[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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "**[***To be provided***]**".

SEC. 2. REQUIREMENTS FOR INFORMATION SECURITY.

(a) REQUIRED SECURITY POLICIES AND PROCEDURES.—Not later than 180 days after the date of enactment of this Act, the Commission shall promulgate regulations to require each person engaged in interstate commerce that owns or possesses data in electronic form containing personal information to establish and implement policies and procedures regarding information security practices and treatment of personal information. Such regulations shall require such policies and procedures to include the following:

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

(A) **[***To be provided***]**

(2) The identification of an officer as the point of contact with responsibility for information security issues.

(3) A process for taking preventive and corrective action to mitigate against any vulnerability identified in the system maintained by such person that contains such electronic data, including encryption, implementing any changes to its security practices and the architecture, installation, or implementation of its network or operating software.

(b) SPECIAL REQUIREMENTS FOR INFORMATION BROKERS.—

(1) SUBMISSION OF POLICIES TO THE FTC.—

(A) ANNUAL SUBMISSION.—The rules promulgated under subsection (a) shall require information brokers to submit their security policies to the Commission on an annual basis.

(B) AUDIT.—The Commission shall conduct, on an annual basis, an audit of the security policies and procedures of each information broker required to submit a security policy under subparagraph (A).

(2) INDIVIDUAL ACCESS TO PERSONAL INFORMATION.—Each information broker shall—

(A) provide to each individual whose personal information it maintains, at the individual's request at least one time per year and at no cost to the individual, a means for such individual to review any personal information of the individual maintained by the information broker and any other information about the individual maintained by the information broker; and

(B) place a conspicuous notice on its Internet website (if the information broker maintains such a website) instructing individuals how to

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

SEC. 3. NOTIFICATION OF DATABASE 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, notify—

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

(2) the Commission; and

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

(b) BREACH OF SECURITY.—The Commission shall, by rule, define the term ''breach of security'' for purposes of this section, including the conditions and circumstances constituting such a breach of security. At minimum, such term shall mean the compromise of the security, confidentiality, or integrity of data that results in, or there is a reasonable basis to conclude has resulted in, the acquisi-

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

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

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

(1) IN GENERAL.—

(A) METHOD OF NOTICE.—A person required to provide notification under subsection (a) shall be in compliance with this section if the person—

(i) provides the individual whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person with—

(I) written notification; and

(II) email notification, if the person has an email address for the individual and if the individual has consented to receive such email notification; and

(ii) places a conspicuous notice on the Internet website of the person, if such person maintains an Internet website.

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

(i) a description of the categories of personal information that was, or is reasonably believed to have been, acquired by an unauthorized person, including Social Security numbers, driver's license or State identification numbers, and financial data;

(ii) a telephone number that the individual may use, at no cost to such individual, to contact the person to inquire about the security breach or the information the person maintained about that individual;

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

(I) the major credit reporting agencies; and

(II) credit repair services; and

(iv) a toll-free telephone number and Internet website address for the Commission whereby the individual may obtain information regarding identity theft.

(2) SUBSTITUTE NOTICE.—The Commission shall establish criteria for the provision of substitute notice under this section, including the circumstances under which such substitute notice may be provided in lieu of the notification required under paragraph (1).

(A) CIRCUMSTANCES GIVING RISE TO SUBSTITUTE NOTICE.—Such criteria may include circumstances under which notification under paragraph (1) is not feasible due to—

(i) excessive cost to the person required to provide such notification relative to the resources of such person; or

(ii) lack of sufficient contact information for the individuals required to be notified.

(B) CONTENT OF SUBSTITUTE NOTICE.—Such criteria shall require that substitute notice include—

(i) notification to major print and broadcast media, including major media in metropolitan and rural areas where the individuals whose personal information was, or may have been, acquired resides; and

(ii) a conspicuous notice on the Internet website of the person, if such person maintains an Internet website.

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

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

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

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

SEC. 4. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

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

(b) POWERS OF COMMISSION.—The Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any person who violates such regulations shall be subject to the penalties and entitled to the privileges and immunities provided in that Act. Nothing in this Act shall be construed to limit the authority of the Commission under any other provision of law.

SEC. 5. DEFINITIONS.

In this Act the following definitions apply:

(1) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(2) DATA IN ELECTRONIC FORM.—The term ''data in electronic form'' means any data stored electronically or digitally on any computer system or

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

(3) IDENTITY THEFT.—The term ''identity theft'' means the unauthorized assumption of another person's identity for the purpose of engaging in commercial transactions under the name of such other person.

(4) INFORMATION BROKER.—The term ''information broker'' means a commercial entity whose business is to collect, assemble, or maintain personal information for the sale or transmission of such information or the provision of access to such information to any third party, whether such collection, assembly, or maintenance of personal information is performed by the information broker directly, or by contract or subcontract with any other entity.

(5) PERSONAL INFORMATION.—

(A) DEFINITION.—The term ''personal information'' means an individual's first and last name in combination with any 1 or more of the following data elements for that individual:

(i) Social Security account number.

(ii) Driver's license number or other State identification number.

(iii) Financial account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(B) MODIFIED DEFINITION BY RULEMAKING.—The Commission may, by rule, modify the definition of ''personal information'' under subparagraph (A).

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

SEC. 6. EFFECT ON OTHER LAWS.

This Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State that expressly—

(1) regulates breaches of security of data in electronic form that result in unauthorized acquisition of personal information; or

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

SEC. 7. EFFECTIVE DATE AND SUNSET.

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

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

SEC. 8. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated to the Commission **[**$_____**]** for fiscal years **[**_____**]** to carry out this Act.