

112TH CONGRESS
1ST SESSION

S. 1207

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 SENATE OF THE UNITED STATES

JUNE 15, 2011

Mr. PRYOR (for himself and Mr. ROCKEFELLER) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

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 “Data Security and
5 Breach Notification Act 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 every covered
5 entity that owns or possesses data containing per-
6 sonal information, or contracts to have any third-
7 party entity maintain such data for such covered en-
8 tity, to establish and implement policies and proce-
9 dures regarding information security practices for
10 the treatment and protection of personal information
11 taking into consideration—

12 (A) the size of, and the nature, scope, and
13 complexity of the activities engaged in by, such
14 covered entity;

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

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

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

23 (A) A security policy with respect to the
24 collection, use, sale, other dissemination, and
25 maintenance of such personal information.

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

5 (C) A process for identifying and assessing
6 any reasonably foreseeable vulnerabilities in the
7 system or systems maintained by such covered
8 entity that contains such data, which shall in-
9 clude regular monitoring for a breach of secu-
10 rity of such system or systems.

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

18 (E) A process for disposing of data in elec-
19 tronic form containing personal information by
20 shredding, permanently erasing, or otherwise
21 modifying the personal information contained in
22 such data to make such personal information
23 permanently unreadable or indecipherable.

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

4 (3) TREATMENT OF ENTITIES GOVERNED BY
5 OTHER LAW.—Any covered entity that is in compli-
6 ance with any other Federal law that requires such
7 covered entity to maintain standards and safeguards
8 for information security and protection of personal
9 information that, taken as a whole and as the Com-
10 mission shall determine in the rulemaking required
11 under paragraph (1), provide protections substan-
12 tially similar to, or greater than, those required
13 under this subsection, shall be deemed to be in com-
14 pliance with this subsection.

15 (b) SPECIAL REQUIREMENTS FOR INFORMATION
16 BROKERS.—

17 (1) SUBMISSION OF POLICIES TO THE FTC.—
18 The regulations promulgated under subsection (a)
19 shall require each information broker to submit its
20 security policies to the Commission in conjunction
21 with a notification of a breach of security under sec-
22 tion 3 or upon request of the Commission.

23 (2) POST-BREACH AUDIT.—For any information
24 broker required to provide notification of a security
25 breach under section 3, the Commission may con-

1 duct audits of the information security practices of
2 such information broker, or require the information
3 broker to conduct independent audits of such prac-
4 tices (by an independent auditor who has not au-
5 dited such information broker's security practices
6 during the preceding 5 years).

7 (3) ACCURACY OF AND INDIVIDUAL ACCESS TO
8 PERSONAL INFORMATION.—

9 (A) ACCURACY.—

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

20 (ii) LIMITED EXCEPTION FOR FRAUD
21 DATABASES.—The requirement in clause
22 (i) shall not prevent the collection or main-
23 tenance of information that may be inac-
24 curate with respect to a particular indi-

1 vidual when that information is being col-
2 lected or maintained solely—

3 (I) for the purpose of indicating
4 whether there may be a discrepancy
5 or irregularity in the personal infor-
6 mation that is associated with an indi-
7 vidual; and

8 (II) to help identify, or authen-
9 ticate the identity of, an individual, or
10 to protect against or investigate fraud
11 or other unlawful conduct.

12 (B) CONSUMER ACCESS TO INFORMA-
13 TION.—

14 (i) ACCESS.—Each information broker
15 shall—

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

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

6 (II) place a conspicuous notice on
7 its Internet Web site (if the informa-
8 tion broker maintains such a Web
9 site) instructing individuals how to re-
10 quest access to the information re-
11 quired to be provided under subclause
12 (I), and, as applicable, how to express
13 a preference with respect to the use of
14 personal information for marketing
15 purposes under clause (iii).

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

1 (I) correct any inaccuracy; or

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

14 (bb) in the case of information
15 that is non-public information, note
16 the information that is disputed, in-
17 cluding the individual's statement dis-
18 puting such information, and take
19 reasonable steps to independently
20 verify such information under the pro-
21 cedures outlined in subparagraph (A)
22 if such information can be independ-
23 ently verified.

24 (iii) ALTERNATIVE PROCEDURE FOR
25 CERTAIN MARKETING INFORMATION.—In

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

17 (iv) LIMITATIONS.—An information
18 broker may limit the access to information
19 required under subparagraph (B)(i)(I) and
20 is not required to provide notice to individ-
21 uals as required under subparagraph
22 (B)(i)(II) in the following circumstances:

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

1 (II) If the information is used for
2 a legitimate governmental, child pro-
3 tection, or fraud prevention purpose
4 that would be compromised by such
5 access.

6 (III) If the information consists
7 of a published media record, unless
8 that record has been included in a re-
9 port about an individual shared with a
10 third party.

11 (v) RULEMAKING.—Not later than 1
12 year after the date of the enactment of this
13 Act, the Commission shall promulgate reg-
14 ulations under section 553 of title 5,
15 United States Code, to carry out this para-
16 graph and to facilitate the purposes of this
17 Act. In addition, the Commission shall
18 issue regulations, as necessary, under sec-
19 tion 553 of title 5, United States Code, on
20 the scope of the application of the limita-
21 tions in clause (iv), including any addi-
22 tional circumstances in which an informa-
23 tion broker may limit access to information
24 under such clause that the Commission de-
25 termines to be appropriate.

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

9 (4) REQUIREMENT OF AUDIT LOG OF ACCESSED
10 AND TRANSMITTED INFORMATION.—Not later than
11 1 year after the date of the enactment of this Act,
12 the Commission shall promulgate regulations under
13 section 553 of title 5, United States Code, to require
14 information brokers to establish measures which fa-
15 cilitate the auditing or retracing of any internal or
16 external access to, or transmission of, any data con-
17 taining personal information collected, assembled, or
18 maintained by such information broker. The Com-
19 mission may provide exceptions to such requirements
20 for the purposes of furthering or protecting law en-
21 forcement or national security activities.

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

24 (A) PROHIBITION ON OBTAINING PER-
25 SONAL INFORMATION BY FALSE PRETENSES.—

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

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

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

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

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 to the extent that the service provider is exclusively en-
5 gaged in the transmission, routing, or temporary, inter-
6 mediate, or transient storage of that communication.

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

9 (a) NATIONWIDE NOTIFICATION.—Any covered enti-
10 ty that owns or possesses data in electronic form con-
11 taining personal information shall, following the discovery
12 of a breach of security of the system maintained by such
13 covered entity that contains such data—

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

18 (2) notify the Commission.

19 (b) SPECIAL NOTIFICATION REQUIREMENTS.—

20 (1) THIRD-PARTY AGENTS.—In the event of a
21 breach of security of the system maintained by any
22 third-party entity that has been contracted to main-
23 tain or process data in electronic form containing
24 personal information on behalf of any other covered
25 entity who owns or possesses such data, such third-

1 party entity shall be required to notify such covered
2 entity of the breach of security. Upon receiving such
3 notification from such third party, such covered enti-
4 ty shall provide the notification required under sub-
5 section (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 covered entity that
10 connects to or uses a system or network provided by
11 the 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 covered entity who initiated such connection, trans-
16 mission, routing, or storage if such covered entity
17 can be reasonably identified. Upon receiving such
18 notification from a service provider, such covered en-
19 tity shall provide the notification required under
20 subsection (a).

21 (3) COORDINATION OF NOTIFICATION WITH
22 CREDIT REPORTING AGENCIES.—If a covered entity
23 is required to provide notification to more than
24 5,000 individuals under subsection (a)(1), the cov-
25 ered entity also shall notify the major credit report-

1 ing agencies that compile and maintain files on con-
2 sumers on a nationwide basis, of the timing and dis-
3 tribution of the notices. Such notice shall be given
4 to the credit reporting agencies without unreason-
5 able delay and, if it will not delay notice to the af-
6 fected individuals, prior to the distribution of notices
7 to the affected individuals.

8 (c) TIMELINESS OF NOTIFICATION.—

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

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

24 (A) LAW ENFORCEMENT.—If a Federal,
25 State, or local law enforcement agency deter-

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

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

1 by a subsequent written request if further delay
2 is necessary.

3 (d) METHOD AND CONTENT OF NOTIFICATION.—

4 (1) DIRECT NOTIFICATION.—

5 (A) METHOD OF NOTIFICATION.—A cov-
6 ered entity required to provide notification to
7 individuals under subsection (a)(1) shall be in
8 compliance with such requirement if the covered
9 entity provides conspicuous and clearly identi-
10 fied notification by one of the following methods
11 (provided the selected method can reasonably be
12 expected to reach the intended individual):

13 (i) Written notification.

14 (ii) Notification by e-mail or other
15 electronic means, if—

16 (I) the covered entity's primary
17 method of communication with the in-
18 dividual is by e-mail or such other
19 electronic means; or

20 (II) the individual has consented
21 to receive such notification and the
22 notification is provided in a manner
23 that is consistent with the provisions
24 permitting electronic transmission of
25 notices under section 101 of the Elec-

1 tronic Signatures in Global Commerce
2 Act (15 U.S.C. 7001).

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

7 (i) the date, estimated date, or esti-
8 mated date range of the breach of security;

9 (ii) a description of the personal infor-
10 mation that was acquired or accessed by
11 an unauthorized person;

12 (iii) a telephone number that the indi-
13 vidual may use, at no cost to such indi-
14 vidual, to contact the covered entity to in-
15 quire about the breach of security or the
16 information the covered entity maintained
17 about that individual;

18 (iv) notice that the individual is enti-
19 tled to receive, at no cost to such indi-
20 vidual, consumer credit reports on a quar-
21 terly basis for a period of 2 years, or credit
22 monitoring or other service that enables
23 consumers to detect the misuse of their
24 personal information for a period of 2
25 years, and instructions to the individual on

1 requesting such reports or service from the
2 covered entity, except when the only infor-
3 mation which has been the subject of the
4 security breach is the individual's first
5 name or initial and last name, or address,
6 or phone number, in combination with a
7 credit or debit card number, and any re-
8 quired security code;

9 (v) the toll-free contact telephone
10 numbers and addresses for the major cred-
11 it reporting agencies; and

12 (vi) a toll-free telephone number and
13 Internet Web site address for the Commis-
14 sion whereby the individual may obtain in-
15 formation regarding identity theft.

16 (2) SUBSTITUTE NOTIFICATION.—

17 (A) CIRCUMSTANCES GIVING RISE TO SUB-
18 STITUTE NOTIFICATION.—A covered entity re-
19 quired to provide notification to individuals
20 under subsection (a)(1) may provide substitute
21 notification in lieu of the direct notification re-
22 quired by paragraph (1) if the covered entity
23 owns or possesses data in electronic form con-
24 taining personal information of fewer than

1 1,000 individuals and such direct notification is
2 not feasible due to—

3 (i) excessive cost to the covered entity
4 required to provide such notification rel-
5 ative to the resources of such covered enti-
6 ty, as determined in accordance with the
7 regulations issued by the Commission
8 under paragraph (3)(A); or

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

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

15 (i) e-mail notification to the extent
16 that the covered entity has e-mail address-
17 es of individuals to whom it is required to
18 provide notification under subsection
19 (a)(1);

20 (ii) a conspicuous notice on the Inter-
21 net Web site of the covered entity (if such
22 covered entity maintains such a Web site);
23 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 covered entity, except when the only infor-
18 mation which has been the subject of the
19 security breach is the individual's first
20 name or initial and last name, or address,
21 or phone number, in combination with a
22 credit or debit card number, and any re-
23 quired security 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 cov-
14 ered entity required to provided such notifica-
15 tion relative to the resources of such covered
16 entity. Such regulations may also identify other
17 circumstances where substitute notification
18 would be appropriate for any covered entity, in-
19 cluding circumstances under which the cost of
20 providing notification exceeds the benefits to
21 consumers.

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

1 (i) a description of written or e-mail
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 covered entity required to
11 provide notification under subsection (a) shall, upon
12 request of an individual whose personal information
13 was included in the breach of security, provide or ar-
14 range for the provision of, to each such individual
15 and at 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—

10 (A) determine the circumstances under
11 which a covered entity required to provide noti-
12 fication under subsection (a)(1) shall provide or
13 arrange for the provision of free consumer cred-
14 it reports or credit monitoring or other service
15 to affected individuals; and

16 (B) establish a simple process under which
17 a covered entity that is a small business or
18 small non-profit organization may request a
19 partial waiver or a modified or alternative
20 means of responding if providing or arranging
21 for such reports, monitoring, or service is not
22 feasible due to excessive costs relative to the re-
23 sources of the small business or small non-prof-
24 it entity and the level of harm to consumers
25 caused by the data breach.

1 (f) EXEMPTION.—

2 (1) GENERAL EXEMPTION.—A covered entity
3 shall be exempt from the requirements under this
4 section if, following a breach of security, such cov-
5 ered entity determines that there is no reasonable
6 risk of identity theft, fraud, or other unlawful con-
7 duct.

8 (2) PRESUMPTION.—

9 (A) IN GENERAL.—If the data in electronic
10 form containing personal information is ren-
11 dered unusable, unreadable, or indecipherable
12 through a security technology or methodology
13 (if the technology or methodology is generally
14 accepted by experts in the information security
15 field), there shall be a presumption that no rea-
16 sonable risk of identity theft, fraud, or other
17 unlawful conduct exists following a breach of
18 security of such data. Any such presumption
19 may be rebutted by facts demonstrating that
20 the security technologies or methodologies in a
21 specific case, have been or are reasonably likely
22 to be compromised.

23 (B) METHODOLOGIES OR TECH-
24 NOLOGIES.—Not later than 1 year after the
25 date of the enactment of this Act and bian-

1 nually thereafter, the Commission, after con-
2 sultation with the National Institute of Stand-
3 ards and Technology, shall issue rules (pursu-
4 ant to section 553 of title 5, United States
5 Code) or guidance to identify security meth-
6 odologies or technologies, such as encryption,
7 which render data in electronic form unusable,
8 unreadable, or indecipherable, that shall, if ap-
9 plied to such data, establish a presumption that
10 no reasonable risk of identity theft, fraud, or
11 other unlawful conduct exists following a breach
12 of security of such data. Any such presumption
13 may be rebutted by facts demonstrating that
14 any such methodology or technology in a spe-
15 cific case has been or is reasonably likely to be
16 compromised. In issuing such rules or guidance,
17 the Commission also shall consult with relevant
18 industries, consumer organizations, and data
19 security and identity theft prevention experts
20 and established standards setting bodies.

21 (3) FTC GUIDANCE.—Not later than 1 year
22 after the date of the enactment of this Act the Com-
23 mission, after consultation with the National Insti-
24 tute of Standards and Technology, shall issue guid-

1 ance regarding the application of the exemption in
2 paragraph (1).

3 (g) WEB SITE 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 Web site
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 Web site.

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 covered entity who is in compliance with any
24 other Federal law that requires such covered entity to pro-
25 vide notification to individuals following a breach of secu-

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

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

7 (a) GENERAL APPLICATION.—The requirements of
8 sections 2 and 3 apply to—

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

13 (2) notwithstanding section 4 and section
14 5(a)(2) of that Act (15 U.S.C. 44 and 45(a)(2)),
15 any non-profit organization, including any organiza-
16 tion described in section 501(c) of the Internal Rev-
17 enue Code of 1986 that is exempt from taxation
18 under section 501(a) of such Code.

19 (b) ENFORCEMENT BY THE FEDERAL TRADE COM-
20 MISSION.—

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

1 57a(a)(1)(B)) regarding unfair or deceptive acts or
2 practices.

3 (2) POWERS OF COMMISSION.—The Commis-
4 sion shall enforce this Act in the same manner, by
5 the same means, and with the same jurisdiction,
6 powers, and duties as though all applicable terms
7 and provisions of the Federal Trade Commission Act
8 (15 U.S.C. 41 et seq.) were incorporated into and
9 made a part of this Act. Any covered entity who vio-
10 lates such regulations shall be subject to the pen-
11 alties and entitled to the privileges and immunities
12 provided in that Act.

13 (3) LIMITATION.—In promulgating rules under
14 this Act, the Commission shall not require the de-
15 ployment or use of any specific products or tech-
16 nologies, including any specific computer software or
17 hardware.

18 (c) ENFORCEMENT BY STATE ATTORNEYS GEN-
19 ERAL.—

20 (1) CIVIL ACTION.—In any case in which the
21 attorney general of a State, or an official or agency
22 of a State, has reason to believe that an interest of
23 the residents of that State has been or is threatened
24 or adversely affected by any covered entity who vio-
25 lates section 2 or 3 of this Act, the attorney general,

1 official, or agency of the State, as *parens patriae*,
2 may bring a civil action on behalf of the residents
3 of the State in a district court of the United States
4 of appropriate jurisdiction—

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

7 (B) to compel compliance with such sec-
8 tion;

9 (C) to obtain damages, restitution, or other
10 compensation on behalf of such residents, or to
11 obtain such further and other relief as the court
12 may deem appropriate; or

13 (D) to obtain civil penalties in the amount
14 determined under paragraph (2).

15 (2) CIVIL PENALTIES.—

16 (A) CALCULATION.—

17 (i) TREATMENT OF VIOLATIONS OF
18 SECTION 2.—For purposes of paragraph
19 (1)(D) with regard to a violation of section
20 2, the amount determined under this para-
21 graph is the amount calculated by multi-
22 plying the number of days that a covered
23 entity is not in compliance with such sec-
24 tion by an amount not greater than
25 \$11,000.

1 (ii) TREATMENT OF VIOLATIONS OF
2 SECTION 3.—For purposes of paragraph
3 (1)(D) with regard to a violation of section
4 3, the amount determined under this para-
5 graph is the amount calculated by multi-
6 plying the number of violations of such
7 section by an amount not greater than
8 \$11,000. Each failure to send notification
9 as required under section 3 to a resident of
10 the State shall be treated as a separate
11 violation.

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

23 (C) MAXIMUM TOTAL LIABILITY.—Not-
24 withstanding the number of actions which may
25 be brought against a covered entity under this

1 subsection the maximum civil penalty for which
2 any covered entity may be liable under this sub-
3 section shall not exceed—

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

6 (ii) \$5,000,000 for all violations of
7 section 3 resulting from a single breach of
8 security.

9 (3) INTERVENTION BY THE FTC.—

10 (A) NOTICE AND INTERVENTION.—The
11 State shall provide prior written notice of any
12 action under paragraph (1) to the Commission
13 and provide the Commission with a copy of its
14 complaint, except in any case in which such
15 prior notice is not feasible, in which case the
16 State shall serve such notice immediately upon
17 instituting such action. The Commission shall
18 have the right—

19 (i) to intervene in the action;

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

22 (iii) to file petitions for appeal.

23 (B) LIMITATION ON STATE ACTION WHILE
24 FEDERAL ACTION IS PENDING.—If the Commis-
25 sion has instituted a civil action for violation of

1 this Act, no State attorney general, or official
 2 or agency of a State, may bring an action under
 3 this subsection during the pendency of that ac-
 4 tion against any defendant named in the com-
 5 plaint of the Commission for any violation of
 6 this Act alleged in the complaint.

7 (4) CONSTRUCTION.—For purposes of bringing
 8 any civil action under paragraph (1), nothing in this
 9 Act shall be construed to prevent an attorney gen-
 10 eral of a State from exercising the powers conferred
 11 on the attorney general by the laws of that State
 12 to—

13 (A) conduct investigations;

14 (B) administer oaths or affirmations; or

15 (C) compel the attendance of witnesses or
 16 the production of documentary and other evi-
 17 dence.

18 (d) AFFIRMATIVE DEFENSE FOR A VIOLATION OF
 19 SECTION 3.—

20 (1) IN GENERAL.—It shall be an affirmative de-
 21 fense to an enforcement action brought under sub-
 22 section (b), or a civil action brought under sub-
 23 section (c), based on a violation of section 3, that all
 24 of the personal information contained in the data in
 25 electronic form that was acquired or accessed as a

1 result of a breach of security of the defendant is
2 public record information that is lawfully made
3 available to the general public from Federal, State,
4 or local government records and was acquired by the
5 defendant from such records.

6 (2) NO EFFECT ON OTHER REQUIREMENTS.—
7 Nothing in this subsection shall be construed to ex-
8 empt any covered entity from the requirement to no-
9 tify the Commission of a breach of security as re-
10 quired under section 3(a).

11 **SEC. 5. DEFINITIONS.**

12 In this Act the following definitions apply:

13 (1) BREACH OF SECURITY.—The term “breach
14 of security” means unauthorized access to or acqui-
15 sition of data in electronic form containing personal
16 information.

17 (2) COMMISSION.—The term “Commission”
18 means the Federal Trade Commission.

19 (3) COVERED ENTITY.—The term “covered en-
20 tity” means a sole proprietorship, partnership, cor-
21 poration, trust, estate, cooperative, association, or
22 other commercial entity, and any charitable, edu-
23 cational, or nonprofit organization, that acquires,
24 maintains, or utilizes personal information.

1 (4) DATA IN ELECTRONIC FORM.—The term
2 “data in electronic form” means any data stored
3 electronically or digitally on any computer system or
4 other database and includes recordable tapes and
5 other mass storage devices.

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

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

21 (7) INFORMATION BROKER.—The term “infor-
22 mation broker”—

23 (A) means a commercial entity whose busi-
24 ness is to collect, assemble, or maintain per-
25 sonal information concerning individuals who

1 are not current or former customers of such en-
2 tity in order to sell such information or provide
3 access to such information to any nonaffiliated
4 third party in exchange for consideration,
5 whether such collection, assembly, or mainte-
6 nance of personal information is performed by
7 the information broker directly, or by contract
8 or subcontract with any other entity; and

9 (B) does not include a commercial entity to
10 the extent that such entity processes informa-
11 tion collected by or on behalf of and received
12 from or on behalf of a nonaffiliated third party
13 concerning individuals who are current or
14 former customers or employees of such third
15 party to enable such third party directly or
16 through parties acting on its behalf to: (1) pro-
17 vide benefits for its employees; or (2) directly
18 transact business with its customers.

19 (8) MAJOR CREDIT REPORTING AGENCY.—The
20 term “major credit reporting agency” means a con-
21 sumer reporting agency that compiles and maintains
22 files on consumers on a nationwide basis within the
23 meaning of section 603(p) of the Fair Credit Re-
24 porting Act (5 U.S.C. 1681a(p)).

25 (9) PERSONAL INFORMATION.—

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

6 (i) Social Security number.

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

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

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

21 (i) for the purpose of section 2 to the
22 extent that such modification will not un-
23 reasonably impede interstate commerce,
24 and will accomplish the purposes of this
25 Act; or

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

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

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

18 (12) SERVICE PROVIDER.—The term “service
19 provider” means a covered entity that provides elec-
20 tronic data transmission, routing, intermediate and
21 transient storage, or connections to its system or
22 network, where the covered entity providing such
23 services does not select or modify the content of the
24 electronic data, is not the sender or the intended re-
25 cipient of the data, and such covered entity trans-

1 mits, routes, stores, or provides connections for per-
2 sonal information in a manner that personal infor-
3 mation is undifferentiated from other types of data
4 that such covered entity transmits, routes, stores, or
5 provides connections. Any such covered entity shall
6 be treated as a service provider under this Act only
7 to the extent that it is engaged in the provision of
8 such transmission, routing, intermediate and tran-
9 sient storage or connections.

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

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

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

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

23 (b) **ADDITIONAL PREEMPTION.**—

24 (1) **IN GENERAL.**—No person other than a per-
25 son specified in section 4(c) may bring a civil action

1 under the laws of any State if such action is pre-
2 mised in whole or in part upon the defendant vio-
3 lating any provision of this Act.

4 (2) PROTECTION OF CONSUMER PROTECTION
5 LAWS.—Except as provided in subsection (a) of this
6 section, this subsection shall not be construed to
7 limit the enforcement of any State consumer protec-
8 tion law by an Attorney General of a State.

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

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

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

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

19 **SEC. 7. EFFECTIVE DATE.**

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

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

2 There are authorized to be appropriated to the Com-
3 mission \$1,000,000 for each of fiscal years 2012 through
4 2016 to carry out this Act.

○