22 electronic means, if—

23 (I) the person's primary method  
24 of communication with the individual

1 is by email or such other electronic  
2 means; or

3 (II) the individual has consented  
4 to receive such notification and the  
5 notification is provided in a manner  
6 that is consistent with the provisions  
7 permitting electronic transmission of  
8 notices under section 101 of the Elec-  
9 tronic Signatures in Global and Na-  
10 tional Commerce Act (15 U.S.C.  
11 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 may have been acquired or  
18 accessed by an unauthorized 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, or credit  
5 monitoring or other service that enables  
6 consumers to detect the misuse of their  
7 personal information for a period of 2  
8 years, and instructions to the individual on  
9 requesting such reports or service from the  
10 person, except when the only information  
11 which has been the subject of the security  
12 breach is the individual's first name or ini-  
13 tial and last name, or address, or phone  
14 number, in combination with a credit or  
15 debit card number, and any required secu-  
16 rity code;

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

20 (v) a toll-free telephone number and  
21 website address for the Commission where-  
22 by the individual may obtain information  
23 regarding identity theft.

24 (2) SUBSTITUTE NOTIFICATION.—

1 (A) CIRCUMSTANCES GIVING RISE TO SUB-  
2 STITUTE NOTIFICATION.—A person required to  
3 provide notification to individuals under sub-  
4 section (a)(4)(B) may provide substitute notifi-  
5 cation in lieu of the direct notification required  
6 by paragraph (1) if the person owns or pos-  
7 sesses data in electronic form containing per-  
8 sonal information of fewer than 1,000 individ-  
9 uals and such direct notification is not feasible  
10 due to—

11 (i) excessive cost to the person re-  
12 quired to provide such notification relative  
13 to the resources of such person, as deter-  
14 mined in accordance with the regulations  
15 issued by the Commission under paragraph  
16 (3)(A); or

17 (ii) lack of sufficient contact informa-  
18 tion for the individual required to be noti-  
19 fied.

20 (B) FORM OF SUBSTITUTE NOTIFICA-  
21 TION.—Such substitute notification shall in-  
22 clude—

23 (i) email notification to the extent  
24 that the person has email addresses of in-

1 individuals to whom it is required to provide  
2 notification under subsection (a)(4)(B);

3 (ii) a conspicuous notice on the  
4 website of the person (if such person main-  
5 tains a website); and

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

11 (C) CONTENT OF SUBSTITUTE NOTICE.—

12 Each form of substitute notice under this para-  
13 graph shall include—

14 (i) notice that individuals whose per-  
15 sonal information is included in the breach  
16 of security are entitled to receive, at no  
17 cost to the individuals, consumer credit re-  
18 ports on a quarterly basis for a period of  
19 2 years, or credit monitoring or other serv-  
20 ice that enables consumers to detect the  
21 misuse of their personal information for a  
22 period of 2 years, and instructions on re-  
23 questing such reports or service from the  
24 person, except when the only information  
25 which has been the subject of the security

1 breach is the individual's first name or ini-  
2 tial and last name, or address, or phone  
3 number, in combination with a credit or  
4 debit card number, and any required secu-  
5 rity code; 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) REGULATIONS AND GUIDANCE.—

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

1           which the cost of providing notification exceeds  
2           the benefits to consumers.

3           (B) GUIDANCE.—In addition, the Commis-  
4           sion shall provide and publish general guidance  
5           with respect to compliance with this subsection.  
6           Such guidance shall include—

7                   (i) a description of written or email  
8                   notification that complies with the require-  
9                   ments of paragraph (1); and

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

15           (e) OTHER OBLIGATIONS FOLLOWING BREACH.—

16                   (1) IN GENERAL.—A person required to provide  
17                   notification under subsection (a)(4)(B) shall, in ac-  
18                   cordance with the determination described in para-  
19                   graph (3), upon request of an individual whose per-  
20                   sonal information was included in the breach of se-  
21                   curity, provide or arrange for the provision of, to  
22                   each such individual and at no cost to such indi-  
23                   vidual—

24                           (A) consumer credit reports from at least  
25                   one of the major credit reporting agencies be-

1           ginning not later than 60 days following the in-  
2           dividual's request and continuing on a quarterly  
3           basis for a period of 2 years thereafter; or

4           (B) a credit monitoring or other service  
5           that enables consumers to detect the misuse of  
6           their personal information, beginning not later  
7           than 60 days following the individual's request  
8           and continuing for a period of 2 years.

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

15          (3) RULEMAKING.—As part of the Commis-  
16          sion's rulemaking described in subsection (d)(3), the  
17          Commission shall determine the circumstances under  
18          which a person required to provide notification  
19          under subsection (a)(4)(B) shall provide or arrange  
20          for the provision of free consumer credit reports or  
21          credit monitoring or other service to affected individ-  
22          uals.

23          (f) PRESUMPTION CONCERNING DATA IN CERTAIN  
24          FORMS.—



1           (1) IN GENERAL.—If the data in electronic  
2 form containing personal information is unusable,  
3 unreadable, or indecipherable to an unauthorized  
4 person by encryption or other security technology or  
5 methodology (if the method of encryption or such  
6 other technology or methodology is generally accept-  
7 ed by experts in the information security field),  
8 there shall be a presumption, for purposes of sub-  
9 section (a)(4), that no reasonable risk of identity  
10 theft, fraud, or other unlawful conduct exists fol-  
11 lowing a breach of security of such data. Any such  
12 presumption may be rebutted by facts demonstrating  
13 that the encryption or other security technologies or  
14 methodologies in a specific case have been or are  
15 reasonably likely to be compromised.

16           (2) METHODOLOGIES OR TECHNOLOGIES.—The  
17 Commission may issue guidance to identify security  
18 methodologies or technologies that render data in  
19 electronic form unusable, unreadable, or indecipher-  
20 able, 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 fol-  
23 lowing a breach of security of such data. Any such  
24 presumption may be rebutted by facts demonstrating  
25 that any such methodology or technology in a spe-

1       cific case has been or is reasonably likely to be com-  
2       promised. In issuing such rules or guidance, the  
3       Commission shall consult with relevant industries,  
4       consumer organizations, and data security and iden-  
5       tity theft prevention experts and established stand-  
6       ards setting bodies.

7       (g) WEBSITE NOTICE OF FEDERAL TRADE COMMIS-  
8       SION.—If the Commission, upon receiving notification of  
9       any breach of security that is reported to the Commission  
10      under subsection (a)(4)(A), finds that notification of such  
11      a breach of security available on the Commission’s website  
12      would be in the public interest or for the protection of  
13      consumers, the Commission may place such a notice in  
14      a clear and conspicuous location on such website.

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

22      (i) GENERAL RULEMAKING AUTHORITY.—The Com-  
23      mission may promulgate regulations, pursuant to section  
24      553 of title 5, United States Code, as necessary to effec-

1 tively implement and enforce the requirements of this sec-  
2 tion.

3 **SEC. 4. APPLICATION AND ENFORCEMENT.**

4 (a) GENERAL APPLICATION.—The requirements of  
5 sections 2 and 3 apply, according to their terms, to—

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

10 (2) notwithstanding section 4 and section  
11 5(a)(2) of that Act (15 U.S.C. 44 and 45(a)(2)),  
12 any organization described in section 501(c) of the  
13 Internal Revenue Code of 1986 that is exempt from  
14 taxation under section 501(a) of such Code.

15 (b) ENFORCEMENT BY THE FEDERAL TRADE COM-  
16 MISSION.—

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

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

1 the same means, and with the same jurisdiction,  
2 powers, and duties as though all applicable terms  
3 and provisions of the Federal Trade Commission Act  
4 (15 U.S.C. 41 et seq.) were incorporated into and  
5 made a part of this Act. Any person who violates  
6 section 2 or 3 shall be subject to the penalties and  
7 entitled to the privileges and immunities provided in  
8 that Act, except that the Commission may not assess  
9 civil penalties for a violation of section 3(a)(1).

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

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

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

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

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

3 (2) CIVIL PENALTIES.—

4 (A) CALCULATION.—

5 (i) TREATMENT OF VIOLATIONS OF  
6 SECTION 2.—For purposes of paragraph  
7 (1)(C) with regard to a violation of section  
8 2, the amount determined under this para-  
9 graph is the amount calculated by multi-  
10 plying the number of days that a person is  
11 not in compliance with such section by an  
12 amount not greater than \$11,000.

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

24 (B) ADJUSTMENT FOR INFLATION.—Be-  
25 ginning on the date that the Consumer Price

1 Index is first published by the Bureau of Labor  
2 Statistics that is at least 1 year after the date  
3 of enactment of this Act, and each year there-  
4 after, the amounts specified in clauses (i) and  
5 (ii) of subparagraph (A) shall be increased by  
6 the percentage increase in the Consumer Price  
7 Index published on that date from the Con-  
8 sumer Price Index published the previous year.

9 (C) MAXIMUM TOTAL LIABILITY.—Not-  
10 withstanding the number of actions which may  
11 be brought against a person under this sub-  
12 section, the maximum civil penalty for which  
13 any person may be liable under this subsection  
14 shall not exceed—

15 (i) \$5,000,000 for all related viola-  
16 tions of section 2; and

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

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           (d) ENTITIES GOVERNED BY HIPAA AND GRAMM-  
5 LEACH-BLILEY.—

6           (1) HIPAA.—

7           (A) INFORMATION SECURITY REQUIRE-  
8           MENTS.—To the extent that the information se-  
9           curity requirements of part C of title XI of the  
10          Social Security Act (42 U.S.C. 1320d et seq.)  
11          apply in any circumstance to a person who is  
12          subject to such part, including as applied under  
13          subtitle D of title IV of the Health Information  
14          Technology for Economic and Clinical Health  
15          Act (42 U.S.C. 17921 et seq.), such person  
16          shall be exempt from the requirements of sec-  
17          tion 2.

18          (B) NOTIFICATION REQUIREMENTS.—To  
19          the extent that the breach notification require-  
20          ments of part C of title XI of the Social Secu-  
21          rity Act (42 U.S.C. 1320d et seq.) apply in any  
22          circumstance to a person who is subject to such  
23          part, including as applied under subtitle D of  
24          title IV of the Health Information Technology  
25          for Economic and Clinical Health Act (42



1 U.S.C. 17921 et seq.), such person shall be ex-  
2 empt from the requirements of section 3.

3 (2) GRAMM-LEACH-BLILEY.—

4 (A) IN GENERAL.—Except as provided in  
5 subparagraph (B), a person who is subject to  
6 title V of the Gramm-Leach-Bliley Act (15  
7 U.S.C. 6801 et seq.)—

8 (i) with regard to information security  
9 requirements, shall be exempt from the re-  
10 quirements of section 2; and

11 (ii) with regard to notification require-  
12 ments, shall be exempt from the require-  
13 ments of section 3.

14 (B) EXCEPTION.—Notwithstanding sub-  
15 paragraph (A), those persons subject to the ju-  
16 risdiction of the Federal Trade Commission  
17 under section 505(a)(7) of the Gramm-Leach-  
18 Bliley Act (15 U.S.C. 6805) shall be subject to  
19 the requirements of this Act. If such person is  
20 in compliance with the information security re-  
21 quirements of title V of such Act, such person  
22 shall be deemed in compliance with section 2 of  
23 this Act.

24 **SEC. 5. DEFINITIONS.**

25 In this Act the following definitions apply:

1           (1) BREACH OF SECURITY.—The term “breach  
2 of security” means any unauthorized access to or ac-  
3 quisition of data in electronic form containing per-  
4 sonal information.

5           (2) COMMISSION.—The term “Commission”  
6 means the Federal Trade Commission.

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

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

22           (5) IDENTITY THEFT.—The term “identity  
23 theft” means the unauthorized use of another per-  
24 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”—

5               (A) means a commercial entity whose busi-  
6       ness is to collect, assemble, or maintain per-  
7       sonal information concerning individuals who  
8       are not current or former customers of such en-  
9       tity in order to sell such information or provide  
10      access to such information to any nonaffiliated  
11      third party in exchange for consideration,  
12      whether such collection, assembly, or mainte-  
13      nance of personal information is performed by  
14      the information broker directly, or by contract  
15      or subcontract with any other entity; and

16              (B) does not include a commercial entity to  
17      the extent that such entity processes informa-  
18      tion collected by or on behalf of and received  
19      from or on behalf of a nonaffiliated third party  
20      concerning individuals who are current or  
21      former customers or employees of such third  
22      party to enable such third party directly or  
23      through parties acting on its behalf to provide  
24      benefits for its employees or directly transact  
25      business with its customers.

1 (7) PERSONAL INFORMATION.—

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

7 (i) Social Security number.

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

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

17 (B) PUBLIC RECORD INFORMATION.—Such  
18 term does not include public record information.

19 (C) MODIFIED DEFINITION BY RULE-  
20 MAKING.—The Commission may, by rule pro-  
21 mulgated under section 553 of title 5, United  
22 States Code, modify the definition of “personal  
23 information” under subparagraph (A)—

24 (i) for the purpose of section 2, to the  
25 extent that such modification is necessary

1 to accomplish the purposes of such section  
2 as a result of changes in technology or  
3 practices and will not unreasonably impede  
4 technological innovation or otherwise ad-  
5 versely affect interstate commerce; and

6 (ii) for the purpose of section 3, if the  
7 Commission determines that access to or  
8 acquisition of the additional data elements  
9 in the event of a breach of security would  
10 create an unreasonable risk of identity  
11 theft, fraud, or other unlawful conduct and  
12 that such modification will not unreason-  
13 ably impede technological innovation or  
14 otherwise adversely affect interstate com-  
15 merce.

16 (8) PUBLIC RECORD INFORMATION.—The term  
17 “public record information” means information  
18 about an individual that is lawfully made available  
19 to the general public from Federal, State, or local  
20 government records.

21 (9) SERVICE PROVIDER.—The term “service  
22 provider” means a person that provides electronic  
23 data transmission, routing, intermediate and tran-  
24 sient storage, or connections to its system or net-  
25 work, where the person providing such services does

1 not select or modify the content of the electronic  
2 data, is not the sender or the intended recipient of  
3 the data, and does not differentiate personal infor-  
4 mation from other information that such person  
5 transmits, routes, or stores, or for which such per-  
6 son provides connections. Any such person shall be  
7 treated as a service provider under this Act only to  
8 the extent that it is engaged in the provision of such  
9 transmission, routing, intermediate and transient  
10 storage, or connections.

11 **SEC. 6. RELATION TO OTHER LAWS AND CONFORMING**  
12 **AMENDMENTS.**

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 any entity subject to this Act, that  
17 contains—

18 (1) requirements for information security prac-  
19 tices or treatment of data similar to those under sec-  
20 tion 2; or

21 (2) requirements for notification of a breach of  
22 security similar to the notification required under  
23 section 3.

24 (b) **ADDITIONAL PREEMPTION.**—

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

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

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

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

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

16          (d) PRESERVATION OF FTC AUTHORITY.—Nothing  
17          in this Act may be construed in any way to limit or affect  
18          the Commission’s authority under any other provision of  
19          law.

20          (e) CONFORMING AMENDMENT.—Section 631(c)(1)  
21          of the Communications Act of 1934 (47 U.S.C. 551(c)(1))  
22          is amended by striking “and shall take such actions as  
23          are necessary to prevent unauthorized access to such in-  
24          formation by a person other than the subscriber or cable  
25          operator”.

1 **SEC. 7. EFFECTIVE DATE.**

2       This Act shall take effect 1 year after the date of  
3 enactment of this Act.

○