

[STAFF DISCUSSION DRAFT]

109TH CONGRESS
1ST SESSION

H. R. _____

To require persons engaged in interstate commerce and in possession of electronic data containing personal information to establish comprehensive policies and procedures to prevent unauthorized acquisition of such information and to notify individuals of any such unauthorized acquisition.

IN THE HOUSE OF REPRESENTATIVES

M. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To require persons engaged in interstate commerce and in possession of electronic data containing personal information to establish comprehensive policies and procedures to prevent unauthorized acquisition of such information and to notify individuals of any such unauthorized acquisition.

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 "[*To be provided*]".



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

2 (a) REQUIRED SECURITY POLICIES AND PROCE-
3 DURES.—Not later than 180 days after the date of enact-
4 ment of this Act, the Commission shall promulgate regula-
5 tions to require each person engaged in interstate com-
6 merce that owns or possesses data in electronic form con-
7 taining personal information to establish and implement
8 policies and procedures regarding information security
9 practices and treatment of personal information. Such reg-
10 ulations shall require such policies and procedures to in-
11 clude the following:

12 (1) A security policy and statement with respect
13 to the collection, use, sale, other dissemination, and
14 security of such personal information. Such policy
15 and statement shall include the following:

16 (A) [*To be provided*]

17 (2) The identification of an officer as the point
18 of contact with responsibility for information secu-
19 rity issues.

20 (3) A process for taking preventive and correc-
21 tive action to mitigate against any vulnerability iden-
22 tified in the system maintained by such person that
23 contains such electronic data, including encryption,
24 implementing any changes to its security practices
25 and the architecture, installation, or implementation
26 of its network or operating software.



1 (b) SPECIAL REQUIREMENTS FOR INFORMATION
2 BROKERS.—

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

4 (A) ANNUAL SUBMISSION.—The rules pro-
5 mulgated under subsection (a) shall require in-
6 formation brokers to submit their security poli-
7 cies to the Commission on an annual basis.

8 (B) AUDIT.—The Commission shall con-
9 duct, on an annual basis, an audit of the secu-
10 rity policies and procedures of each information
11 broker required to submit a security policy
12 under subparagraph (A).

13 (2) INDIVIDUAL ACCESS TO PERSONAL INFOR-
14 MATION.—Each information broker shall—

15 (A) provide to each individual whose per-
16 sonal information it maintains, at the individ-
17 ual's request at least one time per year and at
18 no cost to the individual, a means for such indi-
19 vidual to review any personal information of the
20 individual maintained by the information broker
21 and any other information about the individual
22 maintained by the information broker; and

23 (B) place a conspicuous notice on its Inter-
24 net website (if the information broker maintains
25 such a website) instructing individuals how to



1 request access to the information required to be
2 provided under subparagraph (A).

3 **SEC. 3. NOTIFICATION OF DATABASE SECURITY BREACH.**

4 (a) **NATIONWIDE NOTIFICATION.**—Any person en-
5 gaged in interstate commerce that owns or possesses data
6 in electronic form containing personal information shall,
7 following the discovery of a breach of security of the sys-
8 tem maintained by such person that contains such data,
9 notify—

10 (1) any individual of the United States whose
11 personal information was, or is reasonably believed
12 to have been, acquired by an unauthorized person as
13 a result of such a breach of security;

14 (2) the Commission; and

15 (3) in the case of breach of financial account
16 information by a merchant, the financial institution
17 that issued the account.

18 (b) **BREACH OF SECURITY.**—The Commission shall,
19 by rule, define the term “breach of security” for purposes
20 of this section, including the conditions and circumstances
21 constituting such a breach of security. At minimum, such
22 term shall mean the compromise of the security, confiden-
23 tiality, or integrity of data that results in, or there is a
24 reasonable basis to conclude has resulted in, the acquisi-



1 tion of personal information by an unauthorized person
2 that may result in identity theft.

3 (c) TIMELINESS OF NOTIFICATION.—All notifications
4 required under subsection (a) shall be made as promptly
5 as possible and without unreasonable delay following the
6 discovery of a breach of security of the system and any
7 measures necessary to determine the scope of the breach,
8 prevent further breach or unauthorized disclosures, and
9 reasonably restore the integrity of the data system.

10 (d) METHOD AND CONTENT OF NOTIFICATION.—Not
11 later than 180 days after the date of enactment of this
12 Act, the Commission shall, by rule, prescribe the method
13 and content of the notification required under this section,
14 including, at minimum, the following requirements:

15 (1) IN GENERAL.—

16 (A) METHOD OF NOTICE.—A person re-
17 quired to provide notification under subsection
18 (a) shall be in compliance with this section if
19 the person—

20 (i) provides the individual whose per-
21 sonal information was, or is reasonably be-
22 lieved to have been, acquired by an unau-
23 thorized person with—

24 (I) written notification; and



1 (II) email notification, if the per-
2 son has an email address for the indi-
3 vidual and if the individual has con-
4 sented to receive such email notifica-
5 tion; and

6 (ii) places a conspicuous notice on the
7 Internet website of the person, if such per-
8 son maintains an Internet website.

9 (B) CONTENT OF NOTIFICATION.—Such
10 notice shall include—

11 (i) a description of the categories of
12 personal information that was, or is rea-
13 sonably believed to have been, acquired by
14 an unauthorized person, including Social
15 Security numbers, driver's license or State
16 identification numbers, and financial data;

17 (ii) a telephone number that the indi-
18 vidual may use, at no cost to such indi-
19 vidual, to contact the person to inquire
20 about the security breach or the informa-
21 tion the person maintained about that indi-
22 vidual;

23 (iii) the toll-free contact telephone
24 numbers and addresses for—



1 (I) the major credit reporting
2 agencies; and

3 (II) credit repair services; and
4 (iv) a toll-free telephone number and
5 Internet website address for the Commis-
6 sion whereby the individual may obtain in-
7 formation regarding identity theft.

8 (2) SUBSTITUTE NOTICE.—The Commission
9 shall establish criteria for the provision of substitute
10 notice under this section, including the cir-
11 cumstances under which such substitute notice may
12 be provided in lieu of the notification required under
13 paragraph (1).

14 (A) CIRCUMSTANCES GIVING RISE TO SUB-
15 STITUTE NOTICE.—Such criteria may include
16 circumstances under which notification under
17 paragraph (1) is not feasible due to—

18 (i) excessive cost to the person re-
19 quired to provide such notification relative
20 to the resources of such person; or

21 (ii) lack of sufficient contact informa-
22 tion for the individuals required to be noti-
23 fied.



1 (B) CONTENT OF SUBSTITUTE NOTICE.—

2 Such criteria shall require that substitute notice
3 include—

4 (i) notification to major print and
5 broadcast media, including major media in
6 metropolitan and rural areas where the in-
7 dividuals whose personal information was,
8 or may have been, acquired resides; and

9 (ii) a conspicuous notice on the Inter-
10 net website of the person, if such person
11 maintains an Internet website.

12 Such notification to media and notice on the
13 website shall include a phone number where an
14 individual can, at no cost to such individual,
15 learn whether or not that individual's personal
16 information is included in the security breach.

17 (e) OTHER OBLIGATIONS FOLLOWING BREACH.—A
18 person required to provide notification under subsection
19 (a) shall provide or arrange for the provision of, to each
20 individual to whom notification is required under such
21 subsection and at no cost to such individual—

22 (1) an individual consumer credit report from
23 each of the major credit reporting agencies; and

24 (2) a 1-year subscription to a credit monitoring
25 service.



1 **SEC. 4. ENFORCEMENT BY THE FEDERAL TRADE COMMIS-**
2 **SION.**

3 (a) **UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—**
4 A violation of section 3 or 4 shall be treated as a violation
5 of a regulation under section 18(a)(1)(B) of the Federal
6 Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regard-
7 ing unfair or deceptive acts or practices.

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

19 **SEC. 5. DEFINITIONS.**

20 In this Act the following definitions apply:

21 (1) **COMMISSION.—**The term “Commission”
22 means the Federal Trade Commission.

23 (2) **DATA IN ELECTRONIC FORM.—**The term
24 “data in electronic form” means any data stored
25 electronically or digitally on any computer system or



1 other database and includes recordable tapes and
2 other mass storage devices.

3 (3) IDENTITY THEFT.—The term “identity
4 theft” means the unauthorized assumption of an-
5 other person’s identity for the purpose of engaging
6 in commercial transactions under the name of such
7 other person.

8 (4) INFORMATION BROKER.—The term “infor-
9 mation broker” means a commercial entity whose
10 business is to collect, assemble, or maintain personal
11 information for the sale or transmission of such in-
12 formation or the provision of access to such informa-
13 tion to any third party, whether such collection, as-
14 sembly, or maintenance of personal information is
15 performed by the information broker directly, or by
16 contract or subcontract with any other entity.

17 (5) PERSONAL INFORMATION.—

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

22 (i) Social Security account number.

23 (ii) Driver’s license number or other
24 State identification number.



1 (iii) Financial account number, or
2 credit or debit card number, in combina-
3 tion with any required security code, access
4 code, or password that would permit access
5 to an individual's financial account.

6 (B) MODIFIED DEFINITION BY RULE-
7 MAKING.—The Commission may, by rule, mod-
8 ify the definition of “personal information”
9 under subparagraph (A).

10 (6) PERSON.—The term “person” has the same
11 meaning given such term in section 551(2) of title
12 5, United States Code.

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

14 This Act supersedes any provision of a statute, regu-
15 lation, or rule of a State or political subdivision of a State
16 that expressly—

17 (1) regulates breaches of security of data in
18 electronic form that result in unauthorized acquisi-
19 tion of personal information; or

20 (2) requires notification to individuals of such a
21 breach of security or unauthorized acquisition of
22 personal information.

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

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



1 (b) SUNSET.—This Act shall not apply after the date
2 that is 10 years from the date of enactment of this Act.

3 **SEC. 8. AUTHORIZATION OF APPROPRIATIONS.**

4 There is authorized to be appropriated to the Com-
5 mission [\$_____] for fiscal years
6 [_____] to carry out this Act.

