AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

109TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 109–453
Part 2

DATA ACCOUNTABILITY AND TRUST ACT (DATA)

MAY 26, 2006.—Ordered to be printed

Mr. SENSENBRENNER, from the Committee on the Judiciary submitted the following

R E P O R T

[To accompany H.R. 4127]

[Including Committee on the Judiciary cost estimate]

The Committee on the Judiciary, to whom was referred the bill (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 security breach, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

	Page
The Amendment	1
Purpose and Summary	9
Background and Need for Legislation	10
Hearings	11
Committee Consideration	12
Vote of the Committee	12
Committee Oversight Findings	12
New Budget Authority and Tax Expenditures	12
Committee Cost Estimate	12
Performance Goals and Objectives	13
Constitutional Authority Statement	13
Section-by-Section Analysis and Discussion	13

THE AMENDMENT

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Data Accountability and Trust Act (DATA)".

SEC. 2. REQUIREMENTS FOR INFORMATION SECURITY.

(a) GENERAL SECURITY POLICIES AND PROCEDURES.—

(1) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to require each person engaged in interstate commerce that owns or possesses data in electronic form containing personal information, or contracts to have any third party entity maintain such data for such person, to establish and implement policies and procedures regarding information security practices for the treatment and protection of personal informtion taking into consideration—

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

(B) the current state of the art in administrative, technical, and physical safeguards for protecting such information; and

(C) the cost of implementing such safeguards.

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

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

(B) The identification of an officer or other individual as the point of contact with responsibility for the management of information security.

(C) A process for identifying and assessing any reasonably foreseeable vulnerabilities in the system maintained by such person that contains such electronic data, which shall include regular monitoring for a breach of security of such system.

(D) A process for taking preventive and corrective action to mitigate against any vulnerabilities identified in the process required by subparagraph (C), which may include implementing any changes to security practices and the architecture, installation, or implementation of network or operating software.

(E) A process for disposing of obsolete data in electronic form containing personal information by shredding, permanently erasing, or otherwise modifying the personal information contained in such data to make such personal information permanently unreadable or undecipherable.

(3) TREATMENT OF ENTITIES GOVERNED BY OTHER LAW.—In promulgating the regulations under this subsection, the Commission may determine to be in compliance with this subsection any person who is required under any other Federal law to maintain standards and safeguards for information security and protection of personal information that provide equal or greater protection than those required under this subsection.

(b) DESTRUCTION OF OBSOLETE PAPER RECORDS CONTAINING PERSONAL INFORMATION.—

(1) STUDY.—Not later than 1 year after the date of enactment of this Act, the Commission shall conduct a study on the practicality of requiring a standard method or methods for the destruction of obsolete paper documents and other non-electronic data containing personal information by persons engaged in interstate commerce who own or possess such paper documents and non-electronic data. The study shall consider the cost, benefit, feasibility, and effect of a requirement of shredding or other permanent destruction of such paper documents and non-electronic data.

(2) REGULATIONS.—The Commission may promulgate regulations under section 553 of title 5, United States Code, requiring a standard method or methods for the destruction of obsolete paper documents and other non-electronic data containing personal information by persons engaged in interstate commerce who own or possess such paper documents and non-electronic data if the Commission finds that—

(A) the improper disposal of obsolete paper documents and other non-electronic data creates a reasonable risk of identity theft, fraud, or other unlawful conduct;

(B) such a requirement would be effective in preventing identity theft, fraud, or other unlawful conduct;

(C) the benefit in preventing identity theft, fraud, or other unlawful conduct would outweigh the cost to persons subject to such a requirement; and

(D) compliance with such a requirement would be practicable.

In enforcing any such regulations, the Commission may determine to be in compliance with such regulations any person who is required under any other Federal law to dispose of obsolete paper documents and other non-electronic data containing personal information if such other Federal law provides equal or greater protection or personal information than the regulations promulgated under this subsection.

(c) SPECIAL REQUIREMENTS FOR INFORMATION BROKERS.—

(1) SUBMISSION OF POLICIES TO THE FTC.—The regulations promulgated under subsection (a) shall require information brokers to submit their security policies to the Commission in conjunction with a notification of a breach of security under section 3 or upon request of the Commission.

(2) POST-BREACH AUDIT.—For any information broker required to provide notification under section 3, the Commission shall conduct an audit of the information security practices of such information broker, or require the information broker to conduct an independent audit of such practices (by an independent auditor who has not audited such information broker's security practices during the preceding 5 years). The Commission may conduct or require additional audits for a period of 5 years following the breach of security or until the Commission determines that the security practices of the information broker are in compliance with the requirements of this section and are adequate to prevent further breaches of security.

(3) VERIFICATION OF AND INDIVIDUAL ACCESS TO PERSONAL INFORMATION.—

(A) VERIFICATION.—Each information broker shall establish reasonable procedures to verify the accuracy of the personal information it collects, assembles, or maintains, and any other information it collects, assembles, or maintains that specifically identifies an individual, other than information which merely identifies an individual's name or address.

(B) CONSUMER ACCESS TO INFORMATION.—

(i) ACCESS.—Each information broker shall—

(I) provide to each individual whose personal information it maintains, at the individual's request at least 1 time per year and at no cost to the individual, and after verifying the identity of such individual, a means for the individual to review any personal information regarding such individual maintained by the information broker and any other information maintained by the information broker that specifically identifies such individual, other than information which merely identifies an individual's name or address; and

(II) 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 subclause (I).

(ii) DISPUTED INFORMATION.—Whenever an individual whose information the information broker maintains makes a written request disputing the accuracy of any such information, the information broker, after verifying the identity of the individual making such request and unless there are reasonable grounds to believe such request is frivolous or irrelevant, shall—

(I) correct any inaccuracy; or

(II)(aa) in the case of information that is public record information, inform the individual of the source of the information, and, if reasonably available, where a request for correction may be directed; or

(bb) in the case of information that is non-public information, note the information that is disputed, including the individual's statement disputing such information, and take reasonable steps to independently verify such information under the procedures outlined in subparagraph (A) if such information can be independently verified.

(iii) LIMITATIONS.—An information broker may limit the access to information required under subparagraph (B) in the following circumstances:

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

(II) If the information is used for a legitimate governmental or fraud prevention purpose that would be compromised by such access.

(iv) RULEMAKING.—The Commission shall issue regulations, as necessary, under section 553 of title 5, United States Code, on the application of the limitations in clause (iii).

(C) TREATMENT OF ENTITIES GOVERNED BY OTHER LAW.—The Commission may promulgate rules (under section 553 of title 5, United States Code) to determine to be in compliance with this paragraph any person who is a consumer reporting agency, as defined in section 603(f) of the Fair Credit Reporting Act, with respect to those products and services that are subject to and in compliance with the requirements of that Act.

(4) REQUIREMENT OF AUDIT LOG OF ACCESSED AND TRANSMITTED INFORMATION.—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to require information brokers to establish measures which facilitate the auditing or retracing of any internal or external access to, or transmissions of, any data in electronic form containing personal information collected, assembled, or maintained by such information broker.

(5) PROHIBITION ON PRETEXTING BY INFORMATION BROKERS.—

(A) PROHIBITION ON OBTAINING PERSONAL INFORMATION BY FALSE PRETENSES.—It shall be unlawful for an information broker to obtain or attempt to obtain, or cause to be disclosed or attempt to cause to be disclosed to any person, personal information or any other information relating to any person by—

(i) making a false, fictitious, or fraudulent statement or representation to any person; or

(ii) providing any document or other information to any person that the information broker knows or should know to be forged, counterfeit, lost, stolen, or fraudulently obtained, or to contain a false, fictitious, or fraudulent statement or representation.

(B) PROHIBITION ON SOLICITATION TO OBTAIN PERSONAL INFORMATION UNDER FALSE PRETENSES.—It shall be unlawful for an information broker to request a person to obtain personal information or any other information relating to any other person, if the information broker knew or should have known that the person to whom such a request is made will obtain or attempt to obtain such information in the manner described in subsection (a).

(d) EXEMPTION FOR TELECOMMUNICATIONS CARRIER, CABLE OPERATOR, INFORMATION SERVICE, OR INTERACTIVE COMPUTER SERVICE.—Nothing in this section shall apply to any electronic communication by a third party stored by a telecommunications carrier, cable operator, or information service, as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153), or an interactive computer service, as such term is defined in section 230(f)(2) of such Act (47 U.S.C. 230(f)(2)).

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) notify each individual who is a citizen or resident of the United States whose personal information was acquired by an unauthorized person as a result of such a breach of security; and

(2) notify the Commission.

(b) SPECIAL NOTIFICATION REQUIREMENT FOR CERTAIN ENTITIES.—

(1) THIRD PARTY AGENTS.—In the event of a breach of security by any third party entity that has been contracted to maintain or process data in electronic form containing personal information on behalf of any other person who owns or possesses such data, such third party entity shall be required only to notify such person of the breach of security. Upon receiving such notification from such third party, such person shall provide the notification required under subsection (a).

(2) TELECOMMUNICATIONS CARRIERS, CABLE OPERATORS, INFORMATION SERVICES, AND INTERACTIVE COMPUTER SERVICES.—If a telecommunications carrier, cable operator, or information service (as such terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153)), or an interactive computer service (as such term is defined in section 230(f)(2) of such Act (47 U.S.C. 230(f)(2))), becomes aware of a breach of security during the transmission of data in electronic form containing personal information that is owned or possessed by another person utilizing the means of transmission of such telecommunications carrier, cable operator, information service, or interactive computer service, such telecommunications carrier, cable operator, information service, or interactive computer service shall be required only to notify the person who initiated such transmission of such a breach of security if such person can be reasonably identified. Upon receiving such notification from a telecommunications carrier, cable operator, information service, or interactive computer service, such person shall provide the notification required under subsection (a).

(3) BREACH OF HEALTH INFORMATION.—If the Commission receives a notification of a breach of security and determines that information included in such breach is individually identifiable health information (as such term is defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), the Commis-

sion shall send a copy of such notification to the Secretary of Health and Human Services.

(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 consistent with 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.—

(1) DIRECT NOTIFICATION.—

(A) METHOD OF NOTIFICATION.—A person required to provide notification to individuals under subsection (a)(1) shall be in compliance with such requirement if the person provides conspicuous and clearly identified notification by one of the following methods (provided the selected method can reasonably be expected to reach the intended individual):

(i) Written notification.

(ii) Email notification, if—

(I) the person's primary method of communication with the individual is by email; or

(II) the individual has consented to receive such notification and the notification is provided in a manner that is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global Commerce Act (15 U.S.C. 7001).

(B) CONTENT OF NOTIFICATION.—Regardless of the method by which notification is provided to an individual under subparagraph (A), such notification shall include—

(i) a description of the personal information that was acquired by an unauthorized person;

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

(iii) notice that the individual is entitled to receive, at no cost to such individual, consumer credit reports on a quarterly basis for a period of 2 years, and instructions to the individual on requesting such reports from the person;

(iv) the toll-free contact telephone numbers and addresses for the major credit reporting agencies; and

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

(2) SUBSTITUTE NOTIFICATION.—

(A) CIRCUMSTANCES GIVING RISE TO SUBSTITUTE NOTIFICATION.—A person required to provide notification to individuals under subsection (a)(1) may provide substitute notification in lieu of the direct notification required by paragraph (1) if—

(i) the person owns or possesses data in electronic form containing personal information of fewer than 1,000 individuals; and

(ii) such direct notification is not feasible due to—

(I) excessive cost to the person required to provide such notification relative to the resources of such person, as determined in accordance with the regulations issued by the Commission under paragraph (3)(A); or

(II) lack of sufficient contact information for the individual required to be notified.

(B) FORM OF SUBSTITUTE NOTICE.—Such substitute notification shall include—

(i) email notification to the extent that the person has email addresses of individuals to whom it is required to provide notification under subsection (a)(1);

(ii) a conspicuous notice on the Internet website of the person (if such person maintains such a website); and

(iii) notification in print and to broadcast media, including major media in metropolitan and rural areas where the individuals whose personal information was acquired reside.

(C) CONTENT OF SUBSTITUTE NOTICE.—Each form of substitute notice under this paragraph shall include—

(i) notice that individuals whose personal information is included in the breach of security are entitled to receive, at no cost to the individ-

uals, consumer credit reports on a quarterly basis for a period of 2 years, and instructions on requesting such reports from the person; and

(ii) a telephone number by which an individual can, at no cost to such individual, learn whether that individual's personal information is included in the breach of security.

(3) FEDERAL TRADE COMMISSION REGULATIONS AND GUIDANCE.—

(A) REGULATIONS.—Not later than 1year after the date of enactment of this Act, the Commission shall, by regulations under section 553 of title 5, United States Code, establish criteria for determining the circumstances under which substitute notification may be provided under paragraph (2), including criteria for determining if notification under paragraph (1) is not feasible due to excessive cost to the person required to provide such notification relative to the resources of such person.

(B) GUIDANCE.—In addition, the Commission shall provide and publish general guidance with respect to compliance with this section. Such guidance shall include—

(i) a description of written or email notification that complies with the requirements of paragraph (1); and

(ii) guidance on the content of substitute notification under paragraph (2)(B), including the extent of notification to print and broadcast media that complies with the requirements of such paragraph.

(e) OTHER OBLIGATIONS FOLLOWING BREACH.—A person required to provide notification under subsection (a) shall, upon request of an individual whose personal information was included in the breach of security, provide or arrange for the provision of, to each such individual and at no cost to such individual, consumer credit reports from at least one of the major credit reporting agencies beginning not later than 2 months following the discovery of a breach of security and continuing on a quarterly basis for a period of 2 years thereafter.

(f) EXEMPTION.—

(1) GENERAL EXEMPTION.—A person shall be exempt from the requirements under this section if, following a breach of security, such person determines that there is no reasonable risk of identity theft, fraud, or other unlawful conduct.

(2) PRESUMPTIONS.—

(A) ENCRYPTION.—The encryption of data in electronic form shall establish a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security of such data. Any such presumption may be rebutted by facts demonstrating that the encryption has been or is reasonably likely to be compromised.

(B) ADDITIONAL METHODOLOGIES OR TECHNOLOGIES.—Not later than 270 days after the date of the enactment of this Act, the Commission shall, by rule pursuant to section 553 of title 5, United States Code, identify any additional security methodology or technology, other than encryption, which renders data in electronic form unreadable or indecipherable, that shall, if applied to such data, establish a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security of such data. Any such presumption may be rebutted by facts demonstrating that any such methodology or technology has been or is reasonably likely to be compromised. In promulgating such a rule, the Commission shall consult with relevant industries, consumer organizations, and data security and identity theft prevention experts and established standards setting bodies.

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

(g) WEBSITE NOTICE OF FEDERAL TRADE COMMISSION.—If the Commission, upon receiving notification of any breach of security that is reported to the Commission under subsection (a)(2), finds that notification of such a breach of security via the Commission's Internet website would be in the public interest or for the protection of consumers, the Commission shall place such a notice in a clear and conspicuous location on its Internet website.

(h) FTC STUDY ON NOTIFICATION IN LANGUAGES IN ADDITION TO ENGLISH.—Not later than 1 year after the date of enactment of this Act, the Commission shall conduct a study on the practicality and cost effectiveness of requiring the notification required by subsection (d)(1) to be provided in a language in addition to English to individuals known to speak only such other language.

(i) SPECIAL NOTIFICATION REQUIREMENT FOR FEDERAL AGENCIES.—

(1) NATIONWIDE NOTIFICATION.—Any Federal agency 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 agency that con-

tains such data, notify each individual who is a citizen or resident of the United States whose personal information was acquired by an unauthorized person as a result of such a breach of security

(2) METHOD AND CONTENT OF NOTIFICATION.—

(A) METHOD OF NOTIFICATION.—A Federal agency required to provide written notification to individuals under paragraph (1) shall be in compliance with such requirement if the agency provides conspicuous and clearly identified written notification that includes the content required under subparagraph (B).

(B) CONTENT OF NOTIFICATION.—Notification required under this subsection shall include—

(i) a description of the personal information that was acquired by an unauthorized person;

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

(iii) the toll-free contact telephone number and addresses for the major credit reporting agencies; and

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

(3) EXEMPTION.—A Federal agency shall be exempt from the requirements of this subsection if, following a breach of security, such agency determines that there is no reasonable risk of identity theft, fraud, or other unlawful conduct.

SEC. 4. ENFORCEMENT.

(a) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 2 or 3 shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57*a*(a)(1)(B)) regarding unfair or deceptive acts or practices.

(2) 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.

(3) LIMITATION.—In promulgating rules under this Act, the Commission shall not require the deployment or use of any specific products or technologies, including any specific computer software or hardware.

(b) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

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

(A) to enjoin further violation of such section by the defendant;

(B) to compel compliance with such section; or

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

(2) CIVIL PENALTIES.—

(A) CALCULATION.—

(i) TREATMENT OF VIOLATIONS OF SECTION 2.—For purposes of paragraph (1)(C) with regard to a violation of section 2, the amount determined under this paragraph is the amount calculated by multiplying the number of violations of such section by an amount not greater than $11,000. Each day that a person is not in compliance with the requirements of such section shall be treated as a separate violation. The maximum civil penalty calculated under this clause shall not exceed $5,000,000.

(ii) TREATMENT OF VIOLATIONS OF SECTION 3.—For purposes of paragraph (1)(C) with regard to a violation of section 3, the amount determined under this paragraph is the amount calculated by multiplying the number of violations of such section by an amount not greater than $11,000. Each failure to send notification as required under section 3 to a resident of the State shall be treated as a separate violation. The

maximum civil penalty calculated under this clause shall not exceed $5,000,000.

(B) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index is first published by the Bureau of Labor Statistics that is after 1 year after the date of enactment of this Act, and each year thereafter, the amounts specified in clauses (i) and (ii) of subparagraph (A) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(3) INTERVENTION BY THE FTC.—

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

(i) to intervene in the action;

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

(iii) to file petitions for appeal.

(B) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING.—If the Commission has instituted a civil action for violation of this Act, no State attorney general, or official or agency of a State, may bring an action under this subsection during the pendency of that action against any defendant named in the complaint of the Commission for any violation of this Act alleged in the complaint.

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

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(c) AFFIRMATIVE DEFENSE FOR A VIOLATION OF SECTION 3.—It shall be an affirmative defense to an enforcement action brought under subsection (a), or a civil action brought under subsection (b), based on a violation of section 3, that all of the personal information contained in the data in electronic form that was acquired as a result of a breach of security of the defendant is public record information that is lawfully made available to the general public from Federal, State, or local government records and was acquired by the defendant from such records.

SEC. 5. DEFINITIONS.

In this Act the following definitions apply:

(1) BREACH OF SECURITY.—The term "breach of security" means the unauthorized acquisition of data in electronic form containing personal information.

(2) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(3) 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.

(4) ENCRYPTION.—The term "encryption" means the protection of data in electronic form in storage or in transit using an encryption technology that has been adopted by an established standards setting body which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data. Such encryption must include appropriate management and safeguards of such keys to protect the integrity of the encryption.

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

(6) INFORMATION BROKER.—The term "information broker" means a commercial entity whose business is to collect, assemble, or maintain personal information concerning individuals who are not current or former customers of such entity in order to sell such information or provide access to such information to any nonaffiliated third party in exchange for consideration, 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.

(7) PERSONAL INFORMATION.—

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

(i) Social Security number.

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

(iii) Financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to 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) to the extent that such modification is necessary to accommodate changes in technology or practices, will not unreasonably impede interstate commerce, and will accomplish the purposes of this Act.

(8) PUBLIC RECORD INFORMATION.—The term "public record information" means information about an individual which has been obtained originally from records of a Federal, State, or local government entity that are available for public inspection.

(9) NON-PUBLIC INFORMATION.—The term "non-public information" means information about an individual that is of a private nature and neither available to the general public nor obtained from a public record.

SEC. 6. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE INFORMATION SECURITY LAWS.—This Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State, with respect to those entities covered by the regulations issued pursuant to this Act, that expressly—

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

(2) requires notification to individuals of a breach of security resulting in unauthorized acquisition of data in electronic form containing personal information.

(b) ADDITIONAL PREEMPTION.—

(1) IN GENERAL.—No person other than the Attorney General of a State may bring a civil action under the laws of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act.

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

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

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

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

(d) PRESERVATION OF FTC AUTHORITY.—Nothing in this Act may be construed in any way to limit or affect the Commission's authority under any other provision of law, including the authority to issue advisory opinions (under part 1 of volume 16 of the Code of Federal Regulations), policy statements, or guidance regarding this Act.

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 cease to be in effect on 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 $1,000,000 for each of fiscal years 2006 through 2010 to carry out this Act.

PURPOSE AND SUMMARY

As reported by the Committee on the Judiciary, H.R. 4127, the "Data Accountability and Trust Act of 2006," is intended to protect consumers by requiring security policies and procedures to protect computerized data containing personal information, and to provide nationwide notice to consumers in the event of a breach of such data. The bill authorizes the Federal Trade Commission (FTC) to establish such policies and procedures, which would be enforced by

the FTC and State Attorneys General. An amendment added by the Judiciary Committee would also require Federal departments and agencies to notify consumers of data breaches in the same manner as the private sector.

BACKGROUND AND NEED FOR THE LEGISLATION

On May 4, 2006, the Committee on Energy and Commerce reported H.R. 4127, the "Data Accountability and Trust Act of 2006." [1] The bill was sequentially referred to the Committee on the Judiciary for a period ending not later than June 2, 2006. The sections within the jurisdiction of the Committee on the Judiciary pertain to civil enforcement by State Attorneys General, and related civil penalties, as well as the bill's effect on State laws related to trespass, contract, tort law and acts of fraud.

The Committee on the Judiciary became acutely aware of the need to provide greater oversight and regulation of personally identifiable data with the revelation in February 2005 that organized criminals had fraudulently obtained personal data on nearly 145,000 consumers from ChoicePoint, Inc., an Alpharetta, Georgia-based data broker.[2] The criminals used the data to commit various acts of identity theft. Since that watershed breach, businesses that maintain such data, including other data brokers,[3] financial institutions,[4] media companies,[5] retailers,[6] universities,[7] and Federal government agencies [8] have experienced similar breaches involving sensitive information that can be used to commit identity theft.

Although the focus of public attention has been on the missteps of data brokers, the Judiciary Committee understands that data brokers provide a wide array of beneficial information services to business and government entities, particularly law enforcement. For example, data broker information is used by Federal, State and local law enforcement officials in locating criminals, such as those who fail to appear at trial, or fail to pay court-ordered child support. Businesses also use data broker-provided services to detect and deter fraudulent transactions. Despite these benefits, the seeming epidemic in data breaches over the last year raises serious questions about the aggregation of sensitive consumer information, whether this information is protected adequately from misuse and unauthorized disclosure, and the relationship, if any, to the increase in identity theft and other crimes.

Data security breaches have raised questions about the sufficiency of current laws to protect consumer information from identity theft. Although there are Federal laws that provide standards for disclosure of some types of personal information and require certain entities to take steps to safeguard personal information, there is no comprehensive Federal law dealing with data security.

---

[1] See H.R. Rep. No. 109–453, Part I (2006).

[2] Joseph Menn, Fraud Ring Taps Into Credit Data, L.A. Times, February 15, 2005 at 1.

[3] David Colker, ID Thieves Tap Files at 2nd Big Data Firm, L.A. Times, March 10, 2005 at 1.

[4] Mark Mueller, Inside Ring is Charged in Financial Data Scheme, Nwrk. Star-Ledger, April 29, 2005 at 21.

[5] Jon Swartz, Time-Warner Data on 600,000 Missing, USA Today, May 3, 2005.

[6] Bill Husted & David Markiewicz, I.D. Theft Slams Chain, 1.4 Million Cards Stolen, Atl.J-Const., April 20, 2005 at 1.

[7] Allison Kolodziej, Data Thieves Prey on Colleges: Schools Becoming More Vigilant to Safeguard Personal Information, Columbus Dis., May 13, 2006 (online version).

[8] Christopher Lee, Personal Data on Veterans is Stolen, Wash. Post, May 23, 2006 at A1.

In addition, many of our Federal laws have not been adequately updated since the growth of the Internet as a tool of commerce during the last decade, making consumers as vulnerable as they have ever been to the threat of identity theft.

H.R. 4127 attempts to create a uniform Federal standard for the protection of sensitive personal information and for providing notice to consumers in the event that their personal information is compromised by a security breach. The bill authorizes the Federal Trade Commission (FTC) to set such standards, and enforce those standards as violations of Section 5 of the Federal Trade Commission Act. The legislation also authorizes State Attorneys General to enforce the Federal law and obtain civil penalties for violations of the Act.

The Committee on the Judiciary supports the goal of crafting comprehensive, rational, and non-duplicative national standards for handling data breaches involving personal information. Unfortunately, H.R. 4127 as reported to the Judiciary Committee falls short of that goal in a few key areas.

First, the bill permits the FTC to regulate the data collection and retention activities of virtually any entity that owns or possesses personal information. This includes financial services firms that are already subject to stringent privacy and information security standards under the Federal Gramm-Leach-Bliley Act. Rather than expressly exempting federally-regulated institutions from the scope of the bill's coverage, H.R. 4127 allows the FTC to determine whether and how financial institutions should be covered by the law. The FTC has little expertise in the area of financial data regulation, and the Judiciary Committee believes that this expansion of the FTC's jurisdiction is unwarranted, and potentially could result in duplicative and burdensome Federal regulation.

Second, the bill permits State Attorneys General to enforce the bill's data protection and consumer notice requirements if the FTC fails to act. Again, because the bill sweeps in virtually every entity that owns or possesses personal information, the bill would allow State Attorneys General to bring enforcement actions against financial institutions, rather than leaving regulation and enforcement of these entities to the Federal financial regulators. The Committee believes that State Attorneys General can and should play an important role in enforcing violations of State and Federal law, including in the area of data security. H.R. 4127 goes too far, however, by expanding State Attorney General enforcement in an area traditionally reserved to Federal financial regulators.

Finally, the bill's preemption provision undermines the legislation's general effort to create a uniform set of Federal requirements governing data security and consumer notice. Although the bill attempts to create national standards, it expressly protects State consumer protection laws and does not preempt any State law relating to fraud. These broad exceptions raise questions about whether entities regulated under H.R. 4127 will be subject to conflicting State and Federal laws and regulations, undermining the goal of a nationwide standard for the protection of personal data.

HEARINGS

No hearings were held in the Committee on the Judiciary on H.R. 4127. On May 9, 2006, the House Judiciary Committee's Sub-

committee on Crime, Terrorism and Homeland Security held a hearing on the policy issues raised by the increase in computer crime and identity theft. The Subcommittee received testimony from: Ms. Laura H. Parsky, Deputy Assistant Attorney General, Criminal Division, United States Department of Justice; Mr. Joseph LaRocca, Vice President, Loss Prevention, National Retail Federation; Ms. Anne Wallace, Executive Director, Identity Theft Assistance Corporation; and Ms. Susanna Montezemolo, Policy Analyst, Consumers Union.

COMMITTEE CONSIDERATION

On Thursday, May 25, 2006, the Committee met in open session and ordered favorably reported the bill, H.R. 4127, by voice vote with an amendment, a quorum being present.

VOTE OF THE COMMITTEE

In compliance with clause 3(b) of Rule XIII of the Rules of the House of Representatives, the Committee notes that there were no recorded votes on H.R. 4127 during the Committee on the Judiciary's consideration of the bill.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee reports that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

NEW BUDGET AUTHORITY AND TAX EXPENDITURES

Clause 3(c)(2) of House Rule XIII is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

COMMITTEE COST ESTIMATE

In compliance with clause 3(d)(2) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to H.R. 4127, the following estimate. This Committee primarily adopts the Congressional Budget Office's prepared cost estimate of H.R. 4127 as reported by the House Committee and Energy Commerce, which is included in their report.[9] An amendment was adopted to the bill that would require Federal departments and agencies to notify consumers of data breaches in the same manner as the private sector. The following excerpt draws Congressional Budget Office's prepared cost for S. 1789, and is describing a substantively identical provision in that legislation. The Committee believes the cost analysis for this amendment would be virtually identical to the following analysis.

The Federal Information Security Management Act of 2002 provides requirements for securing the federal government's information systems, including the protection of personal privacy. The National Institute of Standards and Technology develops information

[9] See H.R. Rep. No. 109–453, Part I (2006).

security standards and guidelines for other federal agencies, and the Office of Management and Budget (OMB) oversees information technology security policies and practices. OMB estimates that federal agencies spend around $5 billion a year to secure the government's information systems.

In the event of a security breach involving a significant risk of identity theft, government agencies would be required to notify an individual whose information may have been compromised. Notification would be in the form of individual notice (written notice to a home mailing address, via telephone, or via e-mail) as well as through the mass media. The cost of such notification would depend on the number of security breaches that occur, the number of persons affected, and the cost per person of notification. CBO cannot estimate the number of security breaches that might occur within the federal government in any year.

Nationwide, only the largest breaches are identified and reported. Limited anecdotal information over the last two years suggests that security breaches involving the federal government have occurred regularly usually involving the theft of computers containing personal information from specific agencies. Such thefts have affected the personal information of about 3 percent of the 4 million civilian and military federal employees (about 120,000). Based on that data and information from OMB and other agencies, CBO does not expect that there would be significant notification costs under the bill in any one year. Thus, CBO estimates that implementing the notification provision in S. 1789 would cost less than $500,000 annually.

Nonetheless, the federal government is also one of the largest providers, collectors, consumers, and disseminators of personnel information in the United States. The cost to notify individuals of a security breach to personnel information may cost up to $2 per notification. Although, CBO cannot anticipate the number of security breaches, a significant breach of security involving a major collector of personnel information, such as the Internal Revenue Service or the Social Security Administration could involve millions of individuals and would have a significant budgetary impact.[10]

PERFORMANCE GOALS AND OBJECTIVES

The goal of H.R. 4127 is to protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information, and to provide for uniform nationwide notice in the event of a security breach.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds the authority for this legislation in art. I, § 8 of the Constitution.

SECTION-BY-SECTION ANALYSIS AND DISCUSSION

The following section-by-section analysis describes the sections of H.R. 4127 as reported that fall within the Rule X jurisdiction of the

[10] Congressional Budget Office Cost Estimate of S. 1789, the "Personal Data Privacy and Security Act of 2005," as reported by the Senate Judiciary Committee on November 17, 2005, available at http://cbo.gov/ftpdocs/71xx/doc7161/s1789.pdf.

Committee on the Judiciary. For a description of the other sections of the bill, please refer to the report of the Committee on Energy and Commerce.[11]

Section 3. Notification of information security breach

Section 3 requires any entity engaged in interstate commerce that owns or possesses personal information in electronic form to notify individuals whose information was acquired by an unauthorized person and the FTC, following the discovery of a breach of security of the system containing such information.

Section 3(b) requires special notification for entities that do not own the data subject to a security breach. Specifically, a third party agent contracted to maintain or process data in electronic form on behalf of an entity who owns or possesses such personal information is required to notify the person or entity that owns or possesses the data who in turn provides notice as required by section 3(a). The Committee recognizes that many companies are contracted to provide data services for companies that own or possess personal information. Contracted entities in many an instance do not have contact information for an individual whose information was breached and would therefore be unable to provide notice. Additionally, the Committee believes for a notice to be most effective, it should come from the entity with whom the individuals are most likely to identify or recognize by means of a relationship.

Similarly, section 3(b)(2) recognizes that telecommunications carriers, cable operators, information service or interactive computer services provide transmission utility for data in transit. As such, a breach of data in transit that utilizes the means of transmission may not be identifiable. Further, in such cases where a breach is identifiable, the nature of the data and identity of the sender of the data may not be readily identifiable by the provider of the transmission utility. This subsection provides that such third party entity will only be required to notify the entity that initiated the transmission of the data of the breach, provided such entity can be reasonably identified.

Section 3(b)(3) addresses security breaches that include individually identifiable health information. Upon receiving notice from the entity that suffered the breach, the FTC is required to provide a copy of such notice to the Secretary of Health and Human Services.

Section 3(c) requires notices be made as promptly as possible but consistent with any measures undertaken to determine the scope of the breach, prevent further breach, and restore integrity of the system. Section 3(d) provides for the method of the notification. Entities required to send notice may do so by either written notification or by email. Notice by email is only permitted in cases when it is the entity's primary contact method with the individual or the individual has consented to receive such notification by email and the notification is consistent with applicable law.

Section 3(e) provides that an entity required to provide notice for a breach of security shall provide, or make arrangements for the provision of, quarterly consumer credit reports for two years from

[11] *Id.*

one of the major credit reporting agencies, and at no cost to the individual, upon request from the individual.

Section 3(f) provides an exemption from the requirements of section 3 under certain circumstances. Specifically, under section 3(f)(1) an entity is not required to provide notice if it determines there is no reasonable risk of identity theft, fraud, or other unlawful conduct following a breach of security. The Committee expects these determinations will be fact specific and will take account of the types of information breached, the party that acquired the information, and the usability of the information by the party who acquired it. Further, section 3(f)(2)(A) establishes a rebuttable presumption that there is no reasonable risk of identity theft, fraud, or other unlawful conduct if the data that is breached is encrypted. The presumption may be rebutted by facts demonstrating that the encryption has been or is likely to be compromised. The Committee recognizes that, given sufficient time, all encryption may be "compromised" as encryption standards evolve and forms of encryption become outdated.

Although encryption is a widely used and accepted practice of securing data, the Committee does not intend to deem encryption as the only effective method or technology of securing and protecting data. In fact, many industry experts take the position that other methods and technologies used to protect data are equally, and in some cases more, effective than encryption. Section 3(f)(2)(B) provides that the FTC shall, by rule and within nine months of the date of enactment of the Act, identify any other methods or technologies that render electronic data unreadable or indecipherable. The Committee's intent in requiring the FTC to undertake this rulemaking is that the Commission should not be limited in determining any other effective data protection technologies or methods, in addition to encryption, which would render data unusable and therefore establish a presumption there is no reasonable risk of identity theft, fraud, or other unlawful activity.

Section 3(f)(3) requires the Commission to issue guidance within one year of enactment of the Act regarding the application of the exemption in section 3(f).

Section 3(g) provides the Commission with discretion to place a notice of a breach of security it has received under section 3(a)(2) on its website if the Commission determines such posting is in the public interest and for the protection of consumers.

Section 3(h) provides for an FTC study regarding the practicality and cost effectiveness of requiring notification to be provided in a language in addition to English.

Section 3(i) requires Federal agencies that own or possess data in electronic form containing personal information to provide written notice to each individual who is a citizen or resident of the United States if their personal information is acquired by an unauthorized person as a result of a security breach. Agencies are exempt from making such disclosures if they determine that the breach causes no reasonable risk of identity theft, fraud, or other unlawful conduct. The Committee intends this provision to address circumstances where the Federal government maintains information in a similar manner as the private sector, such as the recent breach of the personal information of nearly 26.5 million veterans maintained by the United States Department of Veterans Affairs,

and does not intend it to apply in circumstances where disclosure of the breach or the information that is the subject of the breach could compromise a criminal investigation or national security.

Section 4. Enforcement

Section 4(a)(1) provides that a violation of the Act shall be enforced by the FTC as an unfair and deceptive act or practice in violation of a regulation under section 18 the Federal Trade Commission Act. The FTC has limited or no jurisdiction over certain types of entities and activities. These include banks, savings associations, and Federal credit unions; regulated common carriers; air carriers; non-retail sales of livestock and meat products; nonprofit entities; and the business of insurance. See, e.g., 15 U.S.C. Sec. §§ 44, 45, 46 (FTC Act); 15 U.S.C. § 21 (Clayton Act); 7 U.S.C. § 227 (Packers and Stockyards Act); 15 U.S.C. § 1011 et seq. (McCarran-Ferguson Act).

Section 4(a)(3) prohibits the FTC from requiring the deployment of any specific products or technologies, including any specific computer software or hardware, in promulgating rules under this Act. The Committee recognizes the rapidly evolving improvements in technologies and products to protect personal information and believes the market is the most effective mechanism in determining which specific products best protect personal information.

Section 4(b) provides for enforcement by an attorney general of a State or an official or agency of a State if the attorney general, or an official or agency of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by a violation of section 2 or 3. The attorney general or official or agency of a State may bring civil action to enjoin further violations of section 2 or 3, compel compliance with section 2 or 3, or to obtain civil penalties for violations of section 2 or 3.

Section 4(b)(2)(A) sets forth the structure for civil penalties. With respect to a violation of section 2, the civil penalty is calculated by multiplying the number of violations of the section by an amount not greater than $11,000, with each day of noncompliance treated as a separate violation. Civil penalties for violations of section 2 are capped at $5 million.

Beginning with the first Consumer Price Index published at least one year after the date of enactment of this Act, and continuing on an annual basis, section 4(b)(2)(B) requires the amounts specified in section 4(b)(2)(A) to be increased by the annual percentage increase in the Consumer Price Index.

Section 4(b)(3) provides specific obligations and limitations on State actions. In particular, section 4(b)(3)(A) requires a State to provide prior written notice to the FTC of any action brought under this Act and to provide the Commission with a copy of the complaint. The Commission has the right to intervene in the action by the State, to be heard on all matters relating to the action, and to file petitions for appeal. Further, if the FTC has instituted a civil action for a violation of this Act, State action is stayed during the pendency of the Federal action.

Section 4(c) provides an affirmative defense to an enforcement action brought under subsection (a) or a civil action brought under subsection (b), if all of the personal information contained in the data was acquired as a result of a breach of security is public

record information and was acquired by the defendant from public records.

Section 6. Effect on other laws

Section 6(a) provides that the Act preempts statutes, regulations, or rules of a State, or a subdivision of a State, with respect to the entities covered by the regulations issued pursuant to the Act, that require information security practices and treatment of data in electronic form containing personal information similar to any of those required under section 2 and notification for a breach of security resulting in an unauthorized acquisition of data in electronic form containing personal information.

Section 6(b) prohibits any person other than the attorney general of a State to bring a civil action under the law of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act, but makes clear that this prohibition shall not be construed to limit the enforcement of any State consumer protection law by an Attorney General of a State. Section 6(c) specifically preserves State trespass, contract, and tort law, and other State laws to the extent those acts relate to acts of general consumer fraud. Section 6(d) preserves the FTC's authority under any other provision of law, including the authority to issue advisory opinions, policy statements, or guidance regarding the Act.

In addition, the Act is not intended to weaken the privacy protections for health information established pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its regulations. This includes maintaining HIPAA's provisions regarding State privacy laws related to identifiable health information that are not contrary to or that are more stringent than the requirements, standards, or implementation specifications imposed under the HIPAA regulation.

○