

109TH CONGRESS
1ST SESSION

H. R. 4127

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

OCTOBER 25, 2005

Mr. STEARNS (for himself, Ms. PRYCE of Ohio, Mr. UPTON, Mr. RADANOVICH, Mr. BASS, Mrs. BONO, Mr. FERGUSON, and Mrs. BLACKBURN) introduced the following bill; which was referred to the Committee on Energy and Commerce

A BILL

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

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

3 **SECTION 1. SHORT TITLE.**

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

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

2 (a) GENERAL SECURITY POLICIES AND PROCE-
3 DURES.—

4 (1) REGULATIONS.—Not later than 1 year after
5 the date of enactment of this Act, the Commission
6 shall promulgate regulations to require each person
7 engaged in interstate commerce that owns or pos-
8 sesses data in electronic form containing personal in-
9 formation to establish and implement policies and
10 procedures regarding information security practices
11 for the treatment and protection of personal infor-
12 mation that are consistent with—

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

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

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

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

24 (A) A security policy with respect to the
25 collection, use, sale, other dissemination, and
26 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 maintained by such person that contains
8 such electronic data.

9 (D) A process for taking preventive and
10 corrective action to mitigate against any
11 vulnerabilities identified in the process required
12 by subparagraph (C), which may include
13 encryption of such data, implementing any
14 changes to security practices and the architec-
15 ture, installation, or implementation of network
16 or operating software.

17 (b) SPECIAL REQUIREMENTS FOR INFORMATION
18 BROKERS.—

19 (1) SUBMISSION OF POLICIES TO THE FTC.—
20 The regulations promulgated under subsection (a)
21 shall require information brokers to submit their se-
22 curity policies to the Commission on an annual
23 basis.

24 (2) POST-BREACH AUDIT.—Following a breach
25 of security of an information broker, the Commis-

1 sion shall conduct an audit of the information secu-
2 rity practices of such information broker. The Com-
3 mission may conduct additional audits, on an annual
4 basis, for a maximum of 5 years following the
5 breach of security or until the Commission deter-
6 mines that the security practices of the information
7 broker are in compliance with the requirements of
8 this section and are adequate to prevent further
9 breaches of security.

10 (3) INDIVIDUAL ACCESS TO PERSONAL INFOR-
11 MATION.—

12 (A) ACCESS TO INFORMATION.—Each in-
13 formation broker shall—

- 14 (i) provide to each individual whose
15 personal information it maintains, at the
16 individual's request at least one time per
17 year and at no cost to the individual, a
18 means for such individual to review any
19 personal information of the individual
20 maintained by the information broker and
21 any other information about the individual
22 maintained by the information broker; and
23 (ii) place a conspicuous notice on its
24 Internet website (if the information broker
25 maintains such a website) instructing indi-

viduals how to request access to the information required to be provided under clause (i).

(B) **DISPUTED INFORMATION.**—Whenever an individual whose information the information broker maintains files a written request disputing the accuracy of any such information, unless there is reasonable grounds to believe such request is frivolous or irrelevant, the information broker shall clearly note in the database maintained by such information broker, and in any subsequent transmission of such information by such information broker, that such information is disputed by the individual to whom the information relates. Such note shall include either the individual’s statement disputing the accuracy of such information or a clear and concise summary thereof.

SEC. 3. NOTIFICATION OF INFORMATION SECURITY BREACH.

(a) **NATIONWIDE NOTIFICATION.**—Any person engaged in interstate commerce that owns or possesses data in electronic form containing personal information shall, following the discovery of a breach of security of the system maintained by such person that contains such data—

1 (1) notify each individual of the United States
2 whose personal information was acquired by an un-
3 authorized person as a result of such a breach of se-
4 curity;

5 (2) notify the Commission;

6 (3) place a conspicuous notice on the Internet
7 website of the person (if such person maintains such
8 a website), which shall include a telephone number
9 that the individual may use, at no cost to such indi-
10 vidual, to contact the person to inquire about the se-
11 curity breach or the information the person main-
12 tained about that individual; and

13 (4) in the case of a breach of financial account
14 information of a merchant, notify the financial insti-
15 tution that issued the account.

16 (b) TIMELINESS OF NOTIFICATION.—All notifica-
17 tions required under subsection (a) shall be made as
18 promptly as possible and without unreasonable delay fol-
19 lowing the discovery of a breach of security of the system
20 and any measures necessary to determine the scope of the
21 breach, prevent further breach or unauthorized dislo-
22 sures, and reasonably restore the integrity of the data sys-
23 tem.

24 (c) METHOD AND CONTENT OF NOTIFICATION.—

25 (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
7 selected method can reasonably be expected to
8 reach the intended individual):

9 (i) Written notification.

10 (ii) Email notification, if the indi-
11 vidual has consented to receive such notifi-
12 cation and the notification is provided in a
13 manner that is consistent with the provi-
14 sions permitting electronic transmission of
15 notices under section 101 of the Electronic
16 Signatures in Global Commerce Act (15
17 U.S.C. 7001).

18 (B) CONTENT OF NOTIFICATION.—Regard-
19 less of the method by which notification is pro-
20 vided to an individual under subparagraph (A),
21 such notification shall include—

22 (i) a description of the personal infor-
23 mation that was acquired by an unauthor-
24 ized person;

1 (ii) a telephone number that the indi-
2 vidual may use, at no cost to such indi-
3 vidual, to contact the person to inquire
4 about the security breach or the informa-
5 tion the person maintained about that indi-
6 vidual;

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

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

14 (2) SUBSTITUTE NOTIFICATION.—

15 (A) CIRCUMSTANCES GIVING RISE TO SUB-
16 STITUTE NOTIFICATION.—A person required to
17 provide notification to individuals under sub-
18 section (a)(1) may provide substitute notifica-
19 tion in lieu of the direct notification required by
20 paragraph (1) if such direct notification is not
21 feasible due to—

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

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

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

6 (B) CONTENT OF SUBSTITUTE NOTIFICA-
7 TION.—Such substitute notification shall in-
8 clude notification in print and broadcast media,
9 including major media in metropolitan and
10 rural areas where the individuals whose per-
11 sonal information was acquired reside. Such no-
12 tification shall include a telephone number
13 where an individual can, at no cost to such indi-
14 vidual, learn whether or not that individual's
15 personal information is included in the security
16 breach.

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

19 (A) REGULATIONS.—Not later than 270
20 days after the date of enactment of this Act,
21 the Commission shall, by regulation, establish
22 criteria for determining the circumstances
23 under which substitute notification may be pro-
24 vided under paragraph (2), including criteria
25 for determining if notification under paragraph

1 (1) is not feasible due to excessive cost to the
2 person required to provide such notification rel-
3 ative to the resources of such person.

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

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

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

16 (d) OTHER OBLIGATIONS FOLLOWING BREACH.—A
17 person required to provide notification under subsection
18 (a) shall provide or arrange for the provision of, to each
19 individual to whom notification is provided under sub-
20 section (c)(1) and at no cost to such individual, consumer
21 credit reports from at least one of the major credit report-
22 ing agencies beginning not later than 2 months following
23 a breach of security and continuing on a quarterly basis
24 for a period of 2 years thereafter. The Commission shall,
25 by regulation, provide alternative requirements under this

1 subsection for persons who qualify to provide substitute
2 notification under subsection (c)(2).

3 (e) WEBSITE NOTICE OF FEDERAL TRADE COMMIS-
4 SION.—The Commission shall place, in a clear and con-
5 spicuous location on its Internet website, a notice of any
6 breach of security that is reported to the Commission
7 under subsection (a)(2).

8 **SEC. 4. ENFORCEMENT BY THE FEDERAL TRADE COMMIS-**
9 **SION.**

10 (a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—
11 A violation of section 2 or 3 shall be treated as a violation
12 of a regulation under section 18(a)(1)(B) of the Federal
13 Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regard-
14 ing unfair or deceptive acts or practices.

15 (b) POWERS OF COMMISSION.—The Commission
16 shall enforce this Act in the same manner, by the same
17 means, and with the same jurisdiction, powers, and duties
18 as though all applicable terms and provisions of the Fed-
19 eral Trade Commission Act (15 U.S.C. 41 et seq.) were
20 incorporated into and made a part of this Act. Any person
21 who violates such regulations shall be subject to the pen-
22 alties and entitled to the privileges and immunities pro-
23 vided in that Act. Nothing in this Act shall be construed
24 to limit the authority of the Commission under any other
25 provision of law.

1 **SEC. 5. DEFINITIONS.**

2 In this Act the following definitions apply:

3 (1) **BREACH OF SECURITY.**—The term “breach
4 of security” means the unauthorized acquisition of
5 data in electronic form containing personal informa-
6 tion that establishes a reasonable basis to conclude
7 that there is a significant risk of identity theft to the
8 individual to whom the personal information relates.
9 The encryption of such data, combined with appro-
10 priate safeguards of the keys necessary to enable
11 decryption of such data, shall establish a presump-
12 tion that no such reasonable basis exists. Any such
13 presumption may be rebutted by facts demonstrating
14 that the method of encryption has been or is likely
15 to be compromised.

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

18 (3) **DATA IN ELECTRONIC FORM.**—The term
19 “data in electronic form” means any data stored
20 electronically or digitally on any computer system or
21 other database and includes recordable tapes and
22 other mass storage devices.

23 (4) **ENCRYPTION.**—The term “encryption”
24 means the protection of data in electronic form in
25 storage or in transit using an encryption algorithm
26 implemented within a validated cryptographic mod-

1 ule that has been approved by the National Institute
2 of Standards and Technology or another comparable
3 standards body recognized by the Commission, ren-
4 dering such data indecipherable in the absence of as-
5 sociated cryptographic keys necessary to enable
6 decryption of such data. Such encryption must in-
7 clude appropriate management and safeguards of
8 such keys to protect the integrity of the encryption.

9 (5) IDENTITY THEFT.—The term “identity
10 theft” means the unauthorized assumption of an-
11 other person’s identity for the purpose of engaging
12 in commercial transactions under the name of such
13 other person.

14 (6) INFORMATION BROKER.—The term “infor-
15 mation broker” means a commercial entity whose
16 business is to collect, assemble, or maintain personal
17 information concerning individuals who are not cus-
18 tomers of such entity for the sale or transmission of
19 such information or the provision of access to such
20 information to any third party, whether such collec-
21 tion, assembly, or maintenance of personal informa-
22 tion is performed by the information broker directly,
23 or by contract or subcontract with any other entity.

24 (7) PERSONAL INFORMATION.—

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

5 (i) Social Security number.

6 (ii) Driver’s license number or other
7 State identification number.

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

13 (B) MODIFIED DEFINITION BY RULE-
14 MAKING.—The Commission may, by rule, mod-
15 ify the definition of “personal information”
16 under subparagraph (A) to the extent that such
17 modification is necessary to accommodate
18 changes in technology or practices, will not un-
19 reasonably impede interstate commerce, and
20 will accomplish the purposes of this Act.

21 (8) PERSON.—The term “person” has the same
22 meaning given such term in section 551(2) of title
23 5, United States Code.

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

2 (a) PREEMPTION OF STATE INFORMATION SECURITY
3 LAWS.—This Act supersedes any provision of a statute,
4 regulation, or rule of a State or political subdivision of
5 a State that expressly—

6 (1) requires information security practices and
7 treatment of personal information similar to any of
8 those required under section 2; and

9 (2) requires notification to individuals of a
10 breach of security resulting in unauthorized acquisi-
11 tion of their personal information.

12 (b) ADDITIONAL PREEMPTION.—

13 (1) IN GENERAL.—No person other than the
14 Attorney General of a State may bring a civil action
15 under the laws of any State if such action is pre-
16 mised in whole or in part upon the defendant vio-
17 lating any provision of this Act.

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

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

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

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

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

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

6 (b) SUNSET.—This Act shall cease to be in effect on
7 the date that is 10 years from the date of enactment of
8 this Act.

9 **SEC. 8. AUTHORIZATION OF APPROPRIATIONS.**

10 There is authorized to be appropriated to the Com-
11 mission \$1,000,000 for each of fiscal years 2006 through
12 2010 to carry out this Act.

○