

## Union Calendar No. 214

111<sup>TH</sup> CONGRESS  
1<sup>ST</sup> SESSION

# H. R. 2221

[Report No. 111-362]

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

APRIL 30, 2009

Mr. RUSH (for himself, Mr. STEARNS, Mr. BARTON of Texas, Ms. SCHAKOWSKY, and Mr. RADANOVICH) introduced the following bill; which was referred to the Committee on Energy and Commerce

DECEMBER 8, 2009

Reported with amendments, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in *italie*]

[For text of introduced bill, see copy of bill as introduced on April 30, 2009]

# **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 and*  
5 *Trust Act”.*

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

7 *(a) GENERAL SECURITY POLICIES AND PROCE-*  
8 *DURES.—*

9 *(1) REGULATIONS.—Not later than 1 year after*  
10 *the date of enactment of this Act, the Commission*  
11 *shall promulgate regulations under section 553 of title*  
12 *5, United States Code, to require each person engaged*  
13 *in interstate commerce that owns or possesses data*  
14 *containing personal information, or contracts to have*  
15 *any third party entity maintain such data for such*  
16 *person, to establish and implement policies and proce-*  
17 *dures regarding information security practices for the*  
18 *treatment and protection of personal information tak-*  
19 *ing into consideration—*

20 *(A) the size of, and the nature, scope, and*  
21 *complexity of the activities engaged in by, such*  
22 *person;*

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

1           (C) *the cost of implementing such safe-*  
2           *guards.*

3           (2) *REQUIREMENTS.*—*Such regulations shall re-*  
4           *quire the policies and procedures to include the fol-*  
5           *lowing:*

6                   (A) *A security policy with respect to the col-*  
7                   *lection, use, sale, other dissemination, and main-*  
8                   *tenance of such personal information.*

9                   (B) *The identification of an officer or other*  
10                  *individual as the point of contact with responsi-*  
11                  *bility for the management of information secu-*  
12                  *rity.*

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

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

1           (E) A process for disposing of data in elec-  
2           tronic form containing personal information by  
3           shredding, permanently erasing, or otherwise  
4           modifying the personal information contained in  
5           such data to make such personal information  
6           permanently unreadable or undecipherable.

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

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

21          (b) *SPECIAL REQUIREMENTS FOR INFORMATION BRO-*  
22          *KERS.*—

23          (1) *SUBMISSION OF POLICIES TO THE FTC.*—The  
24          regulations promulgated under subsection (a) shall re-  
25          quire each information broker to submit its security

1 *policies to the Commission in conjunction with a no-*  
2 *tification of a breach of security under section 3 or*  
3 *upon request of the Commission.*

4 (2) *POST-BREACH AUDIT.—For any information*  
5 *broker required to provide notification under section*  
6 *3, the Commission may conduct audits of the infor-*  
7 *mation security practices of such information broker,*  
8 *or require the information broker to conduct inde-*  
9 *pendent audits of such practices (by an independent*  
10 *auditor who has not audited such information bro-*  
11 *ker’s security practices during the preceding 5 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 procedures*  
17 *to assure the maximum possible accuracy of*  
18 *the personal information it collects, assem-*  
19 *bles, or maintains, and any other informa-*  
20 *tion it collects, assembles, or maintains that*  
21 *specifically identifies an individual, other*  
22 *than information which merely identifies*  
23 *an individual’s name or address.*

24 (ii) *LIMITED EXCEPTION FOR FRAUD*  
25 *DATABASES.—The requirement in clause (i)*

1 shall not prevent the collection or mainte-  
2 nance of information that may be inac-  
3 curate with respect to a particular indi-  
4 vidual when that information is being col-  
5 lected or maintained solely—

6 (I) for the purpose of indicating  
7 whether there may be a discrepancy or  
8 irregularity in the personal informa-  
9 tion that is associated with an indi-  
10 vidual; and

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

15 (B) CONSUMER ACCESS TO INFORMATION.—

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 to  
22 the individual, and after verifying the  
23 identity of such individual, a means  
24 for the individual to review any per-  
25 sonal information regarding such indi-

1            *vidual maintained by the information*  
2            *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 information*  
10           *broker maintains such a website) in-*  
11           *structing individuals how to request*  
12           *access to the information required to be*  
13           *provided under subclause (I), and, as*  
14           *applicable, how to express a preference*  
15           *with respect to the use of personal in-*  
16           *formation for marketing purposes*  
17           *under clause (iii).*

18           *(ii) DISPUTED INFORMATION.—When-*  
19           *ever an individual whose information the*  
20           *information broker maintains makes a*  
21           *written request disputing the accuracy of*  
22           *any such information, the information*  
23           *broker, after verifying the identity of the in-*  
24           *dividual making such request and unless*

1                    *there are reasonable grounds to believe such*  
2                    *request is frivolous or irrelevant, shall—*

3                    *(I) correct any inaccuracy; or*

4                    *(II)(aa) in the case of information*  
5                    *that is public record information, in-*  
6                    *form the individual of the source of the*  
7                    *information, and, if reasonably avail-*  
8                    *able, where a request for correction*  
9                    *may be directed and, if the individual*  
10                   *provides proof that the public record*  
11                   *has been corrected or that the informa-*  
12                   *tion broker was reporting the informa-*  
13                   *tion incorrectly, correct the inaccuracy*  
14                   *in the information broker's records; or*

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

1                   (iii) *ALTERNATIVE PROCEDURE FOR*  
2                   *CERTAIN MARKETING INFORMATION.*—*In ac-*  
3                   *cordance with regulations issued under*  
4                   *clause (v), an information broker that*  
5                   *maintains any information described in*  
6                   *clause (i) which is used, shared, or sold by*  
7                   *such information broker for marketing pur-*  
8                   *poses, may, in lieu of complying with the*  
9                   *access and dispute requirements set forth in*  
10                  *clauses (i) and (ii), provide each individual*  
11                  *whose information it maintains with a rea-*  
12                  *sonable means of expressing a preference not*  
13                  *to have his or her information used for such*  
14                  *purposes. If the individual expresses such a*  
15                  *preference, the information broker may not*  
16                  *use, share, or sell the individual's informa-*  
17                  *tion for marketing purposes.*

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

1                   (I) *If access of the individual to*  
2                   *the information is limited by law or le-*  
3                   *gally recognized privilege.*

4                   (II) *If the information is used for*  
5                   *a legitimate governmental or fraud*  
6                   *prevention purpose that would be com-*  
7                   *promised by such access.*

8                   (III) *If the information consists of*  
9                   *a published media record, unless that*  
10                   *record has been included in a report*  
11                   *about an individual shared with a*  
12                   *third party.*

13                   (v) *RULEMAKING.—Not later than 1*  
14                   *year after the date of the enactment of this*  
15                   *Act, the Commission shall promulgate regu-*  
16                   *lations under section 553 of title 5, United*  
17                   *States Code, to carry out this paragraph*  
18                   *and to facilitate the purposes of this Act. In*  
19                   *addition, the Commission shall issue regula-*  
20                   *tions, as necessary, under section 553 of*  
21                   *title 5, United States Code, on the scope of*  
22                   *the application of the limitations in clause*  
23                   *(iv), including any additional cir-*  
24                   *cumstances in which an information broker*  
25                   *may limit access to information under such*

1           *clause that the Commission determines to be*  
2           *appropriate.*

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

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

21          (5) *PROHIBITION ON PRETEXTING BY INFORMA-*  
22          *TION BROKERS.*—

23                 (A) *PROHIBITION ON OBTAINING PERSONAL*  
24                 *INFORMATION BY FALSE PRETENSES.*—*It shall be*  
25                 *unlawful for an information broker to obtain or*

1           *attempt to obtain, or cause to be disclosed or at-*  
2           *tempt to cause to be disclosed to any person, per-*  
3           *sonal information or any other information re-*  
4           *lating to any person by—*

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

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

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

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

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

8           (a) *NATIONWIDE NOTIFICATION.*—*Any person engaged*  
9 *in interstate commerce that owns or possesses data in elec-*  
10 *tronic form containing personal information shall, fol-*  
11 *lowing the discovery of a breach of security of the system*  
12 *maintained by such person that contains such data—*

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

17                   (2) *notify the Commission.*

18           (b) *SPECIAL NOTIFICATION REQUIREMENTS.*—

19                   (1) *THIRD PARTY AGENTS.*—*In the event of a*  
20 *breach of security by any third party entity that has*  
21 *been contracted to maintain or process data in elec-*  
22 *tronic form containing personal information on be-*  
23 *half of any other person who owns or possesses such*  
24 *data, such third party entity shall be required to no-*  
25 *tify such person of the breach of security. Upon re-*

1       ceiving such notification from such third party, such  
2       person shall provide the notification required under  
3       subsection (a).

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

18              (3) *COORDINATION OF NOTIFICATION WITH*  
19      *CREDIT REPORTING AGENCIES.*—If a person is re-  
20      quired to provide notification to more than 5,000 in-  
21      dividuals under subsection (a)(1), the person shall  
22      also notify the major credit reporting agencies that  
23      compile and maintain files on consumers on a na-  
24      tionwide basis, of the timing and distribution of the  
25      notices. Such notice shall be given to the credit report-

1        *ing agencies without unreasonable delay and, if it*  
2        *will not delay notice to the affected individuals, prior*  
3        *to the distribution of notices to the affected individ-*  
4        *uals.*

5        *(c) TIMELINESS OF NOTIFICATION.—*

6            *(1) IN GENERAL.—Unless subject to a delay au-*  
7        *thorized under paragraph (2), a notification required*  
8        *under subsection (a) shall be made not later than 60*  
9        *days following the discovery of a breach of security,*  
10       *unless the person providing notice can show that pro-*  
11       *viding notice within such a time frame is not feasible*  
12       *due to extraordinary circumstances necessary to pre-*  
13       *vent further breach or unauthorized disclosures, and*  
14       *reasonably restore the integrity of the data system, in*  
15       *which case such notification shall be made as prompt-*  
16       *ly as possible.*

17            *(2) DELAY OF NOTIFICATION AUTHORIZED FOR*  
18        *LAW ENFORCEMENT OR NATIONAL SECURITY PUR-*  
19        *POSES.—*

20            *(A) LAW ENFORCEMENT.—If a Federal,*  
21        *State, or local law enforcement agency deter-*  
22        *mines that the notification required under this*  
23        *section would impede a civil or criminal inves-*  
24        *tigation, such notification shall be delayed upon*  
25        *the written request of the law enforcement agency*

1        *for 30 days or such lesser period of time which*  
2        *the law enforcement agency determines is reason-*  
3        *ably necessary and requests in writing. A law*  
4        *enforcement agency may, by a subsequent writ-*  
5        *ten request, revoke such delay or extend the pe-*  
6        *riod of time set forth in the original request*  
7        *made under this paragraph if further delay is*  
8        *necessary.*

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

23        *(d) METHOD AND CONTENT OF NOTIFICATION.—*

24                *(1) DIRECT NOTIFICATION.—*

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

9                   (i) *Written notification.*

10                   (ii) *Notification by email or other elec-*  
11                   *tronic means , if—*

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

16                           (II) *the individual has consented*  
17                           *to receive such notification and the no-*  
18                           *tification is provided in a manner that*  
19                           *is consistent with the provisions per-*  
20                           *mitting electronic transmission of no-*  
21                           *tices under section 101 of the Elec-*  
22                           *tronic Signatures in Global Commerce*  
23                           *Act (15 U.S.C. 7001).*

24           (B) *CONTENT OF NOTIFICATION.*—*Regard-*  
25           *less of the method by which notification is pro-*

1            *vided to an individual under subparagraph (A),*  
2            *such notification shall include—*

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

6                    *(ii) a telephone number that the indi-*  
7                    *vidual may use, at no cost to such indi-*  
8                    *vidual, to contact the person to inquire*  
9                    *about the breach of security or the informa-*  
10                   *tion the person maintained about that indi-*  
11                   *vidual;*

12                   *(iii) notice that the individual is enti-*  
13                   *tled to receive, at no cost to such individual,*  
14                   *consumer credit reports on a quarterly basis*  
15                   *for a period of 2 years, or credit monitoring*  
16                   *or other service that enables consumers to*  
17                   *detect the misuse of their personal informa-*  
18                   *tion for a period of 2 years, and instruc-*  
19                   *tions to the individual on requesting such*  
20                   *reports or service from the person, except*  
21                   *when the only information which has been*  
22                   *the subject of the security breach is the indi-*  
23                   *vidual's first name or initial and last*  
24                   *name, or address, or phone number, in com-*

1                    *ination with a credit or debit card num-*  
2                    *ber, and any required security code;*

3                    *(iv) the toll-free contact telephone num-*  
4                    *bers and addresses for the major credit re-*  
5                    *porting agencies; and*

6                    *(v) a toll-free telephone number and*  
7                    *Internet website address for the Commission*  
8                    *whereby the individual may obtain infor-*  
9                    *mation regarding identity theft.*

10                    *(2) SUBSTITUTE NOTIFICATION.—*

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

20                    *(i) excessive cost to the person required*  
21                    *to provide such notification relative to the*  
22                    *resources of such person, as determined in*  
23                    *accordance with the regulations issued by*  
24                    *the Commission under paragraph (3)(A); or*

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

4                   (B) FORM OF SUBSTITUTE NOTIFICATION.—

5                   Such substitute notification shall include—

6                   (i) email notification to the extent that  
7                   the person has email addresses of individ-  
8                   uals to whom it is required to provide noti-  
9                   fication under subsection (a)(1);

10                  (ii) a conspicuous notice on the Inter-  
11                  net website of the person (if such person  
12                  maintains such a website); and

13                  (iii) notification in print and to  
14                  broadcast media, including major media in  
15                  metropolitan and rural areas where the in-  
16                  dividuals whose personal information was  
17                  acquired reside.

18                  (C) CONTENT OF SUBSTITUTE NOTICE.—

19                  Each form of substitute notice under this para-  
20                  graph shall include—

21                  (i) notice that individuals whose per-  
22                  sonal information is included in the breach  
23                  of security are entitled to receive, at no cost  
24                  to the individuals, consumer credit reports  
25                  on a quarterly basis for a period of 2 years,

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

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

17           (3) *REGULATIONS AND GUIDANCE.*—

18                 (A) *REGULATIONS.*—Not later than 1 year  
19           after the date of enactment of this Act, the Com-  
20           mission shall, by regulation under section 553 of  
21           title 5, United States Code, establish criteria for  
22           determining circumstances under which sub-  
23           stitute notification may be provided under para-  
24           graph (2), including criteria for determining if  
25           notification under paragraph (1) is not feasible

1           *due to excessive costs to the person required to*  
2           *provided such notification relative to the re-*  
3           *sources of such person. Such regulations may*  
4           *also identify other circumstances where sub-*  
5           *stitute notification would be appropriate for any*  
6           *person, including circumstances under which the*  
7           *cost of providing notification exceeds the benefits*  
8           *to consumers.*

9           *(B) GUIDANCE.—In addition, the Commis-*  
10          *sion shall provide and publish general guidance*  
11          *with respect to compliance with this subsection.*  
12          *Such guidance shall include—*

13                 *(i) a description of written or email*  
14                 *notification that complies with the require-*  
15                 *ments of paragraph (1); and*

16                 *(ii) guidance on the content of sub-*  
17                 *stitute notification under paragraph (2),*  
18                 *including the extent of notification to print*  
19                 *and broadcast media that complies with the*  
20                 *requirements of such paragraph.*

21          *(e) OTHER OBLIGATIONS FOLLOWING BREACH.—*

22                 *(1) IN GENERAL.—A person required to provide*  
23                 *notification under subsection (a) shall, upon request*  
24                 *of an individual whose personal information was in-*  
25                 *cluded in the breach of security, provide or arrange*

1     *for the provision of, to each such individual and at*  
2     *no cost to such individual—*

3             *(A) consumer credit reports from at least*  
4             *one of the major credit reporting agencies begin-*  
5             *ning not later than 60 days following the indi-*  
6             *vidual's request and continuing on a quarterly*  
7             *basis for a period of 2 years thereafter; or*

8             *(B) a credit monitoring or other service that*  
9             *enables consumers to detect the misuse of their*  
10            *personal information, beginning not later than*  
11            *60 days following the individual's request and*  
12            *continuing for a period of 2 years.*

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

19            *(3) RULEMAKING.—As part of the Commission's*  
20            *rulemaking described in subsection (d)(3), the Com-*  
21            *mission shall determine the circumstances under*  
22            *which a person required to provide notification under*  
23            *subsection (a)(1) shall provide or arrange for the pro-*  
24            *vision of free consumer credit reports or credit moni-*  
25            *toring or other service to affected individuals.*

1 (f) *EXEMPTION.*—

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

7 (2) *PRESUMPTION.*—

8 (A) *IN GENERAL.*—*If the data in electronic*  
9 *form containing personal information is ren-*  
10 *dered unusable, unreadable, or indecipherable*  
11 *through encryption or other security technology*  
12 *or methodology (if the method of encryption or*  
13 *such other 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 un-*  
17 *lawful conduct exists following a breach of secu-*  
18 *rity of such data. Any such presumption may be*  
19 *rebutted by facts demonstrating that the*  
20 *encryption or other security technologies or*  
21 *methodologies in a specific case, have been or are*  
22 *reasonably likely to be compromised.*

23 (B) *METHODOLOGIES OR TECHNOLOGIES.*—  
24 *Not later than 1 year after the date of the enact-*  
25 *ment of this Act and biannually thereafter, the*

1           Commission shall issue rules (pursuant to sec-  
2           tion 553 of title 5, United States Code) or guid-  
3           ance to identify security methodologies or tech-  
4           nologies which render data in electronic form  
5           unusable, unreadable, or indecipherable, that  
6           shall, if applied to such data, establish a pre-  
7           sumption that no reasonable risk of identity  
8           theft, fraud, or other unlawful conduct exists fol-  
9           lowing a breach of security of such data. Any  
10          such presumption may be rebutted by facts dem-  
11          onstrating that any such methodology or tech-  
12          nology in a specific case has been or is reason-  
13          ably likely to be compromised. In issuing such  
14          rules or guidance, the Commission shall consult  
15          with relevant industries, consumer organizations,  
16          and data security and identity theft prevention  
17          experts and established standards setting bodies.

18          (3) *FTC GUIDANCE*.—Not later than 1 year after  
19          the date of the enactment of this Act the Commission  
20          shall issue guidance regarding the application of the  
21          exemption in paragraph (1).

22          (g) *WEBSITE NOTICE OF FEDERAL TRADE COMMIS-*  
23          *SION*.—If the Commission, upon receiving notification of  
24          any breach of security that is reported to the Commission  
25          under subsection (a)(2), finds that notification of such a

1 *breach of security via the Commission's Internet website*  
2 *would be in the public interest or for the protection of con-*  
3 *sumers, the Commission shall place such a notice in a clear*  
4 *and conspicuous location on its Internet website.*

5       *(h) FTC STUDY ON NOTIFICATION IN LANGUAGES IN*  
6 *ADDITION TO ENGLISH.—Not later than 1 year after the*  
7 *date of enactment of this Act, the Commission shall conduct*  
8 *a study on the practicality and cost effectiveness of requir-*  
9 *ing the notification required by subsection (d)(1) to be pro-*  
10 *vided in a language in addition to English to individuals*  
11 *known to speak only such other language.*

12       *(i) GENERAL RULEMAKING AUTHORITY.—The Com-*  
13 *mission may promulgate regulations necessary under sec-*  
14 *tion 553 of title 5, United States Code, to effectively enforce*  
15 *the requirements of this section.*

16       *(j) TREATMENT OF PERSONS GOVERNED BY OTHER*  
17 *LAW.—A person who is in compliance with any other Fed-*  
18 *eral law that requires such person to provide notification*  
19 *to individuals following a breach of security, and that,*  
20 *taken as a whole, provides protections substantially similar*  
21 *to, or greater than, those required under this section, as the*  
22 *Commission shall determine by rule (under section 553 of*  
23 *title 5, United States Code), shall be deemed to be in compli-*  
24 *ance with this section.*

1 **SEC. 4. APPLICATION AND ENFORCEMENT.**

2       (a) *GENERAL APPLICATION.*—*The requirements of sec-*  
3 *tions 2 and 3 shall only apply to those persons, partner-*  
4 *ships, or corporations over which the Commission has au-*  
5 *thority pursuant to section 5(a)(2) of the Federal Trade*  
6 *Commission Act.*

7       (b) *ENFORCEMENT BY THE FEDERAL TRADE COMMIS-*  
8 *SION.*—

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 Commission*  
17 *shall enforce this Act in the same manner, by the*  
18 *same means, and with the same jurisdiction, powers,*  
19 *and duties as though all applicable terms and provi-*  
20 *sions of the Federal Trade Commission Act (15*  
21 *U.S.C. 41 et seq.) were incorporated into and made*  
22 *a part of this Act. Any person who violates such regu-*  
23 *lations shall be subject to the penalties and entitled to*  
24 *the privileges and immunities provided in that Act.*

25           (3) *LIMITATION.*—*In promulgating rules under*  
26 *this Act, the Commission shall not require the deploy-*

1 *ment or use of any specific products or technologies,*  
2 *including any specific computer software or hard-*  
3 *ware.*

4 *(c) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—*

5 *(1) CIVIL ACTION.—In any case in which the at-*  
6 *torney general of a State, or an official or agency of*  
7 *a State, has reason to believe that an interest of the*  
8 *residents of that State has been or is threatened or*  
9 *adversely affected by any person who violates section*  
10 *2 or 3 of this Act, the attorney general, official, or*  
11 *agency of the State, as parens patriae, may bring a*  
12 *civil action on behalf of the residents of the State in*  
13 *a district court of the United States of appropriate*  
14 *jurisdiction—*

15 *(A) to enjoin further violation of such sec-*  
16 *tion by the defendant;*

17 *(B) to compel compliance with such section;*

18 *or*

19 *(C) to obtain civil penalties in the amount*  
20 *determined under paragraph (2).*

21 *(2) CIVIL PENALTIES.—*

22 *(A) CALCULATION.—*

23 *(i) TREATMENT OF VIOLATIONS OF*  
24 *SECTION 2.—For purposes of paragraph*  
25 *(1)(C) with regard to a violation of section*

1           2, the amount determined under this para-  
2           graph is the amount calculated by multi-  
3           plying the number of days that a person is  
4           not in compliance with such section by an  
5           amount not greater than \$11,000.

6           (ii) *TREATMENT OF VIOLATIONS OF*  
7           *SECTION 3.*—For purposes of paragraph  
8           (1)(C) with regard to a violation of section  
9           3, the amount determined under this para-  
10          graph is the amount calculated by multi-  
11          plying the number of violations of such sec-  
12          tion by an amount not greater than  
13          \$11,000. Each failure to send notification  
14          as required under section 3 to a resident of  
15          the State shall be treated as a separate vio-  
16          lation.

17          (B) *ADJUSTMENT FOR INFLATION.*—Begin-  
18          ning on the date that the Consumer Price Index  
19          is first published by the Bureau of Labor Statis-  
20          tics that is after 1 year after the date of enact-  
21          ment of this Act, and each year thereafter, the  
22          amounts specified in clauses (i) and (ii) of sub-  
23          paragraph (A) shall be increased by the percent-  
24          age increase in the Consumer Price Index pub-

1            *lished on that date from the Consumer Price*  
2            *Index published the previous year.*

3            (C) *MAXIMUM TOTAL LIABILITY.*—*Notwith-*  
4            *standing the number of actions which may be*  
5            *brought against a person under this subsection*  
6            *the maximum civil penalty for which any person*  
7            *may be liable under this subsection shall not ex-*  
8            *ceed—*

9                            (i) *\$5,000,000 for each violation of sec-*  
10                           *tion 2; and*

11                           (ii) *\$5,000,000 for all violations of sec-*  
12                           *tion 3 resulting from a single breach of se-*  
13                           *curity.*

14            (3) *INTERVENTION BY THE FTC.*—

15                           (A) *NOTICE AND INTERVENTION.*—*The State*  
16                           *shall provide prior written notice of any action*  
17                           *under paragraph (1) to the Commission and*  
18                           *provide the Commission with a copy of its com-*  
19                           *plaint, except in any case in which such prior*  
20                           *notice is not feasible, in which case the State*  
21                           *shall serve such notice immediately upon insti-*  
22                           *tuting such action. The Commission shall have*  
23                           *the right—*

24                                            (i) *to intervene in the action;*

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

3                   (iii) to file petitions for appeal.

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

13                  (4) *CONSTRUCTION.*—For purposes of bringing  
14                  any civil action under paragraph (1), nothing in this  
15                  Act shall be construed to prevent an attorney general  
16                  of a State from exercising the powers conferred on the  
17                  attorney general by the laws of that State to—

18                         (A) conduct investigations;

19                         (B) administer oaths or affirmations; or

20                         (C) compel the attendance of witnesses or  
21                         the production of documentary and other evi-  
22                         dence.

23                  (d) *AFFIRMATIVE DEFENSE FOR A VIOLATION OF SEC-*  
24                  *TION 3.*—

1           (1) *IN GENERAL.*—*It shall be an affirmative de-*  
2 *fense to an enforcement action brought under sub-*  
3 *section (b), or a civil action brought under subsection*  
4 *(c), based on a violation of section 3, that all of the*  
5 *personal information contained in the data in elec-*  
6 *tronic form that was acquired or accessed as a result*  
7 *of a breach of security of the defendant is public*  
8 *record information that is lawfully made available to*  
9 *the general public from Federal, State, or local gov-*  
10 *ernment records and was acquired by the defendant*  
11 *from such records.*

12           (2) *NO EFFECT ON OTHER REQUIREMENTS.*—  
13 *Nothing in this subsection shall be construed to ex-*  
14 *empt any person from the requirement to notify the*  
15 *Commission of a breach of security as required under*  
16 *section 3(a).*

17 **SEC. 5. DEFINITIONS.**

18 *In this Act the following definitions apply:*

19           (1) *BREACH OF SECURITY.*—*The term “breach of*  
20 *security” means unauthorized access to or acquisition*  
21 *of data in electronic form containing personal infor-*  
22 *mation.*

23           (2) *COMMISSION.*—*The term “Commission”*  
24 *means the Federal Trade Commission.*

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

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

15           (5) *IDENTITY THEFT.*—*The term “identity theft”*  
16           *means the unauthorized use of another person’s per-*  
17           *sonal information for the purpose of engaging in com-*  
18           *mercial transactions under the name of such other*  
19           *person.*

20           (6) *INFORMATION BROKER.*—*The term “informa-*  
21           *tion broker”—*

22                    (A) *means a commercial entity whose busi-*  
23                    *ness is to collect, assemble, or maintain personal*  
24                    *information concerning individuals who are not*  
25                    *current or former customers of such entity in*

1           *order to sell such information or provide access*  
2           *to such information to any nonaffiliated third*  
3           *party in exchange for consideration, whether*  
4           *such collection, assembly, or maintenance of per-*  
5           *sonal information is performed by the informa-*  
6           *tion broker directly, or by contract or sub-*  
7           *contract with any other entity; and*

8           *(B) does not include a commercial entity to*  
9           *the extent that such entity processes information*  
10          *collected by and received from a nonaffiliated*  
11          *third party concerning individuals who are cur-*  
12          *rent or former customers or employees of such*  
13          *third party to enable such third party to (1)*  
14          *provide benefits for its employees or (2) directly*  
15          *transact business with its customers.*

16          (7) *PERSONAL INFORMATION.*—

17                 (A) *DEFINITION.*—*The term “personal in-*  
18                 *formation” means an individual’s first name or*  
19                 *initial and last name, or address, or phone num-*  
20                 *ber, in combination with any 1 or more of the*  
21                 *following data elements for that individual:*

22                         (i) *Social Security number.*

23                         (ii) *Driver’s license number, passport*  
24                         *number, military identification number, or*

1            *other similar number issued on a govern-*  
2            *ment document used to verify identity.*

3            *(iii) Financial account number, or*  
4            *credit or debit card number, and any re-*  
5            *quired security code, access code, or pass-*  
6            *word that is necessary to permit access to*  
7            *an individual’s financial account.*

8            *(B) MODIFIED DEFINITION BY RULE-*  
9            *MAKING.—The Commission may, by rule pro-*  
10           *mulgated under section 553 of title 5, United*  
11           *States Code, modify the definition of “personal*  
12           *information” under subparagraph (A)—*

13           *(i) for the purpose of section 2 to the*  
14           *extent that such modification will not un-*  
15           *reasonably impede interstate commerce, and*  
16           *will accomplish the purposes of this Act; or*

17           *(ii) for the purpose of section 3, to the*  
18           *extent that such modification is necessary to*  
19           *accommodate changes in technology or prac-*  
20           *tices, will not unreasonably impede inter-*  
21           *state commerce, and will accomplish the*  
22           *purposes of this Act.*

23           *(8) PUBLIC RECORD INFORMATION.—The term*  
24           *“public record information” means information about*  
25           *an individual which has been obtained originally*

1       *from records of a Federal, State, or local government*  
2       *entity that are available for public inspection.*

3               (9) *NON-PUBLIC INFORMATION.*—*The term “non-*  
4       *public information” means information about an in-*  
5       *dividual that is of a private nature and neither avail-*  
6       *able to the general public nor obtained from a public*  
7       *record.*

8               (10) *SERVICE PROVIDER.*—*The term “service*  
9       *provider” means an entity that provides to a user*  
10       *transmission, routing, intermediate and transient*  
11       *storage, or connections to its system or network, for*  
12       *electronic communications, between or among points*  
13       *specified by such user of material of the user’s choos-*  
14       *ing, without modification to the content of the mate-*  
15       *rial as sent or received . Any such entity shall be*  
16       *treated as a service provider under this Act only to*  
17       *the extent that it is engaged in the provision of such*  
18       *transmission, routing, intermediate and transient*  
19       *storage or connections.*

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

21               (a) *PREEMPTION OF STATE INFORMATION SECURITY*  
22       *LAWS.*—*This Act supersedes any provision of a statute, reg-*  
23       *ulation, or rule of a State or political subdivision of a*  
24       *State, with respect to those entities covered by the regula-*  
25       *tions issued pursuant to this Act, that expressly—*

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

4           (2) *requires notification to individuals of a*  
5 *breach of security resulting in unauthorized access to*  
6 *or acquisition of data in electronic form containing*  
7 *personal information.*

8           (b) *ADDITIONAL PREEMPTION.—*

9           (1) *IN GENERAL.—No person other than a person*  
10 *specified in section 4(c) may bring a civil action*  
11 *under the laws of any State if such action is premised*  
12 *in whole or in part upon the defendant violating any*  
13 *provision of this Act.*

14           (2) *PROTECTION OF CONSUMER PROTECTION*  
15 *LAWS.—This subsection shall not be construed to limit*  
16 *the enforcement of any State consumer protection law*  
17 *by an Attorney General of a State.*

18           (c) *PROTECTION OF CERTAIN STATE LAWS.—This Act*  
19 *shall not be construed to preempt the applicability of—*

20           (1) *State trespass, contract, or tort law; or*

21           (2) *other State laws to the extent that those laws*  
22 *relate to acts of fraud.*

23           (d) *PRESERVATION OF FTC AUTHORITY.—Nothing in*  
24 *this Act may be construed in any way to limit or affect*

1 *the Commission's authority under any other provision of*  
2 *law.*

3 **SEC. 7. EFFECTIVE DATE.**

4 *This Act shall take effect 1 year after the date of enact-*  
5 *ment of this Act.*

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

7 *There is authorized to be appropriated to the Commis-*  
8 *sion \$1,000,000 for each of fiscal years 2010 through 2015*  
9 *to carry out this Act.*

Amend the title so as to read: “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.”.

Union Calendar No. 214

11<sup>TH</sup> CONGRESS  
1<sup>ST</sup> Session

**H. R. 2221**

[Report No. 111-362]

---

---

## **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.

---

---

DECEMBER 8, 2009

Reported with amendments, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed