

[DISCUSSION DRAFT]

JUNE 10, 2011

112TH CONGRESS
1ST SESSION**H. R.** _____

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

Mrs. BONO MACK introduced the following bill; which was referred to the Committee on _____

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”.

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 any person
8 engaged in interstate commerce that owns or pos-
9 sesses data containing personal information related
10 to that commercial activity, including an information
11 broker and any third party that has contracted with
12 such person to maintain such data on behalf of such
13 person, to establish and implement policies and pro-
14 cedures regarding information security practices for
15 the treatment and protection of personal informa-
16 tion, taking into consideration—

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

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

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

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

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

7 (B) The identification of an officer [or
8 other individual] as the point of contact with
9 responsibility for the management of informa-
10 tion security.

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

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

24 (E) A process for disposing of data in elec-
25 tronic form containing personal information by

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

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

8 **[(3) DATA MINIMIZATION REQUIREMENTS.—A**
9 person subject to the requirements under paragraph
10 (1) shall establish a plan and procedures for mini-
11 mizing the amount of data containing personal infor-
12 mation maintained by such person. Such a plan and
13 procedures shall provide for the retention of such
14 personal information only as reasonably needed for
15 the legitimate business purposes of such person or
16 as necessary to comply with any legal obligation.]

17 (b) TREATMENT OF ENTITIES GOVERNED BY HIPAA
18 AND GRAMM-LEACH-BLILEY.—Any person who is subject
19 to the requirements of part C of title XI of the Social
20 Security Act (42 U.S.C. 1301 et seq.) or title V of the
21 Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) to
22 maintain standards and safeguards for information secu-
23 rity and protection of personal information shall be ex-
24 empt from the requirements of this Act for any activities
25 governed by such requirements under such Acts.

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

6 **SEC. 3. NOTIFICATION AND OTHER REQUIREMENTS IN THE**
7 **EVENT OF A BREACH OF SECURITY.**

8 (a) REQUIREMENTS IN THE EVENT OF A BREACH OF
9 SECURITY.—Any person engaged in interstate commerce
10 that owns or possesses data in electronic form containing
11 personal information related to that commercial activity,
12 following the discovery of a breach of security of any sys-
13 tem maintained by such person that contains such data,
14 shall—

15 (1)(A) notify appropriate law enforcement offi-
16 cials of the breach of security not later than 48
17 hours after such discovery, unless the breach of se-
18 curity involved only inadvertent access to or inad-
19 vertent acquisition of data by an employee or agent
20 of such person; and

21 (B) if the person subsequently determines that
22 the breach of security was not inadvertent, notify
23 appropriate law enforcement officials of the breach
24 of security not later than 48 hours after such deter-
25 mination;

1 (2) assess the nature and scope of such a
2 breach of security, take such steps necessary to pre-
3 vent further breach or unauthorized disclosures, and
4 reasonably restore the integrity of the data system;
5 and

6 (3) not later than 48 hours after completing the
7 assessment required under paragraph (2), if the per-
8 son determines, based on such assessment, that the
9 breach of security presents a reasonable risk of iden-
10 tity theft, fraud, or other unlawful conduct—

11 (A) notify the Commission; and

12 (B) begin to notify as promptly as possible,
13 subject to subsection (c), each individual who is
14 a citizen or resident of the United States whose
15 personal information was acquired or accessed
16 as a result of such a breach of security.

17 (b) SPECIAL NOTIFICATION REQUIREMENTS.—

18 (1) THIRD PARTY AGENTS.—In the event of a
19 breach of security of any third party entity that has
20 contracted with a person to maintain or process data
21 in electronic form containing personal information
22 on behalf of such person, such third party entity
23 shall be required to notify such person of the breach
24 of security. Upon receiving such notification from

1 the third party, such person shall take the actions
2 required under subsection (a).

3 (2) SERVICE PROVIDERS.—If a service provider
4 becomes aware of a breach of security of data in
5 electronic form containing personal information that
6 is owned or possessed by another person that con-
7 nects to or uses a system or network provided by the
8 service provider for the purpose of transmitting,
9 routing, or providing intermediate or transient stor-
10 age of such data, such service provider shall be re-
11 quired to notify of such a breach of security only the
12 person who initiated such connection, transmission,
13 routing, or storage if such person can be reasonably
14 identified. Upon receiving such notification from a
15 service provider, such person shall take the action
16 required under subsection (a).

17 (3) COORDINATION OF NOTIFICATION WITH
18 CREDIT REPORTING AGENCIES.—If a person is re-
19 quired to provide notification to more than 5,000 in-
20 dividuals under subsection (a)(3)(B), the person
21 shall also notify the major credit reporting agencies
22 that compile and maintain files on consumers on a
23 nationwide basis of the timing and distribution of
24 the notices. Such notice shall be given to the credit
25 reporting agencies without unreasonable delay and,

1 if it will not delay notice to the affected individuals,
2 prior to the distribution of notices to the affected in-
3 dividuals.

4 (c) DELAY OF NOTIFICATION AUTHORIZED FOR LAW
5 ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—

6 (1) LAW ENFORCEMENT.—If a Federal, State,
7 or local law enforcement agency determines that the
8 notification required under subsection (a)(3)(B)
9 would impede a civil or criminal investigation, such
10 notification shall be delayed upon the request of the
11 law enforcement agency for 30 days or such lesser
12 period of time which the law enforcement agency de-
13 termines is reasonably necessary. The law enforce-
14 ment agency shall follow up such a request in writ-
15 ing. A law enforcement agency may, by a subsequent
16 written request, revoke such delay or extend the pe-
17 riod of time set forth in the original request made
18 under this paragraph if further delay is necessary.

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

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

8 (d) METHOD AND CONTENT OF NOTIFICATION.—

9 (1) DIRECT NOTIFICATION.—

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

18 (i) Written notification.

19 (ii) Notification by email or other
20 electronic means, if—

21 (I) the person's primary method
22 of communication with the individual
23 is by email or such other electronic
24 means; or

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

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

13 (i) a description of the personal infor-
14 mation that was acquired or accessed by
15 an unauthorized person;

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

22 (iii) notice that the individual is enti-
23 tled to receive, at no cost to such indi-
24 vidual, consumer credit reports on a quar-
25 terly basis for a period of 2 years, or credit

1 monitoring or other service that enables
2 consumers to detect the misuse of their
3 personal information for a period of 2
4 years, and instructions to the individual on
5 requesting such reports or service from the
6 person, except when the only information
7 which has been the subject of the security
8 breach is the individual's first name or ini-
9 tial and last name, or address, or phone
10 number, in combination with a credit or
11 debit card number, and any required secu-
12 rity code;

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-
25 tion in lieu of the direct notification required by

1 paragraph (1) if the person owns or possesses
2 data in electronic form containing personal in-
3 formation of fewer than 1,000 individuals and
4 such direct notification is not feasible due to—

5 (i) excessive cost to the person re-
6 quired to provide such notification relative
7 to the resources of such person, as deter-
8 mined in accordance with the regulations
9 issued by the Commission under paragraph
10 (3)(A); or

11 (ii) lack of sufficient contact informa-
12 tion for the individual required to be noti-
13 fied.

14 (B) FORM OF SUBSTITUTE NOTIFICA-
15 TION.—Such substitute notification shall in-
16 clude—

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

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

24 (iii) notification in print and to broad-
25 cast media, including major media in met-

1 ropolitan and rural areas where the indi-
2 viduals whose personal information was ac-
3 quired reside.

4 (C) CONTENT OF SUBSTITUTE NOTICE.—
5 Each form of substitute notice under this para-
6 graph shall include—

7 (i) notice that individuals whose per-
8 sonal information is included in the breach
9 of security are entitled to receive, at no
10 cost to the individuals, consumer credit re-
11 ports on a quarterly basis for a period of
12 2 years, or credit monitoring or other serv-
13 ice that enables consumers to detect the
14 misuse of their personal information for a
15 period of 2 years, and instructions on re-
16 questing such reports or service from the
17 person, except when the only information
18 which has been the subject of the security
19 breach is the individual's first name or ini-
20 tial and last name, or address, or phone
21 number, in combination with a credit or
22 debit card number, and any required secu-
23 rity code; and

24 (ii) a telephone number by which an
25 individual can, at no cost to such indi-

1 vidual, learn whether that individual's per-
2 sonal information is included in the breach
3 of security.

4 (3) REGULATIONS AND GUIDANCE.—

5 (A) REGULATIONS.—Not later than 1 year
6 after the date of enactment of this Act, the
7 Commission shall, by regulation under section
8 553 of title 5, United States Code, establish cri-
9 teria for determining circumstances under
10 which substitute notification may be provided
11 under paragraph (2), including criteria for de-
12 termining if notification under paragraph (1) is
13 not feasible due to excessive costs to the person
14 required to provide such notification relative to
15 the resources of such person. Such regulations
16 may also identify other circumstances where
17 substitute notification would be appropriate for
18 any person, including circumstances under
19 which the cost of providing notification exceeds
20 the benefits to consumers.

21 (B) GUIDANCE.—In addition, the Commis-
22 sion shall provide and publish general guidance
23 with respect to compliance with this subsection.
24 Such guidance shall include—

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

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

9 (e) OTHER OBLIGATIONS FOLLOWING BREACH.—

10 (1) IN GENERAL.—A person required to provide
11 notification under subsection (a) shall, upon request
12 of an individual whose personal information was in-
13 cluded in the breach of security, provide or arrange
14 for the provision of, to each such individual and at
15 no cost to such individual—

16 (A) consumer credit reports from at least
17 one of the major credit reporting agencies be-
18 ginning not later than 60 days following the in-
19 dividual's request and continuing on a quarterly
20 basis for a period of 2 years thereafter; or

21 (B) a credit monitoring or other service
22 that enables consumers to detect the misuse of
23 their personal information, beginning not later
24 than 60 days following the individual's request
25 and continuing for a period of 2 years.

1 (2) LIMITATION.—This subsection shall not
2 apply if the only personal information which has
3 been the subject of the security breach is the individ-
4 ual’s first name or initial and last name, or address,
5 or phone number, in combination with a credit or
6 debit card number, and any required security code.

7 (3) RULEMAKING.—As part of the Commis-
8 sion’s rulemaking described in subsection (d)(3), the
9 Commission shall determine the circumstances under
10 which a person required to provide notification
11 under subsection (a)(1) shall provide or arrange for
12 the provision of free consumer credit reports or cred-
13 it monitoring or other service to affected individuals.

14 (f) EXEMPTION BASED ON ASSESSMENT OF RISK
15 AND PRESUMPTION.—

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

21 (2) PRESUMPTION.—

22 (A) IN GENERAL.—If the data in electronic
23 form containing personal information is ren-
24 dered unusable, unreadable, or indecipherable
25 through encryption or other security technology

1 or methodology (if the method of encryption or
2 such other technology or methodology is gen-
3 erally accepted by experts in the information se-
4 curity field), there shall be a presumption that
5 no reasonable risk of identity theft, fraud, or
6 other unlawful conduct exists following a breach
7 of security of such data. Any such presumption
8 may be rebutted by facts demonstrating that
9 the encryption or other security technologies or
10 methodologies in a specific case have been or
11 are reasonably likely to be compromised.

12 (B) METHODOLOGIES OR TECH-
13 NOLOGIES.—Not later than 1 year after the
14 date of the enactment of this Act and bian-
15 nually thereafter, the Commission shall issue
16 rules (pursuant to section 553 of title 5, United
17 States Code) or guidance to identify security
18 methodologies or technologies which render data
19 in electronic form unusable, unreadable, or in-
20 decipherable, that shall, if applied to such data,
21 establish a presumption that no reasonable risk
22 of identity theft, fraud, or other unlawful con-
23 duct exists following a breach of security of
24 such data. Any such presumption may be rebut-
25 ted by facts demonstrating that any such meth-

1 odology or technology in a specific case has
2 been or is reasonably likely to be compromised.
3 In issuing such rules or guidance, the Commis-
4 sion shall consult with relevant industries, con-
5 sumer organizations, and data security and
6 identity theft prevention experts and established
7 standards setting bodies.

8 (3) FTC GUIDANCE.—Not later than 1 year
9 after the date of the enactment of this Act the Com-
10 mission shall issue guidance regarding the applica-
11 tion of the exemption in paragraph (1).

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

20 (h) FTC STUDY ON NOTIFICATION IN LANGUAGES
21 IN ADDITION TO ENGLISH.—Not later than 1 year after
22 the date of enactment of this Act, the Commission shall
23 conduct a study on the practicality and cost effectiveness
24 of requiring the notification required by subsection (d)(1)

1 to be provided in a language in addition to English to indi-
2 viduals known to speak only such other language.

3 (i) GENERAL RULEMAKING AUTHORITY.—The Com-
4 mission may promulgate regulations necessary under sec-
5 tion 553 of title 5, United States Code, to effectively en-
6 force the requirements of this section.

7 (j) TREATMENT OF PERSONS GOVERNED BY OTHER
8 LAW.—A person who is in compliance with any other Fed-
9 eral law that requires such person to provide notification
10 to individuals following a breach of security, and that,
11 taken as a whole, provides protections substantially similar
12 to, or greater than, those required under this section, as
13 the Commission shall determine by rule (under section
14 553 of title 5, United States Code), shall be deemed to
15 be in compliance with this section.

16 **SEC. 4. APPLICATION AND ENFORCEMENT.**

17 (a) GENERAL APPLICATION.—The requirements of
18 sections 2 and 3 apply to any information broker or other
19 person engaged in interstate commerce that owns or pos-
20 ses data containing personal information related to that
21 commercial activity, or contracts to have any third party
22 entity maintain such data for such person, including—

23 (1) those persons, partnerships, or corporations
24 over which the Commission has authority pursuant

1 to section 5(a)(2) of the Federal Trade Commission
2 Act; and

3 (2) notwithstanding section 4 and section
4 5(a)(2) of that Act (15 U.S.C. 44 and 45(a)(2)),
5 any non-profit organization, including any organiza-
6 tion described in section 501(c) of the Internal Rev-
7 enue Code of 1986 that is exempt from taxation
8 under section 501(a) of such Code.

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

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

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

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

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

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

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

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

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

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

1 (2) CIVIL PENALTIES.—

2 (A) CALCULATION.—

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

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

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

13 (i) \$5,000,000 for each violation of
14 section 2; and

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

18 (3) INTERVENTION BY THE FTC.—

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

1 instituting such action. The Commission shall
2 have the right—

3 (i) to intervene in the action;

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

6 (iii) to file petitions for appeal.

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

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

22 (A) conduct investigations;

23 (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 **SEC. 5. DEFINITIONS.**

5 In this Act the following definitions apply:

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

10 (2) COMMISSION.—The term “Commission”
11 means the Federal Trade Commission.

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

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

1 and safeguards of such keys to protect the integrity
2 of the encryption.

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

8 (6) INFORMATION BROKER.—The term “infor-
9 mation broker”—

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

21 (B) does not include a commercial entity to
22 the extent that such entity processes informa-
23 tion collected by or on behalf of and received
24 from or on behalf of a nonaffiliated third party
25 concerning individuals who are current or

1 former customers or employees of such third
2 party to enable such third party directly or
3 through parties acting on its behalf to: (1) pro-
4 vide benefits for its employees; or (2) directly
5 transact business with its customers.

6 (7) PERSONAL INFORMATION.—

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

12 (i) Social Security number.

13 (ii) Driver’s license number, passport
14 number, military identification number, or
15 other similar number issued on a govern-
16 ment document used to verify identity.

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

22 [(B) PUBLIC RECORD INFORMATION.—

23 Such term does not include public record infor-
24 mation.]

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

6 (i) for the purpose of section 2 to the
7 extent that such modification is necessary
8 to accomplish the purposes of such section
9 as a result of changes in technology or
10 practices and will not unreasonably impede
11 Internet or other technological innovation
12 or otherwise adversely affect interstate
13 commerce; or

14 (ii) for the purpose of section 3, if the
15 Commission determines that access to or
16 acquisition of the additional data elements
17 in the event of a breach of security would
18 create an unreasonable risk of identity
19 theft, fraud, or other unlawful activity and
20 that such modification will not unreason-
21 ably impede Internet or other technological
22 innovation or otherwise adversely affect
23 interstate commerce.

24 (8) PUBLIC RECORD INFORMATION.—The term
25 “public record information” means information

1 about an individual is lawfully made available to the
2 general public from Federal, State, or local govern-
3 ment records

4 (9) SERVICE PROVIDER.—The term “service
5 provider” means a person that provides electronic
6 data transmission, routing, intermediate and tran-
7 sient storage, or connections to its system or net-
8 work, where the person providing such services does
9 not select or modify the content of the electronic
10 data, is not the sender or the intended recipient of
11 the data, and such person transmits, routes, stores,
12 or provides connections for personal information in
13 a manner such that personal information is undif-
14 ferentiated from other types of data that such per-
15 son transmits, routes, or stores, or for which such
16 person provides such connections. Any such person
17 shall be treated as a service provider under this Act
18 only to the extent that it is engaged in the provision
19 of such transmission, routing, intermediate and
20 transient storage or connections.

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

22 (a) PREEMPTION OF STATE INFORMATION SECURITY
23 LAWS.—This Act supersedes any provision of a statute,
24 regulation, or rule of a State or political subdivision of

1 a State, with respect to those entities covered by the regu-
2 lations issued pursuant to this Act, that expressly—

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

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

10 (b) ADDITIONAL PREEMPTION.—

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

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

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

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

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

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

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

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