

112TH CONGRESS
1ST SESSION

H. R. 1841

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

IN THE HOUSE OF REPRESENTATIVES

MAY 11, 2011

Mr. STEARNS (for himself and Mr. MATHESON) introduced the following bill; which was referred to the Committee on Energy and Commerce

A BILL

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

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

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Data Accountability
5 and Trust Act (DATA) of 2011”.

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 each person
5 engaged in interstate commerce that owns or pos-
6 sesses data in electronic form containing personal in-
7 formation, or contracts to have any third party enti-
8 ty maintain such data for such person, to establish
9 and implement policies and procedures regarding in-
10 formation security practices for the treatment and
11 protection of personal information taking into con-
12 sideration—

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

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

19 (C) the cost of implementing such safe-
20 guards.

21 (2) REQUIREMENTS.—Such regulations shall
22 require the policies and procedures to include the
23 following:

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

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

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

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

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

1 information permanently unreadable or
2 undecipherable.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

24 (I) correct any inaccuracy; or

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

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

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

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

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

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

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

8 (C) TREATMENT OF ENTITIES GOVERNED
9 BY OTHER LAW.—The Commission may pro-
10 mulgate rules (under section 553 of title 5,
11 United States Code) to determine to be in com-
12 pliance with this paragraph any person who is
13 a consumer reporting agency, as defined in sec-
14 tion 603(f) of the Fair Credit Reporting Act
15 (15 U.S.C. 1681a(f)), with respect to those
16 products and services that are subject to and in
17 compliance with the requirements of that Act.

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

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

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

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

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

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

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

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

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

5 (2) notify the Commission.

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

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

18 (2) TELECOMMUNICATIONS CARRIERS, CABLE
19 OPERATORS, PROVIDERS OF INFORMATION SERVICE,
20 AND INTERACTIVE COMPUTER SERVICES.—If a tele-
21 communications carrier (as defined in section 3 of
22 the Communications Act of 1934 (47 U.S.C. 153)),
23 cable operator (as defined in section 602 of such Act
24 (47 U.S.C. 522)), provider of information service (as
25 defined in such section 3), or interactive computer

1 service (as defined in section 230(f)(2) of such Act
2 (47 U.S.C. 230(f)(2))) becomes aware of a breach of
3 security during the transmission of data in electronic
4 form containing personal information that is owned
5 or possessed by another person utilizing the means
6 of transmission of such telecommunications carrier,
7 cable operator, provider of information service, or
8 interactive computer service, such telecommuni-
9 cations carrier, cable operator, provider of informa-
10 tion service, or interactive computer service shall be
11 required only to notify the person who initiated such
12 transmission of such a breach of security if such
13 person can be reasonably identified. Upon receiving
14 such notification from a telecommunications carrier,
15 cable operator, provider of information service, or
16 interactive computer service, such person shall pro-
17 vide the notification required under subsection (a).
18 Notwithstanding section 5(a)(2) of the Federal
19 Trade Commission Act (15 U.S.C. 45(a)(2)), the
20 Commission shall have the authority to enforce this
21 paragraph with respect to a telecommunications car-
22 rier.

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

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

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

14 (d) METHOD AND CONTENT OF NOTIFICATION.—

15 (1) DIRECT NOTIFICATION.—

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

24 (i) Written notification.

25 (ii) Email notification, if—

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

4 (II) the individual has consented
5 to receive such notification and the
6 notification is provided in a manner
7 that is consistent with the provisions
8 permitting electronic transmission of
9 notices under section 101 of the Elec-
10 tronic Signatures in Global and Na-
11 tional Commerce Act (15 U.S.C.
12 7001).

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

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

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

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

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

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

14 (2) SUBSTITUTE NOTIFICATION.—

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

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

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

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

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

12 (B) FORM OF SUBSTITUTE NOTICE.—Such
13 substitute notification shall include—

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

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

21 (iii) notification in print and to broad-
22 cast media, including major media in met-
23 ropolitan and rural areas where the indi-
24 viduals whose personal information was ac-
25 quired reside.

1 (C) CONTENT OF SUBSTITUTE NOTICE.—

2 Each form of substitute notice under this para-
3 graph shall include—

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

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

16 (3) FEDERAL TRADE COMMISSION REGULA-
17 TIONS AND GUIDANCE.—

18 (A) REGULATIONS.—Not later than 1 year
19 after the date of enactment of this Act, the
20 Commission shall, by regulations under section
21 553 of title 5, United States Code, establish cri-
22 teria for determining the circumstances under
23 which substitute notification may be provided
24 under paragraph (2), including criteria for de-
25 termining if notification under paragraph (1) is

1 not feasible due to excessive cost to the person
2 required to provide such notification relative to
3 the resources of such person.

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

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

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

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

1 (f) EXEMPTION.—

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

7 (2) PRESUMPTIONS.—

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

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

1 theft, fraud, or other unlawful conduct exists
2 following a breach of security of such data. Any
3 such presumption may be rebutted by facts
4 demonstrating that any such methodology or
5 technology has been or is reasonably likely to be
6 compromised. In promulgating such a rule, the
7 Commission shall consult with relevant indus-
8 tries, consumer organizations, and data security
9 and identity theft prevention experts and estab-
10 lished standards setting bodies.

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

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

24 (h) FTC STUDY ON NOTIFICATION IN LANGUAGES
25 IN ADDITION TO ENGLISH.—Not later than 1 year after

1 the date of enactment of this Act, the Commission shall
2 conduct a study on the practicality and cost effectiveness
3 of requiring the notification required by subsection (d)(1)
4 to be provided in a language in addition to English to indi-
5 viduals known to speak only such other language.

6 **SEC. 4. ENFORCEMENT.**

7 (a) ENFORCEMENT BY THE FEDERAL TRADE COM-
8 MISSION.—

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

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

1 (3) RULES.—

2 (A) IN GENERAL.—The Commission shall
3 promulgate, under section 553 of title 5, United
4 States Code, such rules as may be necessary to
5 carry out the provisions of this Act.

6 (B) LIMITATION.—In promulgating rules
7 under this Act, the Commission shall not re-
8 quire the deployment or use of any specific
9 products or technologies, including any specific
10 computer software or hardware.

11 (b) ENFORCEMENT BY STATE ATTORNEYS GEN-
12 ERAL.—

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

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

1 (B) to compel compliance with such sec-
2 tion; or

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

5 (2) CIVIL PENALTIES.—

6 (A) CALCULATION.—

7 (i) TREATMENT OF VIOLATIONS OF
8 SECTION 2.—For purposes of paragraph
9 (1)(C) with regard to a violation of section
10 2, the amount determined under this para-
11 graph is the amount calculated by multi-
12 plying the number of violations of such
13 section by an amount not greater than
14 \$11,000. Each day that a person is not in
15 compliance with the requirements of such
16 section shall be treated as a separate viola-
17 tion. The maximum civil penalty calculated
18 under this clause shall not exceed
19 \$5,000,000.

20 (ii) TREATMENT OF VIOLATIONS OF
21 SECTION 3.—For purposes of paragraph
22 (1)(C) with regard to a violation of section
23 3, the amount determined under this para-
24 graph is the amount calculated by multi-
25 plying the number of violations of such

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

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

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 (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 at-
3 torney 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 subpart A of part 1 of title 16, Code of Federal
22 Regulations), policy statements, or guidance regarding
23 this Act.

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

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

4 (b) SUNSET.—This Act shall cease to be in effect on
5 September 30, 2016.

6 **SEC. 8. AUTHORIZATION OF APPROPRIATIONS.**

7 There is authorized to be appropriated to the Com-
8 mission \$1,000,000 for each of fiscal years 2012 through
9 2016 to carry out this Act.

○