

111TH CONGRESS
1ST SESSION

H. R. 2221

AN ACT

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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Data Accountability
3 and Trust Act”.

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

5 (a) GENERAL SECURITY POLICIES AND PROCE-
6 DURES.—

7 (1) REGULATIONS.—Not later than 1 year after
8 the date of enactment of this Act, the Commission
9 shall promulgate regulations under section 553 of
10 title 5, United States Code, to require each person
11 engaged in interstate commerce that owns or pos-
12 sesses data containing personal information, or con-
13 tracts to have any third party entity maintain such
14 data for such person, to establish and implement
15 policies and procedures regarding information secu-
16 rity practices for the treatment and protection of
17 personal information taking into consideration—

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

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

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

1 (2) REQUIREMENTS.—Such regulations shall
2 require the policies and procedures to include the
3 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 re-
9 sponsibility for the management of information
10 security.

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

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 undecipherable.

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) TREATMENT OF ENTITIES GOVERNED BY
9 OTHER LAW.—Any person who is in compliance with
10 any other Federal law that requires such person to
11 maintain standards and safeguards for information
12 security and protection of personal information that,
13 taken as a whole and as the Commission shall deter-
14 mine in the rulemaking required under paragraph
15 (1), provide protections substantially similar to, or
16 greater than, those required under this subsection,
17 shall be deemed to be in compliance with this sub-
18 section.

19 (b) SPECIAL REQUIREMENTS FOR INFORMATION
20 BROKERS.—

21 (1) SUBMISSION OF POLICIES TO THE FTC.—
22 The regulations promulgated under subsection (a)
23 shall require each information broker to submit its
24 security policies to the Commission in conjunction

1 with a notification of a breach of security under sec-
2 tion 3 or upon request of the Commission.

3 (2) POST-BREACH AUDIT.—For any information
4 broker required to provide notification under section
5 3, the Commission may conduct audits of the infor-
6 mation security practices of such information broker,
7 or require the information broker to conduct inde-
8 pendent audits of such practices (by an independent
9 auditor who has not audited such information bro-
10 ker’s security practices during the preceding 5
11 years).

12 (3) ACCURACY OF AND INDIVIDUAL ACCESS TO
13 PERSONAL INFORMATION.—

14 (A) ACCURACY.—

15 (i) IN GENERAL.—Each information
16 broker shall establish reasonable proce-
17 dures to assure the maximum possible ac-
18 curacy of the personal information it col-
19 lects, assembles, or maintains, and any
20 other information it collects, assembles, or
21 maintains that specifically identifies an in-
22 dividual, other than information which
23 merely identifies an individual’s name or
24 address.

1 (ii) LIMITED EXCEPTION FOR FRAUD
2 DATABASES.—The requirement in clause
3 (i) shall not prevent the collection or main-
4 tenance of information that may be inac-
5 curate with respect to a particular indi-
6 vidual when that information is being col-
7 lected or maintained solely—

8 (I) for the purpose of indicating
9 whether there may be a discrepancy
10 or irregularity in the personal infor-
11 mation that is associated with an indi-
12 vidual; and

13 (II) to help identify, or authen-
14 ticate the identity of, an individual, or
15 to protect against or investigate fraud
16 or other unlawful conduct.

17 (B) CONSUMER ACCESS TO INFORMA-
18 TION.—

19 (i) ACCESS.—Each information broker
20 shall—

21 (I) provide to each individual
22 whose personal information it main-
23 tains, at the individual's request at
24 least 1 time per year and at no cost
25 to the individual, and after verifying

1 the identity of such individual, a
2 means for the individual to review any
3 personal information regarding such
4 individual maintained by the informa-
5 tion broker and any other information
6 maintained by the information broker
7 that specifically identifies such indi-
8 vidual, other than information which
9 merely identifies an individual's name
10 or address; and

11 (II) place a conspicuous notice on
12 its Internet website (if the informa-
13 tion broker maintains such a website)
14 instructing individuals how to request
15 access to the information required to
16 be provided under subclause (I), and,
17 as applicable, how to express a pref-
18 erence with respect to the use of per-
19 sonal information for marketing pur-
20 poses under clause (iii).

21 (ii) DISPUTED INFORMATION.—When-
22 ever an individual whose information the
23 information broker maintains makes a
24 written request disputing the accuracy of
25 any such information, the information

1 broker, after verifying the identity of the
2 individual making such request and unless
3 there are reasonable grounds to believe
4 such request is frivolous or irrelevant,
5 shall—

6 (I) correct any inaccuracy; or

7 (II)(aa) in the case of informa-
8 tion that is public record information,
9 inform the individual of the source of
10 the information, and, if reasonably
11 available, where a request for correc-
12 tion may be directed and, if the indi-
13 vidual provides proof that the public
14 record has been corrected or that the
15 information broker was reporting the
16 information incorrectly, correct the in-
17 accuracy in the information broker's
18 records; or

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

1 cedures outlined in subparagraph (A)
2 if such information can be independ-
3 ently verified.

4 (iii) ALTERNATIVE PROCEDURE FOR
5 CERTAIN MARKETING INFORMATION.—In
6 accordance with regulations issued under
7 clause (v), an information broker that
8 maintains any information described in
9 clause (i) which is used, shared, or sold by
10 such information broker for marketing
11 purposes, may, in lieu of complying with
12 the access and dispute requirements set
13 forth in clauses (i) and (ii), provide each
14 individual whose information it maintains
15 with a reasonable means of expressing a
16 preference not to have his or her informa-
17 tion used for such purposes. If the indi-
18 vidual expresses such a preference, the in-
19 formation broker may not use, share, or
20 sell the individual’s information for mar-
21 keting purposes.

22 (iv) LIMITATIONS.—An information
23 broker may limit the access to information
24 required under subparagraph (B)(i)(I) and
25 is not required to provide notice to individ-

1 uals as required under subparagraph
2 (B)(i)(II) in the following circumstances:

3 (I) If access of the individual to
4 the information is limited by law or
5 legally recognized privilege.

6 (II) If the information is used for
7 a legitimate governmental or fraud
8 prevention purpose that would be
9 compromised by such access.

10 (III) If the information consists
11 of a published media record, unless
12 that record has been included in a re-
13 port about an individual shared with a
14 third party.

15 (v) RULEMAKING.—Not later than 1
16 year after the date of the enactment of this
17 Act, the Commission shall promulgate reg-
18 ulations under section 553 of title 5,
19 United States Code, to carry out this para-
20 graph and to facilitate the purposes of this
21 Act. In addition, the Commission shall
22 issue regulations, as necessary, under sec-
23 tion 553 of title 5, United States Code, on
24 the scope of the application of the limita-
25 tions in clause (iv), including any addi-

1 tional circumstances in which an informa-
2 tion broker may limit access to information
3 under such clause that the Commission de-
4 termines to be appropriate.

5 (C) FCRA REGULATED PERSONS.—Any
6 information broker who is engaged in activities
7 subject to the Fair Credit Reporting Act and
8 who is in compliance with sections 609, 610,
9 and 611 of such Act with respect to information
10 subject to such Act, shall be deemed to be in
11 compliance with this paragraph with respect to
12 such information.

13 (4) REQUIREMENT OF AUDIT LOG OF ACCESSED
14 AND TRANSMITTED INFORMATION.—Not later than
15 1 year after the date of the enactment of this Act,
16 the Commission shall promulgate regulations under
17 section 553 of title 5, United States Code, to require
18 information brokers to establish measures which fa-
19 cilitate the auditing or retracing of any internal or
20 external access to, or transmissions of, any data con-
21 taining personal information collected, assembled, or
22 maintained by such information broker.

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

1 (A) PROHIBITION ON OBTAINING PER-
2 SONAL INFORMATION BY FALSE PRETENSES.—

3 It shall be unlawful for an information broker
4 to obtain or attempt to obtain, or cause to be
5 disclosed or attempt to cause to be disclosed to
6 any person, personal information or any other
7 information relating to any person by—

8 (i) making a false, fictitious, or fraud-
9 ulent statement or representation to any
10 person; or

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

18 (B) PROHIBITION ON SOLICITATION TO
19 OBTAIN PERSONAL INFORMATION UNDER FALSE

20 PRETENSES.—It shall be unlawful for an infor-
21 mation broker to request a person to obtain
22 personal information or any other information
23 relating to any other person, if the information
24 broker knew or should have known that the per-
25 son to whom such a request is made will obtain

1 or attempt to obtain such information in the
2 manner described in subparagraph (A).

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

8 **SEC. 3. NOTIFICATION OF INFORMATION SECURITY**
9 **BREACH.**

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

15 (1) notify each individual who is a citizen or
16 resident of the United States whose personal infor-
17 mation was acquired or accessed as a result of such
18 a breach of security; and

19 (2) notify the Commission.

20 (b) **SPECIAL NOTIFICATION REQUIREMENTS.**—

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

1 data, such third party entity shall be required to no-
2 tify such person of the breach of security. Upon re-
3 ceiving such notification from such third party, such
4 person shall provide the notification required under
5 subsection (a).

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

20 (3) COORDINATION OF NOTIFICATION WITH
21 CREDIT REPORTING AGENCIES.—If a person is re-
22 quired to provide notification to more than 5,000 in-
23 dividuals under subsection (a)(1), the person shall
24 also notify the major credit reporting agencies that
25 compile and maintain files on consumers on a na-

1 tionwide basis, of the timing and distribution of the
2 notices. Such notice shall be given to the credit re-
3 porting agencies without unreasonable delay and, if
4 it will not delay notice to the affected individuals,
5 prior to the distribution of notices to the affected in-
6 dividuals.

7 (c) TIMELINESS OF NOTIFICATION.—

8 (1) IN GENERAL.—Unless subject to a delay au-
9 thorized under paragraph (2), a notification required
10 under subsection (a) shall be made not later than 60
11 days following the discovery of a breach of security,
12 unless the person providing notice can show that
13 providing notice within such a time frame is not fea-
14 sible due to extraordinary circumstances necessary
15 to prevent further breach or unauthorized disclo-
16 sures, and reasonably restore the integrity of the
17 data system, in which case such notification shall be
18 made as promptly as possible.

19 (2) DELAY OF NOTIFICATION AUTHORIZED FOR
20 LAW ENFORCEMENT OR NATIONAL SECURITY PUR-
21 POSES.—

22 (A) LAW ENFORCEMENT.—If a Federal,
23 State, or local law enforcement agency deter-
24 mines that the notification required under this
25 section would impede a civil or criminal inves-

1 tigation, such notification shall be delayed upon
2 the written request of the law enforcement
3 agency for 30 days or such lesser period of time
4 which the law enforcement agency determines is
5 reasonably necessary and requests in writing. A
6 law enforcement agency may, by a subsequent
7 written request, revoke such delay or extend the
8 period of time set forth in the original request
9 made under this paragraph if further delay is
10 necessary.

11 (B) NATIONAL SECURITY.—If a Federal
12 national security agency or homeland security
13 agency determines that the notification required
14 under this section would threaten national or
15 homeland security, such notification may be de-
16 layed for a period of time which the national se-
17 curity agency or homeland security agency de-
18 termines is reasonably necessary and requests
19 in writing. A Federal national security agency
20 or homeland security agency may revoke such
21 delay or extend the period of time set forth in
22 the original request made under this paragraph
23 by a subsequent written request if further delay
24 is necessary.

25 (d) METHOD AND CONTENT OF NOTIFICATION.—

1 (1) DIRECT NOTIFICATION.—

2 (A) METHOD OF NOTIFICATION.—A person
3 required to provide notification to individuals
4 under subsection (a)(1) shall be in compliance
5 with such requirement if the person provides
6 conspicuous and clearly identified notification
7 by one of the following methods (provided the
8 selected method can reasonably be expected to
9 reach the intended individual):

10 (i) Written notification.

11 (ii) Notification by email or other
12 electronic means, if—

13 (I) the person’s primary method
14 of communication with the individual
15 is by email or such other electronic
16 means; or

17 (II) the individual has consented
18 to receive such notification and the
19 notification is provided in a manner
20 that is consistent with the provisions
21 permitting electronic transmission of
22 notices under section 101 of the Elec-
23 tronic Signatures in Global Commerce
24 Act (15 U.S.C. 7001).

1 (B) CONTENT OF NOTIFICATION.—Regard-
2 less of the method by which notification is pro-
3 vided to an individual under subparagraph (A),
4 such notification shall include—

5 (i) a description of the personal infor-
6 mation that was acquired or accessed by
7 an unauthorized person;

8 (ii) a telephone number that the indi-
9 vidual may use, at no cost to such indi-
10 vidual, to contact the person to inquire
11 about the breach of security or the infor-
12 mation the person maintained about that
13 individual;

14 (iii) notice that the individual is enti-
15 tled to receive, at no cost to such indi-
16 vidual, consumer credit reports on a quar-
17 terly basis for a period of 2 years, or credit
18 monitoring or other service that enables
19 consumers to detect the misuse of their
20 personal information for a period of 2
21 years, and instructions to the individual on
22 requesting such reports or service from the
23 person, except when the only information
24 which has been the subject of the security
25 breach is the individual's first name or ini-

1 tial and last name, or address, or phone
2 number, in combination with a credit or
3 debit card number, and any required secu-
4 rity code;

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

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

12 (2) SUBSTITUTE NOTIFICATION.—

13 (A) CIRCUMSTANCES GIVING RISE TO SUB-
14 STITUTE NOTIFICATION.—A person required to
15 provide notification to individuals under sub-
16 section (a)(1) may provide substitute notifica-
17 tion in lieu of the direct notification required by
18 paragraph (1) if the person owns or possesses
19 data in electronic form containing personal in-
20 formation of fewer than 1,000 individuals and
21 such direct notification is not feasible due to—

22 (i) excessive cost to the person re-
23 quired to provide such notification relative
24 to the resources of such person, as deter-
25 mined in accordance with the regulations

1 issued by the Commission under paragraph
2 (3)(A); or

3 (ii) lack of sufficient contact informa-
4 tion for the individual required to be noti-
5 fied.

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

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

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

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

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

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

1 of security are entitled to receive, at no
2 cost to the individuals, consumer credit re-
3 ports on a quarterly basis for a period of
4 2 years, or credit monitoring or other serv-
5 ice that enables consumers to detect the
6 misuse of their personal information for a
7 period of 2 years, and instructions on re-
8 questing such reports or service from the
9 person, except when the only information
10 which has been the subject of the security
11 breach is the individual's first name or ini-
12 tial and last name, or address, or phone
13 number, in combination with a credit or
14 debit card number, and any required secu-
15 rity code; and

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

21 (3) REGULATIONS AND GUIDANCE.—

22 (A) REGULATIONS.—Not later than 1 year
23 after the date of enactment of this Act, the
24 Commission shall, by regulation under section
25 553 of title 5, United States Code, establish cri-

1 teria for determining circumstances under
2 which substitute notification may be provided
3 under paragraph (2), including criteria for de-
4 termining if notification under paragraph (1) is
5 not feasible due to excessive costs to the person
6 required to provided such notification relative to
7 the resources of such person. Such regulations
8 may also identify other circumstances where
9 substitute notification would be appropriate for
10 any person, including circumstances under
11 which the cost of providing notification exceeds
12 the benefits to consumers.

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

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

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

25 (e) OTHER OBLIGATIONS FOLLOWING BREACH.—

1 (1) IN GENERAL.—A person required to provide
2 notification under subsection (a) shall, upon request
3 of an individual whose personal information was in-
4 cluded in the breach of security, provide or arrange
5 for the provision of, to each such individual and at
6 no cost to such individual—

7 (A) consumer credit reports from at least
8 one of the major credit reporting agencies be-
9 ginning not later than 60 days following the in-
10 dividual’s request and continuing on a quarterly
11 basis for a period of 2 years thereafter; or

12 (B) a credit monitoring or other service
13 that enables consumers to detect the misuse of
14 their personal information, beginning not later
15 than 60 days following the individual’s request
16 and continuing for a period of 2 years.

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

23 (3) RULEMAKING.—As part of the Commis-
24 sion’s rulemaking described in subsection (d)(3), the
25 Commission shall determine the circumstances under

1 which a person required to provide notification
2 under subsection (a)(1) shall provide or arrange for
3 the provision of free consumer credit reports or cred-
4 it monitoring or other service to affected individuals.

5 (f) EXEMPTION.—

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

11 (2) PRESUMPTION.—

12 (A) IN GENERAL.—If the data in electronic
13 form containing personal information is ren-
14 dered unusable, unreadable, or indecipherable
15 through encryption or other security technology
16 or methodology (if the method of encryption or
17 such other technology or methodology is gen-
18 erally accepted by experts in the information se-
19 curity field), there shall be a presumption that
20 no reasonable risk of identity theft, fraud, or
21 other unlawful conduct exists following a breach
22 of security of such data. Any such presumption
23 may be rebutted by facts demonstrating that
24 the encryption or other security technologies or

1 methodologies in a specific case, have been or
2 are reasonably likely to be compromised.

3 (B) METHODOLOGIES OR TECH-
4 NOLOGIES.—Not later than 1 year after the
5 date of the enactment of this Act and bian-
6 nually thereafter, the Commission shall issue
7 rules (pursuant to section 553 of title 5, United
8 States Code) or guidance to identify security
9 methodologies or technologies which render data
10 in electronic form unusable, unreadable, or in-
11 decipherable, that shall, if applied to such data,
12 establish a presumption that no reasonable risk
13 of identity theft, fraud, or other unlawful con-
14 duct exists following a breach of security of
15 such data. Any such presumption may be rebut-
16 ted by facts demonstrating that any such meth-
17 odology or technology in a specific case has
18 been or is reasonably likely to be compromised.
19 In issuing such rules or guidance, the Commis-
20 sion shall consult with relevant industries, con-
21 sumer organizations, and data security and
22 identity theft prevention experts and established
23 standards setting bodies.

24 (3) FTC GUIDANCE.—Not later than 1 year
25 after the date of the enactment of this Act the Com-

1 mission shall issue guidance regarding the applica-
2 tion of the exemption in paragraph (1).

3 (g) WEBSITE NOTICE OF FEDERAL TRADE COMMIS-
4 SION.—If the Commission, upon receiving notification of
5 any breach of security that is reported to the Commission
6 under subsection (a)(2), finds that notification of such a
7 breach of security via the Commission’s Internet website
8 would be in the public interest or for the protection of
9 consumers, the Commission shall place such a notice in
10 a clear and conspicuous location on its Internet website.

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

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

22 (j) TREATMENT OF PERSONS GOVERNED BY OTHER
23 LAW.—A person who is in compliance with any other Fed-
24 eral law that requires such person to provide notification
25 to individuals following a breach of security, and that,

1 taken as a whole, provides protections substantially similar
2 to, or greater than, those required under this section, as
3 the Commission shall determine by rule (under section
4 553 of title 5, United States Code), shall be deemed to
5 be in compliance with this section.

6 **SEC. 4. APPLICATION AND ENFORCEMENT.**

7 (a) GENERAL APPLICATION.—The requirements of
8 sections 2 and 3 shall only apply to those persons, partner-
9 ships, or corporations over which the Commission has au-
10 thority pursuant to section 5(a)(2) of the Federal Trade
11 Commission Act.

12 (b) ENFORCEMENT BY THE FEDERAL TRADE COM-
13 MISSION.—

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

21 (2) POWERS OF COMMISSION.—The Commis-
22 sion shall enforce this Act in the same manner, by
23 the same means, and with the same jurisdiction,
24 powers, and duties as though all applicable terms
25 and provisions of the Federal Trade Commission Act

1 (15 U.S.C. 41 et seq.) were incorporated into and
2 made a part of this Act. Any person who violates
3 such regulations shall be subject to the penalties and
4 entitled to the privileges and immunities provided in
5 that Act.

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

11 (c) 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 days that a person is
13 not in compliance with such section by an
14 amount not greater than \$11,000.

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

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

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

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

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

22 (3) INTERVENTION BY THE FTC.—

23 (A) NOTICE AND INTERVENTION.—The
24 State shall provide prior written notice of any
25 action under paragraph (1) to the Commission

1 and provide the Commission with a copy of its
2 complaint, except in any case in which such
3 prior notice is not feasible, in which case the
4 State shall serve such notice immediately upon
5 instituting such action. The Commission shall
6 have the right—

7 (i) to intervene in the action;

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

10 (iii) to file petitions for appeal.

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

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

- 1 (A) conduct investigations;
- 2 (B) administer oaths or affirmations; or
- 3 (C) compel the attendance of witnesses or
- 4 the production of documentary and other evi-
- 5 dence.

6 (d) AFFIRMATIVE DEFENSE FOR A VIOLATION OF

7 SECTION 3.—

8 (1) IN GENERAL.—It shall be an affirmative de-

9 fense to an enforcement action brought under sub-

10 section (b), or a civil action brought under sub-

11 section (c), based on a violation of section 3, that all

12 of the personal information contained in the data in

13 electronic form that was acquired or accessed as a

14 result of a breach of security of the defendant is

15 public record information that is lawfully made

16 available to the general public from Federal, State,

17 or local government records and was acquired by the

18 defendant from such records.

19 (2) NO EFFECT ON OTHER REQUIREMENTS.—

20 Nothing in this subsection shall be construed to ex-

21 empt any person from the requirement to notify the

22 Commission of a breach of security as required

23 under section 3(a).

24 **SEC. 5. DEFINITIONS.**

25 In this Act the following definitions apply:

1 (1) BREACH OF SECURITY.—The term “breach
2 of security” means unauthorized access to or acqui-
3 sition of data in electronic form containing personal
4 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: (1) pro-
24 vide benefits for its employees; or (2) directly
25 transact 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) MODIFIED DEFINITION BY RULE-
18 MAKING.—The Commission may, by rule pro-
19 mulgated under section 553 of title 5, United
20 States Code, modify the definition of “personal
21 information” under subparagraph (A)—

22 (i) for the purpose of section 2 to the
23 extent that such modification will not un-
24 reasonably impede interstate commerce,

1 and will accomplish the purposes of this
2 Act; or

3 (ii) for the purpose of section 3, to the
4 extent that such modification is necessary
5 to accommodate changes in technology or
6 practices, will not unreasonably impede
7 interstate commerce, and will accomplish
8 the purposes of this Act.

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

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

20 (10) SERVICE PROVIDER.—The term “service
21 provider” means a person that provides electronic
22 data transmission, routing, intermediate and tran-
23 sient storage, or connections to its system or net-
24 work, where the person providing such services does
25 not select or modify the content of the electronic

1 data, is not the sender or the intended recipient of
2 the data, and such person transmits, routes, stores,
3 or provides connections for personal information in
4 a manner that personal information is undifferen-
5 tiated from other types of data that such person
6 transmits, routes, stores, or provides connections.
7 Any such person shall be treated as a service pro-
8 vider under this Act only to the extent that it is en-
9 gaged in the provision of such transmission, routing,
10 intermediate and transient storage or connections.

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

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

17 (1) requires information security practices and
18 treatment of data containing personal information
19 similar to any of those required under section 2; and

20 (2) requires notification to individuals of a
21 breach of security resulting in unauthorized access
22 to or acquisition of data in electronic form con-
23 taining personal information.

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 **SEC. 7. EFFECTIVE DATE.**

21 This Act shall take effect 1 year after the date of
22 enactment of this Act.

1 **SEC. 8. AUTHORIZATION OF APPROPRIATIONS.**

2 There is authorized to be appropriated to the Com-
3 mission \$1,000,000 for each of fiscal years 2010 through
4 2015 to carry out this Act.

 Passed the House of Representatives December 8,
2009.

Attest:

Clerk.

111TH CONGRESS
1ST SESSION

H. R. 2221

AN ACT

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.