109TH CONGRESS
2d Session

HOUSE OF REPRESENTATIVES

REPT. 109–453
Part 1

DATA ACCOUNTABILITY AND TRUST ACT (DATA)

MAY 4, 2006.—Ordered to be printed

Mr. BARTON of Texas, from the Committee on Energy and Commerce, submitted the following

REPORT

[To accompany H.R. 4127]

[Including cost estimate of the Congressional Budget Office]

The Committee on Energy and Commerce, 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 a security breach, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

AMENDMENT

The amendment is as follows:

Strike all after the enacting clause and insert the following:

49–006

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 information 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 Commission 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 individuals, 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 1 year 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.

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

H.R. 4127, the "Data Accountability and Trust Act," requires security policies and procedures to protect computerized data containing personal information, and provides for nationwide notice in the event of a security breach involving personal information.

BACKGROUND AND NEED FOR LEGISLATION

Data brokers provide a wide array of beneficial information services to business and government entities. For example, such information is used by law enforcement agencies in locating criminals and witnesses and by businesses and financial institutions in detecting 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 jump in identity theft and other frauds.

In February 2005, ChoicePoint Inc., one of the nation's largest data brokers, announced that personal information on at least 145,000 consumers had been bought from the company by thieves who masqueraded as legitimate business people. Some of that information has been utilized in frauds, while the rest to date has not. Prosecutors have moved against several websites that warehouse and sell stolen personal information. The Privacy Rights Clearinghouse, a San Diego based group, has posted a chronology of the steady stream of data breaches since ChoicePoint. (See *http://www.privacyrights.org/ar/ChronDataBreaches.htm.*) As of March 25, 2006, this chronology noted 147 breaches involving the Social Security number, drivers license number, or financial account number of over 53 million American consumers. While the Committee has not verified these numbers, it has reviewed most of the underlying public announcements and is struck by several things.

Data security breaches by data brokers, financial institutions, and retailers 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 some types of personal information, there is no comprehensive Federal law dealing with data security. The Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLBA) provide privacy and security requirements for financial related information. The Health Insurance Portability and Accountability Act provides privacy and security requirements for health related information. The universe of entities to which these bodies of law apply is limited.

In addition, the Federal Trade Commission Act (FTC Act) deals broadly with "unfair and deceptive acts or practices in or affecting commerce." The FTC uses Section 5 of the FTC Act to enforce against companies that make deceptive claims regarding privacy or security they provide for consumer information. The Commission also uses Section 5 to enforce against unfair practices that are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition.

Because of the absence of a comprehensive Federal law dealing with data security, the Committee intends to address the problem of securing sensitive data and providing notice to consumers in the case of a loss of data that creates a risk of harm to the consumer. Furthermore, the Committee intends to provide for uniform national regulation for data security and breach notification by preempting the matrix of different state laws that regulate these areas. The recent losses of consumer data have created significant policy concerns that the Committee will address through this legislation and ongoing oversight.

HEARINGS

The Subcommittee on Commerce, Trade, and Consumer Protection held an oversight hearing on Tuesday, March 15, 2005, on the policy issues raised by data breaches at ChoicePoint and other information brokers. The Subcommittee received testimony from: The Honorable Deborah Platt Majoras, Chairman, Federal Trade Commission; Mr. Kurt P. Sanford, President and Chief Executive Officer, U.S. Corporate and Federal Government Markets, LexisNexis; Mr. Derek Smith, Chairman and Chief Executive Officer, ChoicePoint, Inc.; Mr. Joseph Ansanelli, Chairman and Chief Executive Officer, Vontu, Inc.; and Mr. Marc Rotenberg, Executive Director, Electronic Privacy Information Center. The Subcommittee also held an oversight hearing on Wednesday, May 11, 2005, on safeguards to protect consumer information. The Subcommittee received testimony from: Ms. Jennifer Barrett, Chief Privacy Officer, Acxiom Corporation; Mr. Steven Buege, Senior Vice President of Business Information, News and Public Records, North American Legal, Thomson West; Mr. Oliver I. Ireland, Partner in the Financial Services Practice Group, Morrison and Foerster LLP, on behalf of Visa USA; Mr. Daniel Burton, Vice President of Government Affairs, Entrust, Inc.; and, Professor Daniel Solove, Associate Professor of Law, George Washington University Law School.

In addition, the Subcommittee on Commerce, Trade, and Consumer Protection held a legislative hearing on a discussion draft on Thursday, July 28, 2005. The Subcommittee received testimony from: Ms. Fran Maier, Executive Director and President, TRUSTe; Mr. Michael Hintze, Senior Attorney, Microsoft Corporation; Mr. Chris Hoofnagle, Senior Counsel & Director, Electronic Privacy Information Center, West Coast Office; and, Mr. Daniel Burton, Vice President of Government Affairs, Entrust, Inc.

COMMITTEE CONSIDERATION

On Thursday, November 3, 2005, the Subcommittee on Commerce, Trade, and Consumer Protection met in open markup session and approved H.R. 4127 for Full Committee consideration, amended, by a recorded vote of 13 yeas and 8 nays, a quorum being present. On Wednesday, March 29, 2006, the Committee on Energy and Commerce met in open markup session and ordered H.R. 4127 reported to the House, amended, by a recorded vote of 41 yeas and 0 nays, a quorum being present.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the record votes on the motion to report legislation and amendments thereto. The following is the recorded vote taken on the motion by Mr. Barton to order H.R. 4127 reported to the House, amended, which was agreed to by a recorded vote of 41 yeas and 0 nays.

COMMITTEE ON ENERGY AND COMMERCE -- 109TH CONGRESS
ROLL CALL VOTE # 105

Bill: H.R. 4127, Data Accountability and Trust Act.

MOTION: Motion by Mr. Barton to order H.R. 4167 reported to the House.

DISPOSITION: **AGREED TO**, by a roll call vote of 41 yeas to 0 nays.

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Mr. Barton	X			Mr. Dingell	X		
Mr. Hall	X			Mr. Waxman			
Mr. Bilirakis	X			Mr. Markey	X		
Mr. Upton	X			Mr. Boucher			
Mr. Stearns	X			Mr. Towns	X		
Mr. Gillmor	X			Mr. Pallone			
Mr. Deal	X			Mr. Brown			
Mr. Whitfield	X			Mr. Gordon			
Mr. Norwood				Mr. Rush			
Ms. Cubin	X			Ms. Eshoo	X		
Mr. Shimkus	X			Mr. Stupak	X		
Ms. Wilson	X			Mr. Engel	X		
Mr. Shadegg				Mr. Wynn			
Mr. Pickering	X			Mr. Green	X		
Mr. Fossella	X			Mr. Strickland	X		
Mr. Blunt				Ms. DeGette	X		
Mr. Buyer				Ms. Capps	X		
Mr. Radanovich	X			Mr. Doyle	X		
Mr. Bass	X			Mr. Allen			
Mr. Pitts	X			Mr. Davis			
Ms. Bono	X			Ms. Schakowsky	X		
Mr. Walden				Ms. Solis	X		
Mr. Terry	X			Mr. Gonzalez	X		
Mr. Ferguson	X			Mr. Inslee	X		
Mr. Rogers				Ms. Baldwin	X		
Mr. Otter	X			Mr. Ross	X		
Ms. Myrick							
Mr. Sullivan	X						
Mr. Murphy	X						
Mr. Burgess	X						
Ms. Blackburn	X						

3/29/2006

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held legislative and oversight hearings and made findings that are reflected in this report.

STATEMENT OF GENERAL 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.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 4127, the Data Accountability and Trust Act, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

COMMITTEE COST ESTIMATE

The committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, April 6, 2006.

Hon. JOE BARTON,
Chairman, Committee on Energy and Commerce,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 4127, the Data Accountability and Trust Act (DATA).

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Melissa Z. Petersen (for federal costs), Sarah Puro (for the impact on state, local, and tribal governments), and Tyler Kruzich (for the impact on the private sector).

Sincerely,

DONALD B. MARRON,
Acting Director.

Enclosure.

H.R. 4127—Data Accountability and Trust Act (DATA)

Summary: H.R. 4127 would require private companies with access to consumers' personal information to take certain precautions to safeguard that information. Under the bill, private companies would be required to notify consumers and the Federal Trade Commission (FTC) whenever there is a breach in the security of a consumer's personal information. The bill also would require companies that maintain databases containing individuals' personal information to supply individuals with their personal electronic records upon request and to provide a means to correct mistakes in those records. The FTC would enforce the restrictions and requirements included in H.R. 4127 and create regulations related to the security of consumers' personal information. Assuming appropriation of the amounts specifically authorized in the bill, CBO estimates that implementing H.R. 4127 would cost less than $500,000 in 2006 and a total of $5 million over the 2006–2011 period.

Enacting H.R. 4127 could increase federal revenues as a result of the collection of additional civil penalties assessed for violations of laws related to information security. Collections of civil penalties are recorded in the budget as revenues. CBO estimates, however, that any additional revenues that would result from enacting the bill would not be significant because of the relatively small number of cases likely to be involved. Enacting the bill would not affect direct spending.

H.R. 4127 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates costs to state, local, and tribal governments, if any, would be small and would not exceed the threshold established in UMRA ($64 million in 2006, adjusted annually for inflation).

H.R. 4127 would impose several private mandates as defined in UMRA. It would require certain businesses and individuals engaged in interstate commerce to implement information security programs and notify individuals in the event of a security breach. It would also place new requirements on information brokers. While CBO cannot estimate the direct cost of complying with each mandate, H.R. 4127 would impose security requirements and notification procedures and practices on millions of private-sector entities. Based on information from industry sources, CBO estimates that the aggregate cost of the mandates in the bill would exceed the annual threshold established by UMRA for private-sector mandates ($128 million in 2006, adjusted annually for inflation) in at least one of the first five years that the mandates are in effect.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 4127 is shown in the following table. The costs of this legislation fall within budget function 370 (commerce and housing credit). For this estimate, CBO assumes that the bill will be enacted before the end of 2006 and that the specified amounts will be appropriated for each year. CBO estimates that implementing H.R. 4127 would cost less than $500,000 in 2006 and about $5 million over the 2006–2011 period for the FTC to issue regulations and enforce the bill's provisions regarding the security of consumers' personal information. Enacting the legislation would not have a significant effect on revenues and would not affect direct spending.

	By fiscal year, in millions of dollars—					
	2006	2007	2008	2009	2010	2011
CHANGES IN SPENDING SUBJECT TO APPROPRIATIONS						
Authorization Level	1	1	1	1	1	0
Estimated	*	1	1	1	1	1

Estimated impact on State, local, and tribal governments: H.R. 4127 contains intergovernmental mandates as defined in UMRA. Provisions in section 4 would require State Attorneys General to notify the FTC of any action taken under the bill, allow the FTC to intervene in those actions, and limit the actions that Attorneys General may take in certain circumstances. Also, provisions in section 6 would preempt state law in about 20 states regarding the protection and use of certain personal data. Those provisions constitute intergovernmental mandates as defined in UMRA. CBO estimates that the aggregate costs, if any, to state, local, and tribal governments of complying with the mandates in the bill would be small and would not exceed the threshold established in UMRA ($64 million in 2006, adjusted annually for inflation).

CBO assumes that the bill would grant to new authority to the FTC to regulate the activities of state and local governments. Under current law, the courts have ruled that the FTC does not have jurisdiction over those governments or over public universities. The provisions of the bill creating requirements to comply with FTC regulations regarding the handling of certain data, therefore, would not apply to such entities.

Estimated impact on the private sector: H.R. 4127 would impose several private-sector mandates as defined in UMRA. It would require certain businesses and individuals engaged in interstate commerce to implement information security programs and notify individuals in the event of a security breach. It also would place new requirements on information brokers. While CBO cannot estimate the direct cost of complying with each mandate, H.R. 4127 would impose security requirements and notification procedures and practices on millions of private-sector entities. Based on information from industry sources, CBO estimates that the aggregate cost of the mandates in the bill would exceed the annual threshold established by UMRA for private-sector mandates ($128 million in 2006, adjusted annually for inflation) in at least one of the first five years that the mandates are in effect.

Requirements for information security and security breach notification

Section 2 would require certain businesses and individuals engaged in interstate commerce that own or possess personal information in electronic form, or that contract a third party to maintain such data, to establish and implement information security practices in compliance with regulations to be set by the FTC.

Such entities would be required to implement information security requirements that take into consideration the nature of the activities in which the entity takes part, available technology, and the cost of implementing the program. Those entities would also have to conduct periodic vulnerability testing on their programs. Additionally, those entities would have to identify an officer responsible for the oversight of the information security program.

Moreover, entities may have to implement a process for disposing of obsolete data in electronic form. Some entities could be determined to be in compliance with section 2 by the FTC if those entities are currently in compliance with other federal regulations to maintain standards and safeguards for information security.

Section 3 would require those private entities to notify each U.S. citizen or resident following the discovery of a security breach in which the individual's special information was acquired by an unauthorized person, as well as to notify the FTC. In addition, the entities would have to provide the credit reports to individuals affected by a breach at no cost to the individual, if requested, as well as a toll-free phone number by which the individual can reach the entity.

Section 3 would allow types of substitute notification if the private entities own or possess personal information on less than 1,000 individuals and direct notification is not feasible due to excessive cost to the entities or a lack of contact information for the individuals. Section 3 also would allow an entity to be exempt from notification requirements, however, if it determines that there is not reasonable risk of identity theft, fraud, or other unlawful conduct. As allowable presumption that no risk of identify theft or fraud exists includes encryption or similar modification of data so that it is rendered unreadable.

The cost of those mandates depends on several factors. If additional security measures are implemented by the entities covered under this bill, the number of security breaches would tend to be lower over time. Conversely, if a large number of security breaches continue to occur in spite of the requirements of the information security program, entities would be required to send a large number of notifications to individuals' personal information was stolen or accessed in security beaches, none of which was encrypted. If private entities would be required to notify a comparative number of individuals, the notification requirements would be costly to those entities.

The mandates in section 2 and section 3 would extend to millions of private entities that use or maintain personal information. CBO estimates that even though per-entity costs of implementing the information security program or providing notification of a security breach required under the bill could be small, the aggregated cost of mandates in those sections would exceed UMRA's annual threshold in at least one of the first five years that the mandates are in effect.

Requirements for information brokers

Section 2 would require information brokers to disclose all personal information to individuals if requested by the individual at no cost to the individual. Additionally, if any incorrect information is contained in the information brokers' records, they would be required to change the information or provide the individual with contact information for the source from which the information broker obtained the individual's information. An information broker is defined in the bill as 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 or provide access to such information to any non-affiliated third party.

The cost to information brokers of providing individuals with their personal information at no cost and having to change individuals' information could be large. Some evidence exists that many individuals' personally identifiable information housed at large information brokerage firms is in part incorrect. If a large number of individuals request data changes, CBO estimates that the time and notification costs to information brokers could be high.

Section 2 would further require information brokers to maintain an audit log of internal and external access to, or transmission of, any data in electronic form containing personal information. It would further require information brokers to submit to an audit by the FTC in the event of a security breach or if requested by the commission. CBO does not have sufficient information about industry practices to estimate the cost of this provision on the private sector.

Previous CBO estimates: CBO has provided estimates for three bills that address the security, handling, and use of certain personally identifying or sensitive data, all of which would require private companies to take certain precautions to safeguard the personal information of consumers. None of the bills would have a significant impact on direct spending or revenues. Each bill would impose private-sector mandates that exceed the threshold in UMRA ($128 million 2006, adjusted annually for inflation) and include intergovernmental mandates as defined in UMRA; all would preempt state and local laws. The bills we have previously reviewed are:

- H.R. 3997, the Financial Data Protection Act of 2006, as ordered reported by the House Committee on Financial Services on March 16, 2006. CBO transmitted a cost estimate for this bill on March 30, 2006. H.R. 3997 includes a provision to allow consumers to place a security freeze on their credit report.
- S. 1326, the Notification of Risk to Personal Data Act, as reported by the Senate Committee on the Judiciary on October 20, 2005. CBO transmitted a cost estimate for this bill on March 10, 2006. In addition to requirements on private-sector companies, S. 1326 would require government agencies at the federal, state, and local level to take certain precautions to safeguard the personal information that they possess. S. 1326 contains intergovernmental mandates that exceed the threshold in UMRA ($64 million in 2006, adjusted annually for inflation).
- S. 1408, the Identity Theft Protection Act, as ordered reported by the Senate Committee on Commerce, Science, and Transportation on July 28, 2005. CBO transmitted a cost estimate for this bill on November 3, 2005. S. 1408 includes a provision to allow consumers to place a security freeze on their credit report. The bill also contains intergovernmental mandates that would exceed the threshold in UMRA ($64 million in 2006, adjusted annually for inflation).

Estimate prepared by: Federal Costs: Melissa Z. Petersen. Impact on State, Local, and Tribal Governments: Sarah Puro. Impact on the Private Sector: Tyler Kruzich.

Estimate approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act. [may need to revisit Based on CBP report]

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds that the Constitutional authority for this legislation is provided in Article I, section 8, clause 3, which grants Congress the power to regulate commerce with foreign nations, among the several States, and with the Indian tribes.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

Section 1 establishes the short title of the Act as the "Data Accountability and Trust Act."

Section 2. Requirements for information security

Section 2(a)(1) directs the Federal Trade Commission (FTC or Commission) to promulgate regulations to require persons engaged in interstate commerce that own or possess electronic data containing personal information to establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information. The regulations would also apply to any person that contracts to have a third party entity maintain data containing personal information on behalf of that person. The Committee intends that this provision apply not only to persons who contract with agents in the United States but also to persons who contract with agents outside of the United States. (See discussion of the FTC's jurisdiction and scope of "person" under section 4 hereinafter).

When promulgating these regulations, the Commission is directed to consider: (1) the size of, and the nature, scope, and complexity of the activities engaged in, by such person; (2) the current state of the art in administrative, technical, and physical safeguards for protecting personal information; and (3) the cost of implementing safeguards. The Committee intends these factors for consideration to shape regulations that set reasonable security standards that are flexible enough to accommodate different business models and different types of personal data, as well as evolving security practices.

Section 2(a)(2) explicitly provides that the regulations issued by the Commission shall require policies and procedures to include: (1) a security policy with respect to the collection, use, sale, other dissemination, and maintenance of personal information; (2) the identification of an individual with responsibility for the management of information security as a point of contact; (3) a process for identifying vulnerabilities in the security system; (4) a process for taking preventative and corrective actions to mitigate against vulnerabilities; and (5) a process for disposing of obsolete electronic data.

Section 2(a)(3) gives the FTC the authority to determine to be in compliance with the requirements of section 2(a), any person who is required under any other Federal law to maintain standards and safeguards for information security that provide equal or greater protection than those required under section 2(a). The Committee expects that the FTC will use this authority to consider whether compliance with rules on security safeguards promulgated pursuant to the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act are sufficient to comply with the provisions of section 2(a) of this Act.

Section 2(b)(1) requires the FTC to conduct a study on the practicality of requiring a standard method for the destruction of obsolete paper documents and other non-electronic data containing personal information. Section 2(b)(2) gives the FTC the authority to promulgate regulations requiring standard methods for the destruction of obsolete paper and non-electronic documents containing personal information if the Commission finds: (1) the improper disposal of obsolete paper or other non-electronic data creates a reasonable risk of identity theft, fraud, or other unlawful conduct; (2) a disposal requirement would be effective in preventing identity theft, fraud, or other unlawful conduct; (3) the benefits of a requirement would outweigh the costs; and (4) compliance with a requirement would be practicable. In enforcing any such regulations, the Commission may determine to be in compliance any person who is required under any other federal law to dispose of obsolete paper or other non-electronic data containing personal information if the Federal law to which that person is subject provides equal or greater protection for the personal information than that required under Section 2(b)(2).

Section 2(c) imposes special requirements on information brokers. Section 2(c)(1) directs the Commission to promulgate regulations that require information brokers to submit their security policies to the Commission in conjunction with a notification of a breach of security under section 3. The Commission may also request submission of policies at any time. Section 2(c)(2) requires the FTC to conduct an audit, or require the information broker to conduct an independent audit of security practices. The Commission may conduct or require the audits for the shorter of five years or until the Commission determines that the security practices are in compliance with the requirements of Section 2. The Committee does not intend the audit requirements of this section to provide precedent for audit requirements agreed upon between the parties under any Commission consent order.

Section 2(c)(3) provides for verification of and individual access to certain information collected, assembled, or maintained by an information broker. Section 2(c)(3)(A) requires each information broker to 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. The information broker is not required to verify information that identifies an individual's name and address and does not include any other information that specifically identifies such individual. The Committee intends that this provision should be interpreted in a similar manner to existing Federal statutes regarding the accuracy of personal information. The Committee requires that the accuracy of information be established through reasonable procedures, with a view to removing doubt concerning such accuracy. It is not required that accuracy be absolutely proven, or that the holders of such information resort to independent third parties to confirm the accuracy of the information.

Section 2(c)(3)(B)(i) requires each information broker to provide to each individual whose personal information it maintains, a means for the individual to review personal information maintained by the information broker as well as any other information maintained by the information broker that specifically identifies the individual. The information broker is not required to provide access to information that identifies an individual's name and address and does not include any other information that specifically identifies such individual. The information broker is required to offer access to the information once a year at no cost to the individual. Before granting access, the information broker must verify the identity of the individual requesting access to the information.

With the exclusion for information that merely identifies an individual's name and address, the Committee intends to exclude marketing and mailing lists and census data from the verification and access requirements of this section.

Section 2(c)(3)(B)(ii) provides the opportunity for an individual to make a written statement disputing the accuracy of the information maintained by an information broker. The information broker must again, verify the identity of the individual making the request. Through the Committee hearings and information gathering process, the Committee became aware of the harms that could result from fraudulent access to personal information. That harm is even greater if the person who fraudulently accesses the information is permitted to make a notation to or to alter the information. The Committee expects a second verification to guard against this. The information broker need take no action on the disputed information if there are reasonable grounds to believe the dispute is frivolous or irrelevant.

If the claim is not found to be frivolous or irrelevant, and the information broker has verified the identity of the individual seeking to dispute the information, the information broker is required to take action with regard to the disputed information. The information broker is required to take one of the following three actions: (1) correct the information; (2) with regard to 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 (3) with regard to non-public information, note that the information is disputed, including the individual's statement disputing the information, and take reasonable steps to independently verify the information under the procedures in Section 2(c)(3)(A) if such information can be independently verified. The Committee notes that the notation need not be incorporated into the data but must be maintained in some manner by the information broker.

Section 2(c)(3)(B)(iii) provides limitations to the access rights under section 2(c)(3)(B)(i). An information broker may limit access to information if access of the individual to the information is limited by law or a legally recognized privilege, or if the information is used for a legitimate governmental or fraud prevention purpose that would be compromised by access. The Committee recognizes that databases that are used to verify an individual's identity for antifraud purposes provide significant benefits to law enforcement, business, and consumers, and that access to such databases could undermine the usefulness of the data as a tool against fraud. Section 2(c)(3)(B)(iv) requires the FTC to issue regulations, as necessary, to implement the limitations in clause (iii) of this section.

Section 2(c)(3)(C) permits the Commission to promulgate rules to determine to be in compliance with Section 2(c)(3) any consumer reporting agency (CRA) in compliance with the requirements of the Fair Credit Reporting Act (FCRA) with respect to those products and services that are subject to FCRA.

Section 2(c)(4) requires the FTC to promulgate regulations to require information brokers to establish an audit log for accessed and transmitted information. The Committee intends these logs to be used as a law enforcement tool in investigating security breaches.

Section 2(c)(5) prohibits pretexting for personal information by information brokers. It also prohibits an information broker from soliciting another to pretext for personal information.

Section 2(d) provides an exemption from the requirements of Section 2 for any electronic communication by a third party stored by a telecommunications carrier, cable operator, information service, or interactive computer service.

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, following the discovery of a breach of security, the individuals whose information was acquired by an unauthorized person and the FTC.

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. For example, receipt of a notice from a data processing entity, whose company name the recipient may have never heard, would not alert the consumer in the same manner or produce the same reaction as a notice from the entity with whom the consumer has an existing 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. The Committee understands that it is necessary for affected entities to take such measures after discovery of a breach and prior to notification, but the Committee expects that an entity that discovers a breach will prioritize its resources in order to take such measures as expeditiously as possible so as not to unreasonably delay the provision of nay required notifications. 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(d)(1)(B) establishes the minimum content of the notification to the individual shall include: (1) a description of the personal information acquired by the unauthorized person; (2) a free telephone number for the individual to contact the entity regarding the breach of security or the information maintained about that individual; and (3) notice that the individual is entitled to receive free credit reports quarterly for two years and instructions for the individual to receive such reports; (4) the toll free telephone numbers and contact addresses for the major credit reporting agencies; and (5) a toll free number and Internet website address for the FTC.

Section 3(d)(2) establishes circumstances that give rise to a substitute notification in lieu of direct notification under Section 3(d)(1) and provides for the form of such substitute notice. A person may provide substitute notice if the person owns or possesses personal information on fewer than 1000 individuals and such direct notification is not feasible due to either excessive cost to the person relative to their resources as determined by the Commission or the person's lack of sufficient contact information for the individual. The Committee intends this provision to be used in recognition that small businesses often may not have the resources or ability to comply with the direct notification requirements. For example, establishing a toll free telephone number may not be commensurate with the resources of the person or the number of individuals affected by a breach.

The form of the substitute notice shall include email to those individuals that have an email address, notice on the entity's Internet website, and notice in print and to broadcast media. Additionally, the content of the substitute notice must include notice regarding the provision of free quarterly credit reports in the same manner as required in direct notification as well as a free telephone number for individuals to inquire whether their information was breached.

Under Section 3(d)(3), the FTC is required to promulgate regulations within nine months after the date of enactment of the Act to establish criteria for which substitute notice may be given. The Commission shall also publish guidance for compliance with both the written and email notification and the content of substitute notice.

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 one of the major credit reporting agencies, and at no cost to the individual, upon request from the individual. The Committee recognizes the evolving nature of the marketplace for products and services to help consumers after a data breach. This provision in no way is intended to limit the provision of any post-breach product or service, in addition to the quarterly credit reports, that is determined to provide effective protection to consumers from identity theft, fraud, or other unlawful conduct.

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. The Committee intends that the person making the determination, and the FTC or States in considering enforcement actions, will look to a reasonable time period following the breach when considering whether the encryption is "likely to be compromised."

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 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. §§ 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). In particular, the Committee does not intend that State or local government agencies be subject to the requirements of this Act. Any person who violates FTC regulations promulgated under this Act shall be subject to the same penalties and subject to the same privileges and immunities provided in the FTC 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. In determining the number of days that a person is not in compliance with a requirement of section 2, the Committee intends the count to begin with the day the person is first notified of noncompliance by an entity authorized to enforce this Act.

With respect to a violation of section 3, the civil penalty is calculated by multiplying the number of violations of section 3 by an amount not greater than $11,000, with each failure to send notice to a resident of a State treated as a separate violation. Civil penalties for violations of section 3 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. The Committee intends for enforcement by the States to be an important supplement to Federal enforcement and therefore discourages the States from bringing the same cause of action against the same actors against whom the FTC has enforced the Act.

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 5. Definitions

Section 5 contains the definitions that apply to the Act. "Breach of security" is defined under paragraph (1) as the unauthorized acquisition of data in electronic form containing personal information. The Committee notes the inclusion of an exemption from notification requirements in section 3. Under the exemption, entities that determine there is no reasonable risk of identity theft, fraud or other unlawful conduct after discovering a breach of security are not required to comply with the notification provisions of section 3.

Paragraph (3) defines "data in electronic form" as any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices. The Committee intends the definition to be inclusive of data on removable and portable storage devices.

Paragraph (4) defines "encryption" as the protection of data in electronic form in storage or transit using an encryption technology that has been adopted by an established standards setting body and which renders such data indecipherable in the absence of associated cryptographic keys necessary to decrypt the data. To meet the definition, encryption must be accompanied by appropriate management and safeguards of such cryptographic keys to protect the integrity of the encryption. The Committee intends the definition, when read in conjunction with the authority of the FTC to determine other technologies or methods which render electronic data indecipherable or unreadable as qualifying for the rebuttable presumption in section 3(f), to be technology neutral.

"Identity theft" is defined in paragraph (5) as the unauthorized use of another person's personal information to engage in commercial transactions under the name of the person. While identify theft has predominantly been account fraud, the Committee intends to capture other equally harmful actions that occur in commerce that do not constitute account fraud.

Paragraph (6) defines an information broker for purposes of this Act. Specifically, an information broker is 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 and do so in order to sell such information or provide access to such information to any non-affiliated third party in exchange for consideration. The definition further states that an entity is an information broker regardless of whether it collects, assembles, or maintains the personal information directly or by contract with another entity. This further clarification is to ensure an entity cannot avoid the responsibilities and obligations of an information broker by contracting out those functions that would otherwise make the entity an information broker.

The Committee does not intend the definition to apply to third party agents that act as data processors. The Committee also notes that a number of technology companies, particularly application service providers (ASP), provide processing and analytical services to customers. In a typical arrangement, an ASP provides a customer access to a database pursuant to a contract or license. The data in the database is either supplied by the customer or by a third party entity specifically on the customer's behalf. In such a scenario, the fee is not consideration for data but for the service and software provided by the ASP. In such cases, an ASP may also be required by contract to provide access to a third party on behalf of its client. This scenario and similar ASP arrangements in which a fee is paid to access software functionality are not intended to be covered by the definition of information broker.

Additionally, the Committee recognizes that Internet search engines identify, catalog, and organize information contained on publicly accessible sites located on the World Wide Web. As a result of this activity, an Internet search engine may collect information that is on a publicly accessible Web site, which in turn becomes available to an Internet user who performs a search query. The Committee recognizes that there may be occasions when the publicly available Web site contains information that might qualify as personal information, however, the Committee does not intend that such routine search engine activity would result in the search engine being considered an "information broker" under the legislation.

Paragraph (7) defines personal information based on a combination of publicly available information, such as first name or initial and last name, address, or phone number and non-public personal identifiers such as social security number, financial account number and a required access or security code (e.g., a PIN), or driver license number or other state-issued identification number. The Committee determined this information, were it breached, could place the individuals whose information was breached at risk of identity theft, fraud, or other unlawful conduct. Given today's technology and the information available, a few sensitive data elements, once acquired, may be used to obtain further information necessary to commit identity theft, fraud, or other unlawful conduct.

The Committee recognizes the definition of personal information may need to be modified in the future in response to changing technology or practices. The FTC is permitted to modify the definition by rule under paragraph (7)(B) of this Section, such that it does not unreasonably impede interstate commerce but will accomplish the purposes of the Act. The Committee intends that any information the Commission adds to the definition of personal information must be information, if acquired in combination with a first name or initial and last name, address, or phone number, is sufficient to effectuate identity theft, fraud, or other unlawful acts.

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 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.

Section 7. Effective date and sunset

Section 7 provides that, except as otherwise provided in the Act, the Act shall take effect one year after the date of enactment. Section 7 also provides for a sunset of the bill 10 years from the date of enactment.

Section 8. Authorization of appropriations

Section 8 authorizes to be appropriated to the FTC $1 million for each of fiscal years 2006 through 2010 to carry out the Act.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

This legislation does not amend any existing Federal statute.

○