111TH CONGRESS } HOUSE OF REPRESENTATIVES { REPORT
1st Session } { 111–362

DATA ACCOUNTABILITY AND TRUST ACT

DECEMBER 8, 2009.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. WAXMAN, from the Committee on Energy and Commerce, submitted the following

R E P O R T

[To accompany H.R. 2221]

[Including cost estimate of the Congressional Budget Office]

The Committee on Energy and Commerce, to whom was referred the bill (H.R. 2221) 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 amendments and recommend that the bill as amended do pass.

CONTENTS

89–006

AMENDMENT

The amendments are 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".

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 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 or systems maintained by such person that contains such data, which shall include regular monitoring for a breach of security of such system or systems.

(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 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.

(F) A standard method or methods for the destruction of paper documents and other non-electronic data containing personal information.

(3) TREATMENT OF ENTITIES GOVERNED BY OTHER LAW.—Any person who is in compliance with any other Federal law that requires such person to maintain standards and safeguards for information security and protection of personal information that, taken as a whole and as the Commission shall determine in the rulemaking required under paragraph (1), provide protections substantially similar to, or greater than, those required under this subsection, shall be deemed to be in compliance with this subsection.

(b) SPECIAL REQUIREMENTS FOR INFORMATION BROKERS.—

(1) SUBMISSION OF POLICIES TO THE FTC.—The regulations promulgated under subsection (a) shall require each information broker to submit its 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 may conduct audits of the information security practices of such information broker, or require the information broker to conduct independent audits of such practices (by an independent auditor who has not audited such information broker's security practices during the preceding 5 years).

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

(A) ACCURACY.—

(i) IN GENERAL.—Each information broker shall establish reasonable procedures to assure the maximum possible 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.

(ii) LIMITED EXCEPTION FOR FRAUD DATABASES.—The requirement in clause (i) shall not prevent the collection or maintenance of information that may be inaccurate with respect to a particular individual when that information is being collected or maintained solely—

(I) for the purpose of indicating whether there may be a discrepancy or irregularity in the personal information that is associated with an individual; and

(II) to help identify, or authenticate the identity of, an individual, or to protect against or investigate fraud or other unlawful conduct.

(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), and, as applicable, how to express a preference with respect to the use of personal information for marketing purposes under clause (iii).

(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 and, if the individual provides proof that the public record has been corrected or that the information broker was reporting the information incorrectly, correct the inaccuracy in the information broker's records; 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) ALTERNATIVE PROCEDURE FOR CERTAIN MARKETING INFORMATION.—In accordance with regulations issued under clause (v), an information broker that maintains any information described in clause (i) which is used, shared, or sold by such information broker for marketing purposes, may, in lieu of complying with the access and dispute requirements set forth in clauses (i) and (ii), provide each individual whose information it maintains with a reasonable means of expressing a preference not to have his or her information used for such purposes. If the individual expresses such a preference, the information broker may not use, share, or sell the individual's information for marketing purposes.

(iv) LIMITATIONS.—An information broker may limit the access to information required under subparagraph (B)(i)(I) and is not required to provide notice to individuals as required under subparagraph (B)(i)(II) 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.

(III) If the information consists of a published media record, unless that record has been included in a report about an individual shared with a third party.

(v) RULEMAKING.—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 carry out this paragraph and to facilitate the purposes of this Act. In addition, the Commission shall issue regulations, as necessary, under section 553 of title 5, United States Code, on the scope of the application of the limitations in clause (iv), including any additional circumstances in which an information broker may limit access to information under such clause that the Commission determines to be appropriate.

(C) FCRA REGULATED PERSONS.—Any information broker who is engaged in activities subject to the Fair Credit Reporting Act and who is in compliance with sections 609, 610, and 611 of such Act with respect to information subject to such Act, shall be deemed to be in compliance with this paragraph with respect to such information.

(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 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 subparagraph (A).

(c) EXEMPTION FOR CERTAIN SERVICE PROVIDERS.—Nothing in this section shall apply to a service provider for any electronic communication by a third party that is transmitted, routed, or stored in intermediate or transient storage by such service provider.

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 or accessed as a result of such a breach of security; and

(2) notify the Commission.

(b) SPECIAL NOTIFICATION REQUIREMENTS.—

(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 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) SERVICE PROVIDERS.—If a service provider becomes aware of a breach of security of data in electronic form containing personal information that is owned or possessed by another person that connects to or uses a system or network provided by the service provider for the purpose of transmitting, routing, or providing intermediate or transient storage of such data, such service provider shall be required to notify of such a breach of security only the person who initiated such connection, transmission, routing, or storage if such person

can be reasonably identified. Upon receiving such notification from a service provider, such person shall provide the notification required under subsection (a).

(3) COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.—If a person is required to provide notification to more than 5,000 individuals under subsection (a)(1), the person shall also notify the major credit reporting agencies that compile and maintain files on consumers on a nationwide basis, of the timing and distribution of the notices. Such notice shall be given to the credit reporting agencies without unreasonable delay and, if it will not delay notice to the affected individuals, prior to the distribution of notices to the affected individuals.

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—Unless subject to a delay authorized under paragraph (2), a notification required under subsection (a) shall be made not later than 60 days following the discovery of a breach of security, unless the person providing notice can show that providing notice within such a time frame is not feasible due to extraordinary circumstances necessary to prevent further breach or unauthorized disclosures, and reasonably restore the integrity of the data system, in which case such notification shall be made as promptly as possible.

(2) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—

(A) LAW ENFORCEMENT.—If a Federal, State, or local law enforcement agency determines that the notification required under this section would impede a civil or criminal investigation, such notification shall be delayed upon the written request of the law enforcement agency for 30 days or such lesser period of time which the law enforcement agency determines is reasonably necessary and requests in writing. A law enforcement agency may, by a subsequent written request, revoke such delay or extend the period of time set forth in the original request made under this paragraph if further delay is necessary.

(B) NATIONAL SECURITY.—If a Federal national security agency or homeland security agency determines that the notification required under this section would threaten national or homeland security, such notification may be delayed for a period of time which the national security agency or homeland security agency determines is reasonably necessary and requests in writing. A Federal national security agency or homeland security agency may revoke such delay or extend the period of time set forth in the original request made under this paragraph by a subsequent written request if further delay is necessary.

(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) Notification by email or other electronic means , if—

(I) the person's primary method of communication with the individual is by email or such other electronic means; 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 or accessed 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, or credit monitoring or other service that enables consumers to detect the misuse of their personal information for a period of 2 years, and instructions to the individual on requesting such reports or service from the person, except when the only information which has

been the subject of the security breach is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code;

(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 the person owns or possesses data in electronic form containing personal information of fewer than 1,000 individuals and 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 NOTIFICATION.—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, or credit monitoring or other service that enables consumers to detect the misuse of their personal information for a period of 2 years, and instructions on requesting such reports or service from the person, except when the only information which has been the subject of the security breach is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code; 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) REGULATIONS AND GUIDANCE.—

(A) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall, by regulation under section 553 of title 5, United States Code, establish criteria for determining 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 costs to the person required to provided such notification relative to the resources of such person. Such regulations may also identify other circumstances where substitute notification would be appropriate for any person, including circumstances under which the cost of providing notification exceeds the benefits to consumers.

(B) GUIDANCE.—In addition, the Commission shall provide and publish general guidance with respect to compliance with this subsection. 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), including the extent of notification to print and broadcast media that complies with the requirements of such paragraph.

(e) OTHER OBLIGATIONS FOLLOWING BREACH.—

(1) IN GENERAL.—A person required to provide notification under subsection (a) shall, upon request of an individual whose personal information was in-

cluded in the breach of security, provide or arrange for the provision of, to each such individual and at no cost to such individual—

(A) consumer credit reports from at least one of the major credit reporting agencies beginning not later than 60 days following the individual's request and continuing on a quarterly basis for a period of 2 years thereafter; or

(B) a credit monitoring or other service that enables consumers to detect the misuse of their personal information, beginning not later than 60 days following the individual's request and continuing for a period of 2 years.

(2) LIMITATION.—This subsection shall not apply if the only personal information which has been the subject of the security breach is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code.

(3) RULEMAKING.—As part of the Commission's rulemaking described in subsection (d)(3), the Commission shall determine the circumstances under which a person required to provide notification under subsection (a)(1) shall provide or arrange for the provision of free consumer credit reports or credit monitoring or other service to affected individuals.

(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) PRESUMPTION.—

(A) IN GENERAL.—If the data in electronic form containing personal information is rendered unusable, unreadable, or indecipherable through encryption or other security technology or methodology (if the method of encryption or such other technology or methodology is generally accepted by experts in the information security field), there shall be 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 or other security technologies or methodologies in a specific case, have been or are reasonably likely to be compromised.

(B) METHODOLOGIES OR TECHNOLOGIES.—Not later than 1 year after the date of the enactment of this Act and biannually thereafter, the Commission shall issue rules (pursuant to section 553 of title 5, United States Code) or guidance to identify security methodologies or technologies which render data in electronic form unusable, 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 in a specific case has been or is reasonably likely to be compromised. In issuing such rules or guidance, 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) GENERAL RULEMAKING AUTHORITY.—The Commission may promulgate regulations necessary under section 553 of title 5, United States Code, to effectively enforce the requirements of this section.

(j) TREATMENT OF PERSONS GOVERNED BY OTHER LAW.—A person who is in compliance with any other Federal law that requires such person to provide notification to individuals following a breach of security, and that, taken as a whole, provides protections substantially similar to, or greater than, those required under this section, as the Commission shall determine by rule (under section 553 of title 5, United States Code), shall be deemed to be in compliance with this section.

SEC. 4. APPLICATION AND ENFORCEMENT.

(a) GENERAL APPLICATION.—The requirements of sections 2 and 3 shall only apply to those persons, partnerships, or corporations over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act.

(b) 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. 57a(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.

(c) 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 days that a person is not in compliance with such section by an amount not greater than $11,000.

(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.

(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.

(C) MAXIMUM TOTAL LIABILITY.—Notwithstanding the number of actions which may be brought against a person under this subsection the maximum civil penalty for which any person may be liable under this subsection shall not exceed—

(i) $5,000,000 for each violation of section 2; and

(ii) $5,000,000 for all violations of section 3 resulting from a single breach of security.

(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.

(d) AFFIRMATIVE DEFENSE FOR A VIOLATION OF SECTION 3.—

(1) IN GENERAL.—It shall be an affirmative defense to an enforcement action brought under subsection (b), or a civil action brought under subsection (c), based on a violation of section 3, that all of the personal information contained in the data in electronic form that was acquired or accessed 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.

(2) NO EFFECT ON OTHER REQUIREMENTS.—Nothing in this subsection shall be construed to exempt any person from the requirement to notify the Commission of a breach of security as required under section 3(a).

SEC. 5. DEFINITIONS.

In this Act the following definitions apply:

(1) BREACH OF SECURITY.—The term "breach of security" means unauthorized access to or 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"—

(A) 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; and

(B) does not include a commercial entity to the extent that such entity processes information collected by and received from a nonaffiliated third party concerning individuals who are current or former customers or employees of such third party to enable such third party to (1) provide benefits for its employees or (2) directly transact business with its customers.

(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, passport number, military identification number, or other similar number issued on a government document used to verify identity.

(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 promulgated under section 553 of title 5, United States Code, modify the definition of "personal information" under subparagraph (A)—

(i) for the purpose of section 2 to the extent that such modification will not unreasonably impede interstate commerce, and will accomplish the purposes of this Act; or

(ii) for the purpose of section 3, 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.

(10) SERVICE PROVIDER.—The term "service provider" means an entity that provides to a user transmission, routing, intermediate and transient storage, or connections to its system or network, for electronic communications, between or among points specified by such user of material of the user's choosing, without modification to the content of the material as sent or received . Any such entity shall be treated as a service provider under this Act only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage or connections.

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 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 access to or acquisition of data in electronic form containing personal information.

(b) ADDITIONAL PREEMPTION.—

(1) IN GENERAL.—No person other than a person specified in section 4(c) 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.

SEC. 7. EFFECTIVE DATE.

This Act shall take effect 1 year after 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 2010 through 2015 to carry out this Act.

Amend the title so as to read:

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

PURPOSE AND SUMMARY

H.R. 2221, the "Data Accountability and Trust Act", was introduced on April 30, 2009, by Reps. Bobby L. Rush (D–IL), Cliff Stearns (R–FL), Joe Barton (R–TX), George Radanovich (R–CA), and Janice Schakowsky (D–IL). The goal of H.R. 2221 is to both reduce the number of data breaches and provide new rights to individuals whose personal information is compromised when a breach occurs. The bill has two major requirements: (1) an entity holding data containing personal information must adopt reasonable and appropriate security measures to protect such data; and (2) that same entity must notify affected consumers in the event of a breach unless the entity determines there is "no reasonable risk of identity theft, fraud, or other unlawful conduct." In addition, the bill requires information brokers to implement reasonable procedures that will ensure data accuracy and provide consumers with access to information and the ability to dispute inaccurate information in certain circumstances.

BACKGROUND AND NEED FOR LEGISLATION

Data breaches can severely compromise the financial well-being of individuals whose personal information is exploited to commit identity theft or fraud. Despite increased publicity surrounding high-profile data breaches, enforcement by the Federal Trade Commission (FTC), and ongoing calls for better data security from Congress and other governmental bodies, data breaches continue at an alarming pace. According to the Privacy Rights Clearinghouse, almost 340 million records containing "sensitive personal information" have been "involved in security breaches since January 2005." [1]

Data breaches have an impact on every sector of the economy. High-profile data breaches have plagued financial institutions, nationwide retailers, online merchants, information brokers, credit card processors, healthcare institutions, high-tech companies, research facilities, and government agencies. The causes of these breaches range from high-tech hacking and skimming to dumpster diving and simple laptop theft.

Data breaches can result in substantial harm to consumers. Personal information that is lost or compromised may be exploited by criminals to commit identity theft, fraud, or other unlawful conduct. According to the FTC's most recent identity theft survey, approximately 8.3 million American adults—3.7% of all American adults—discovered that they were victims of identity theft in 2005.[2] By some estimates, identity theft is the fastest growing type of fraud in the United States.[3] Moreover, although identity theft often is associated with financial transactions, it also can take place in other contexts. For example, thieves can steal identities to gain employment, immigrate into this country, obtain medical care, apply for benefits, and evade law enforcement.

---

[1] Privacy Rights Clearinghouse, A Chronology of Data Breaches (online at *www.privacyrights.org/ar/ChronDataBreaches.htm*) (accessed Oct. 6, 2009).

[2] See Federal Trade Commission, Identity Theft Survey Report, prepared by Synovate, at 3 (2007) www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

[3] Congressional Research Service, Identity Theft: Trends and Issues, at 1 (Aug. 2009) (CRS–R40599).

The best way to prevent identity theft and other harm is for individuals and businesses to properly secure personal information so that it does not fall into the wrong hands in the first place. Currently, several laws address data security requirements for narrow categories of information or specific sectors of the marketplace. These laws include the Gramm-Leach-Bliley Act ("GLB Act") Safeguards Rule,[4] which contains data security requirements for financial institutions and the Fair Credit Reporting Act ("FCRA") Disposal Rule,[5] which imposes safe disposal obligations on entities that maintain consumer report information. In addition, FTC has used its enforcement authority under the FTC Act[6] to bring actions against companies that have made misleading claims about data security procedures or failed to employ reasonable security measures in circumstances that caused substantial injury. There is no comprehensive federal law, however, that requires all companies that hold consumer personal information to implement reasonable measures to protect that data.

Also, there is no federal law that requires companies that experience a data breach to provide notice to those consumers whose personal information was compromised. Consumers need to know when their sensitive information has been compromised in order to detect and prevent identity theft, fraud, or other unlawful conduct. Timely notice allows consumers to take concrete steps to prevent identity theft such as cancelling accounts or requesting new account numbers, monitoring accounts for unusual activity, and placing alerts on credit reports. Victims of identity theft can spend countless hours attempting to fix the myriad problems that can result from the misuse of personal information. Notice, as well as the provision of services to help consumers monitor their accounts for suspicious activity, would aid consumers with the arduous task of preventing and/or recovering from identity theft.

H.R. 2221 is a comprehensive information security regime that will require all companies subject to FTC jurisdiction to implement an information security program to safeguard personal information. This program is applicable to personal information stored electronically and in paper records and would require companies to engage in an ongoing process of evaluating risks and taking reasonable measures to address those risks.

H.R. 2221 also requires companies that experience a data breach to provide consumers with timely notice of the breach so that consumers can take steps to prevent harm. The bill creates uniform, nationwide standards for breach notification for all entities subject to FTC jurisdiction. The bill further requires companies to provide individuals with free monitoring services to detect the misuse of their personal information following a breach.

In addition to the information security and breach notification requirements that apply to all entities subject to FTC jurisdiction, H.R. 2221 includes additional requirements for information brokers, those companies that are in the business of collecting personal information for the purpose of selling it to third parties.

---

[4] 16 CFR Part 314, implementing 15 U.S.C. section 6801(b).
[5] 16 CFR Part 682, implementing 15 U.S.C. section 1681w.
[6] 15 U.S.C. section 45(a).

LEGISLATIVE HISTORY

The Data Accountability and Trust Act originally was introduced as H.R. 4127 in the 109th Congress on October 25, 2005, by Rep. Stearns, who was then Chairman of the Subcommittee on Commerce, Trade, and Consumer Protection. In the 109th Congress, the Subcommittee on Commerce, Trade, and Consumer Protection held two oversight hearings on data breaches, data security, and information brokers, as well as a legislative hearing on a discussion draft of H.R. 4127. The Subcommittee considered H.R. 4127 in markup session and forwarded the bill, amended, to the full Committee on November 3, 2005. On March 29, 2006, the Committee on Energy and Commerce met in open markup session and ordered H.R. 4127 reported to the House, as amended, by a recorded vote of 41 yeas and 0 nays.

In the 110th Congress, H.R. 958 was introduced by Rep. Bobby L. Rush, Chairman of the Subcommittee on Commerce, Trade, and Consumer Protection, with the same language of the bill that passed out of the Committee in the previous Congress.

COMMITTEE CONSIDERATION

In the 111th Congress, Subcommittee Chairman Rush, on behalf of himself, Reps. Stearns, Barton, Radanovich, and Schakowsky, reintroduced the bill as H.R. 2221 on April 30, 2009. The bill was referred to the Subcommittee on Commerce, Trade, and Consumer Protection on May 1, 2009. The Subcommittee held a legislative hearing on H.R. 2221 on May 5, 2009. Testimony was heard from witnesses representing the Bureau of Consumer Protection of the Federal Trade Commission; the Center for Democracy and Technology; the Business Software Alliance; the Distributed Computing Data Industry Association; the Electronic Privacy Information Center; Tiversa, Inc.; and the Center for the Study of Digital Property of the Progress & Freedom Foundation.

On June 3, 2009, the Subcommittee met in open markup session to consider H.R. 2221. The Subcommittee subsequently forwarded H.R. 2221, amended, to the full Committee by a voice vote.

The Committee on Energy and Commerce met in open markup session on September 30, 2009, and considered H.R. 2221 as forwarded by the Subcommittee on June 3, 2009. The Committee adopted a manager's amendment to the bill by a voice vote. The full Committee then ordered H.R. 2221 favorably reported to the House, amended, by a voice vote.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto. A motion by Mr. Waxman to order H.R. 2221 favorably reported to the House, amended, was agreed to by a voice vote. There were no recorded votes taken during consideration and passage of H.R. 2221.

STATEMENT OF COMMITTEE OVERSIGHT FINDINGS AND RECOMMENDATIONS

In compliance with clause 3(c)(1) of rule XIII and clause (2)(b)(1) of rule X of the Rules of the House of Representatives, the over-

sight findings and recommendations of the Committee are reflected in the descriptive portions of this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

Pursuant to clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the estimate of budget authority and revenues regarding H.R. 2221 prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974. The Committee finds that H.R. 2221 would result in no new or increased entitlement authority, or tax expenditures or revenues.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

In accordance with clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the performance goals and objectives of the Committee are reflected in the descriptive portions of this report.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee must include a statement citing the specific powers granted to Congress to enact the law proposed by H.R. 2221. Article I, section 8, clauses 3 and 18 of the Constitution of the United States grants the Congress the power to enact this law.

EARMARKS AND TAX AND TARIFF BENEFITS

H.R. 2221 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9 of rule XXI of the Rules of the House of Representatives.

FEDERAL ADVISORY COMMITTEE STATEMENT

The Committee finds that the legislation does not establish or authorize the establishment of an advisory committee within the definition of 5 U.S.C. App., section 5(b) of the Federal Advisory Committee Act.

APPLICABILITY OF LAW TO THE LEGISLATIVE BRANCH

Section 102(b)(3) of Public Law 104–1 requires a description of the application of this bill to the legislative branch where the bill relates to terms and conditions of employment or access to public services and accommodations.

H.R. 2221 requires commercial entities subject to Federal Trade Commission jurisdiction that own or posses personal information to adopt reasonable and appropriate security measures to protect such data and, in the event such information is breached, that same entity must notify affected consumers of the breach of security. This bill does not relate to employment or access to public services and accommodations in the legislative branch.

FEDERAL MANDATES STATEMENT

Section 423 of the Congressional Budget and Impoundment Control Act of 1974 (as amended by section 101(a)(2) of the Unfunded

Mandates Reform Act, P.L. 104–4) requires a statement on whether the provisions of the report include unfunded mandates. In compliance with this requirement the Committee adopts as its own the estimates of federal mandates prepared by the Director of the Congressional Budget Office.

COMMITTEE COST ESTIMATE

Pursuant to clause 3(d)(2) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the cost estimate of H.R. 2221 prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the Congressional Budget Act of 1974 and with respect to requirements of clause (3)(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the Congressional Budget Act of 1974, the Committee has received the following cost estimate for H.R. 2221 from the Director of Congressional Budget Office:

DECEMBER 7, 2009.

Hon. HENRY A. WAXMAN,
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. 2221, the Data Accountability and Trust Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Susan Willie.

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

H.R. 2221—Data Accountability and Trust Act

Summary: H.R. 2221 would establish new requirements to protect the personal information of individuals that is collected and maintained by commercial entities. The bill would require companies to adopt procedures to protect personal information from improper access, anticipate and mitigate potential vulnerabilities in security systems intended to prevent improper access, and specify methods for disposing of data that is held in electronic and nonelectronic form. H.R. 2221 would require data brokers (entities that collect and maintain personal information for sale to others) to submit their data security policies to the Federal Trade Commission (FTC) and to establish procedures that consumers may follow to review and, if necessary, dispute the accuracy of their personal data. Finally, the bill would require entities covered by the bill to notify individuals when their personal information has been improperly accessed as the result of a breach of security. H.R. 2221 would require the FTC to develop regulations to implement and enforce the new requirements.

Assuming appropriation of the authorized amounts, CBO estimates that implementing H.R. 2221 would cost $5 million over the 2010–2014 period to develop and enforce the new regulations. Enacting H.R. 2221 could increase federal revenues from additional civil penalties assessed for violations of laws related to information security. CBO estimates that any additional revenues would not be significant because of the relatively small number of cases expected to be involved. Enacting H.R. 2221 would not affect direct spending.

H.R. 2221 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates that those mandates would impose no costs on state, local, or tribal governments.

H.R. 2221 would impose several private-sector mandates as defined in UMRA by requiring certain entities engaged in interstate commerce to establish policies and procedures to keep personal information secure and to notify affected individuals in the event of a security breach. The bill also would impose new requirements on information brokers related to data collection and accuracy.

Much of the industry already complies in large part with the many of the bill's requirements. However, some of the requirements in the bill would impose new security standards and notification procedures on millions of entities in the private sector. Based on this information, CBO estimates that the aggregate direct cost of the mandates in the bill would exceed the annual threshold established in UMRA for private-sector mandates ($139 million in 2009, adjusted annually for inflation) in at least one of the first five years the mandates are in effect.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 2221 is shown in the following table. The costs of this legislation fall within budget function 370 (commerce and housing credit).

	By fiscal year, in millions of dollars—					
	2010	2011	2012	2013	2014	2010–2014
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Authorization Level	1	1	1	1	1	5
Estimated Outlays	1	1	1	1	1	5

Basis of estimate: For this estimate, CBO assumes that the bill will be enacted early in calendar year 2010 and that the $1 million authorized to be appropriated for each of fiscal years 2010 through 2015 will be provided for each year. CBO estimates that implementing H.R. 2221 would cost $5 million over the 2010–2014 period for the FTC to issue regulations and enforce the bill's provisions. Enacting the legislation would not have a significant effect on revenues and would not affect direct spending.

Estimated impact on state, local, and tribal governments: H.R. 2221 contains intergovernmental mandates as defined in UMRA. It would preempt state and local laws that require entities that experience security breaches to notify persons whose information is comprised. The bill also would preempt state and local laws that require entities to implement security practices for handling personal information. CBO estimates that because the preemptions

would only limit the application of state law, the mandate would impose no costs on state, local, or tribal governments.

Estimated impact on the private sector: H.R. 2221 would impose several private-sector mandates as defined in UMRA. It would require entities engaged in interstate commerce that own or possess personal information to implement policies and procedures to keep personal information secure, and to notify individuals when their personal information has been compromised as a result of a security breach. The bill also would require information brokers to establish procedures to verify the accuracy of the data they maintain on individuals and allow those individuals to review and correct their files.

Much of the industry already complies in large part with the many of the bill's requirements. However, this legislation would impose new information security requirements and notification procedures and practices on millions of private-sector entities. It also would broaden the definition of "personal information" and expand the circumstances under which businesses must notify individuals of a breach of their information as compared to current law. Based on information from the FTC and industry sources, CBO estimates that the aggregate cost of the mandates in the bill would exceed the annual threshold established in UMRA for private-sector mandates ($139 million in 2009, adjusted annually for inflation) in at least one of the first five years that the mandates are in effect.

Requirements for information security

Section 2 of the bill would require certain entities that own or possess personal information, that are engaged in interstate commerce, or that contract a third party to maintain such data, to establish and implement information security policies and procedures in compliance with regulations to be set by the FTC. Personal information, as defined in the bill, is an individual's first name or initial and last name, or address, or phone number, in combination with any one or more of the following: the individual's social security number, driver's license number, passport number or similar identification number issued on a government document, or a financial account number or credit card number and any security or access code needed to access the account.

Covered entities would have to implement a security policy with respect to the use, sale, dissemination, and maintenance of data and conduct periodic vulnerability testing on their security programs. Additionally, those entities would have to identify an officer responsible for the oversight of the information security. Entities also would have to implement a process for disposing of obsolete electronic and non-electronic data containing personal information. Some businesses could be determined by the FTC to be in compliance with the requirements of section 2 if they are currently in compliance similar federal regulations to maintain standards and safeguards for information security.

The cost of compliance for the data privacy and security requirements would depend on the rules to be established by the FTC, the size of the entity, and the amount of personal information maintained by the entity. Most businesses are already subject to state or other federal laws regulating security policies, and it is the current practice of many businesses to use security measures to pro-

tect sensitive data. However, state laws generally use a more narrow definition of personal information than would apply under the bill. The bill's requirements would apply to varying degrees to millions businesses who own, use, or maintain personal information. Even though the incremental cost per entity of implementing the information security requirements in the bill could be small, the aggregate cost of compliance could be substantial.

Notification of information security breach

Section 3 would require a covered entity that owns or possesses data in electronic form containing personal information to notify individuals and the FTC following a security breach in which such individuals' personal information was accessed or acquired by an unauthorized person. The bill also includes special notification requirements for third party agents and internet service providers.

Notification would have to be written or, in some circumstances, could be sent via email. The bill allows for substitute notification, through postings on the entity's Web site and in print and broadcast media, when the person experiencing the breach owns or possesses the data of fewer than 1,000 individuals, or when direct notification is not feasible due to excessive cost or if the contact information for the individuals is unavailable. Both forms of notification would have to include a description of the information accessed or acquired, certain relevant telephone contact numbers, and notice of the right to receive free credit monitoring services or quarterly credit reports for two years following the breach. Entities would have to provide credit reports or credit monitoring services to individuals affected by a breach at no cost to the individual, if requested.

If the breached personal information consists of an individual's name, address, or phone number in combination with a credit or debit card number and the required security code, under the legislation, breach notification would not be required. The bill also would allow an entity to be exempt from notification requirements, if it determines that there is no reasonable risk of identity theft, fraud, or other unlawful conduct. An allowable presumption that no risk of identity theft or fraud exists includes encryption or similar modification of data so that it is rendered unreadable.

Should entities choose to reduce the likelihood of a data breach by encrypting personal information, the total cost could be substantial. Data encryption software can cost between $150 and $600 or more depending on the type of system used and the amount of data. If even a small portion of the millions of entities affected by this bill were to purchase this software, those costs could exceed the annual threshold.

In 2006, more than 17 million people's social security numbers were stolen or accessed in security breaches, none of which was encrypted. Since 2006, the number of individuals who have had their information accessed illegally has risen. This legislation would elevate other personally identifying information (such as driver's license numbers and passport IDs) to the level of a social security number for the purposes of data breach notification. Therefore, the number of individuals who would have to be notified about a breach could increase under the bill.

The majority of states already have data breach security laws in place; however those laws do not include provisions for mandatory credit monitoring services. The cost of bulk purchases of the credit monitoring services is approximately $60 per person, per year, according to credit industry professionals. Historically, there has been an acceptance rate of such services of about 6 percent to 8 percent. If the large number of security breaches continues, in spite of the requirements for information security programs and encryption, the cost of the notification requirements could be significant.

Special requirements for information brokers

Security Systems Audit. Information Brokers (companies whose business is to collect, assemble, maintain and sell information about individuals who are not their customers) would be required to submit their information-security policies to the FTC for review upon request or accompanying notification of breach of security. As a part of their information security requirements, following a breach in security, information brokers would be required to allow the FTC to conduct a post-breach audit of their security systems, or to have an independent auditor brought in to review the system.

According to industry experts, the cost of a security audit can range from $10,000 to more than $100,000 depending on the thoroughness of the audit and the type of systems being tested. Only 26 audits were required by the FTC between 2001 and 2009. However, the scope of what constitutes a breach could be broadened under the bill, so the number of audits may increase upon enactment of this legislation.

Maintaining the Accuracy of Information. Information brokers would also be required to establish accuracy standards for the personal information they broker. The bill would require information brokers annually to provide individuals with their personal information at no cost. The individual would then have to be given the right to dispute any information held by the broker. If that information is found to be incorrect, information brokers who do not use their data for marketing purposes would be obliged to correct the inaccuracy and, in certain cases, to provide the individual with the source of the data. Information brokers who do use data for marketing purposes would be required to allow individuals to decide how their information should be used.

The cost of providing records upon request depends on the costs of gathering and distributing the information to individuals and the number of individuals requesting their information. According to information from industry sources some information brokers already correct information based on requests from individuals. Industry experts also indicate that the average cost to large information brokers that currently provide this service is about $8.50 each time a record is disclosed and information is disputed by an individual. However, the cost per record may be higher for information brokers who do not currently have systems in place to handle such disputes. Some evidence exists that many individuals' personal information housed at data brokerage firms is in part incorrect.

There were 12 million disputes that lead to investigations in 2006 and providing the means to access and dispute personal information annually could reasonably lead to an increase in the num-

ber of requests. The cost would be the incremental cost incurred by brokers as a consequence of an increase in dispute requests. According to industry leaders, there were around 30 data aggregators and 600 to 700 information brokers nationwide in 2006. Those information brokers that do not currently have the capability to resolve disputes would incur a significant cost for establishing the means to comply with this provision.

The bill would also 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. The current industry standard on data security has not reached that level. According to industry experts, information on a particular individual can be collected from several places and, for large companies, can be accessed by thousands of people from several different locations. The ability to trace each transaction of data containing personal information would be a significant enhancement of data management hardware and software for the majority of business entities. The aggregate cost of implementing such changes could be substantial.

Previous CBO estimate: On December 2, 2009, CBO transmitted a cost estimate for S. 1490, the Personal Data Privacy and security Act of 2009, as ordered reported by the Senate Committee on the Judiciary on November 5, 2009. H.R. 2221 and S. 1490 are concerned with the security of sensitive personal information and notification requirements in the event such information is disclosed to unauthorized entities. CBO estimates that implementing the provisions of S. 1490 that would require agencies to assess the security of sensitive personal information held by the government and to report to the Congress on those assessments would cost $25 million over the 2010–2014 period.

CBO determined that both H.R. 2221 and S. 1490 contain intergovernmental mandates, that would not exceed the threshold established in UMRA ($69 million in 2009, adjusted for inflation). In addition, CBO determined that both bills contain private-sector mandates that would exceed the annual threshold established in UMRA for private-sector mandates ($139 million in 2009, adjusted annually for inflation).

Estimate prepared by: Federal Costs: Susan Willie; Impact on State, Local, and Tribal Governments: Elizabeth Cove Delisle; Impact on the Private Sector: Marin Randall.

Estimate approved by: Theresa Gullo, Deputy Assistant Director for Budget Analysis.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

Section 1 provides that the short title of H.R. 2221 is the "Data Accountability and Trust Act".

Section 2. Requirements for information security

Section 2(a)(1) directs the Federal Trade Commission to promulgate rules requiring persons that own or possess "personal information" to implement security policies and procedures to safeguard that information. This requirement applies to both electronic data and paper records containing personal information. In imple-

menting the regulations under this section, H.R. 2221 directs the FTC to take into consideration: (1) the size of, and the nature, scope, and complexity of the activities engaged in by such persons; (2) the current state of the art in administrative, technical, and physical safeguards for protecting personal information; and (3) the cost of implementing such safeguards. The Committee intends that the consideration of these factors by the FTC result in reasonable procedures that are flexible, that may be implemented by different business models, and that can accommodate changes in technology and evolving best practices.

Section 2(a)(2) sets forth specific requirements for the information security policies that are to be determined by the FTC. For example, the regulations shall require each person to develop a security policy that addresses, at a minimum, the collection, use, sale, other dissemination, and maintenance of paper and electronic personal information. FTC regulations shall require each person to evaluate risks associated with different methods and points of collection for personal information, including the use of terminals or devices to swipe credit and debit cards to purchase goods at unattended locations such as vending machines and fuel pumps.

Section 2(a)(3) requires the FTC to conduct a rulemaking to determine which other federal information security statutes or rules provide protections substantially similar to, or greater than, those required under section 2(a). Any person who is in compliance with such a similar law shall be deemed to be in compliance with section 2(a) and the FTC's implementing regulations. The FTC should consider, for example, whether the information security standards promulgated pursuant to the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act meet this threshold. Although all persons subject to H.R. 2221 must adequately protect personal information, the Committee also seeks to avoid imposing duplicative, inconsistent, or overlapping data security regulations on a person subject to section 2(a) of H.R. 2221.

Section 2(b) imposes special requirements on information brokers. Information brokers, who may collect vast amounts of personal information, provide a wide array of beneficial services to businesses and government entities. Many of the data collection activities of information brokers, however, are largely unregulated.[7] The high-profile data breaches at information brokers in 2005, which sparked the initial call for this legislation, revealed the problems with the significant gaps in regulation.[8]

The distinction between information brokers and most other commercial entities is the amount of information collected, analyzed, mined, and sold, as well as the lack of transparency to consumers. Data brokers collect information from various public and private sources and use it for a wide variety of purposes. This includes the creation of marketing databases that, for the largest brokers, can be used to analyze hundreds of data elements about nearly every American. In addition, unlike retailers or banks that have direct relationships with the consumers about whom they collect information, consumers have no relationship with information brokers and

[7] See Congressional Research Service, Data Brokers: Background and Industry Overview, at 1 (May 2007) (CRS–RS22137).

[8] House Committee on Energy and Commerce, Data Accountability and Trust Act (DATA), 109th Cong., at 10 (2006) (H. Rept. 109–453, Part 1).

may not be aware that their profiles are compiled and sold. For those consumers who are concerned about their privacy and personal information, it is difficult, if not impossible, to discover who has what information about them.

Section 2(b)(1) directs the FTC to promulgate regulations that require information brokers to submit their information security policies to the FTC any time they are required to notify FTC of a breach of security under section 3. The FTC also may request that an information broker submit such policies to the FTC at any time. Section 2(b)(2) provides the FTC with the ability to conduct audits of the information security practices of an information broker that provides notice pursuant to section 3, or requires such information broker to conduct independent audits of its security practices.

Section 2(b)(3) imposes specific requirements concerning accuracy, access, and dispute resolution procedures for information brokers. Section 2(b)(3)(A) requires that an information broker establish reasonable procedures to assure the maximum possible accuracy of the personal information it collects, assembles, or maintains, and any other information it collects, assembles or maintains that specifically identifies an individual. This provision is not limited to personal information as defined in section 5, but expressly covers "any other information it collects, assembles or maintains that specifically identifies an individual." Information, however, which merely identifies an individual's name or address is excluded. This exclusion could include a marketing or mailing list. In addition, section 2(b)(3)(A), which requires "reasonable procedures" to assure information accuracy, does not require that accuracy be absolutely proven or, for example, that an information broker verify the accuracy of information obtained from public records. Moreover, clause (ii) provides a limited exception from the accuracy requirements for fraud databases.

Section 2(b)(3)(B)(i) requires information brokers to provide consumers with the ability to access information and dispute the accuracy of that information. As with the accuracy requirements in section 2(b)(3)(A), this provision is not limited to personal information, but includes any other information maintained by the information broker that specifically identifies an individual, other than information that merely identifies an individual's name or address. The information broker is required to offer access to the information once a year at no cost to the individual.

Section 2(b)(3)(B)(ii) sets forth the procedures that permit an individual to dispute the accuracy of information maintained by an information broker and the actions an information broker must take in response to such a dispute. Upon receiving a consumer request under clause (ii), an information broker must verify the identity of the requesting individual to prevent both fraudulent access to information and the fraudulent alteration of information, which could compromise the integrity of the data and result in harm

Section 2(b)(3)(B)(iii) sets forth alternate procedures the information brokers may use regarding certain marketing information. Specifically, clause (iii) provides that in accordance with regulations issued by the FTC, if information is used, shared, or sold for marketing purposes, the information broker may, in lieu of complying with the access and dispute requirements of clause (ii), provide all individuals whose information it maintains with a reason-

able means of expressing a preference not to have his or her information used for marketing. If the individual expresses that preference, the information broker may not use, share, or sell the individual's information for marketing purposes.

Section 2(b)(3)(B)(iv) provides limitations to the access rights under clause (ii) and website notice requirements under clause (i). Although an information broker must provide conspicuous notice on its website, website notice does not apply to those specific circumstances in which an information broker may limit access to information. Databases that are used to verify an individual's identity for antifraud purposes provide significant benefits to law enforcement, business, and consumers, and access to such databases could undermine the usefulness of the data as a tool against fraud. Pursuant to clause (v), the FTC may implement rules on the scope of the limitations in clause (iv) and add additional circumstances in which an information broker may limit access to information.

Section 2(b)(3)(C) provides that if an information broker is in compliance with the relevant provisions of the Fair Credit Reporting Act (FCRA) for FCRA-covered information, the information broker shall be deemed to be in compliance with paragraph (3) with respect to that information. Thus, the information broker will not need to comply with the accuracy, access, and dispute resolution provisions of this Act. This subparagraph reflects the Committee's intent to avoid the imposition of duplicative, inconsistent, or overlapping regulations on an information broker subject to section 2(b) of H.R. 2221.

Section 2(b)(4) requires the FTC to promulgate regulations requiring information brokers to establish measures that will allow information brokers to keep track of who obtains access to personal information, such as the maintenance of chronological records or logs. Section 2(b)(5) prohibits information brokers from obtaining personal information or any other information relating to a person by pretexting—making false statements to any person for the purpose of obtaining information. It also prohibits an information broker from soliciting another to pretext for information.

Section 2(c) provides a limited exception for certain activities by service providers as that term is defined in section 5(10). Specifically, section 2(c) provides that nothing in section 2 applies to a service provider that is merely serving as the conduit for the transmission (routing or transient storage) of information. In this situation, the entity transmitting the information, the service provider, is neither the sender nor the intended recipient, did not modify the data in any way, and does not treat personal information being transmitted any differently from any other data sent over its pipes. It is the intent of the Committee that this limited exemption only applies to these specific activities where the service provider is merely serving as the conduit for the transmission of information. To the extent a service provider stores electronic personal information outside the provision of transmission or routing services, initiates or is party to a transmission of personal information, maintains paper records, or otherwise owns or possesses personal information, a service provider must comply with the requirements of section 2, unless otherwise exempt from the requirements of this bill.

Section 3. Notification of information security breach

Section 3(a) requires any person engaged in interstate commerce that owns or possesses data in electronic form to notify, following the discovery of a breach of security, the FTC and each individual whose personal information was acquired or accessed as a result of the breach. Unlike section 2, section 3 only applies to data in electronic form.

Section 3(b)(1) limits the breach notification obligations of a third party agent who, pursuant to a contractual relationship, is storing or processing personal information on behalf of another person who owns or possesses such data. In the event of a breach of security, the third party agent must provide notice of the breach to the person who owns or possesses the data. The third party agent must provide notice as soon as reasonably possible and without delay. Upon receiving such notice, the person who contracted with the third party agent and owns or possesses the data must then provide notice to consumers and the FTC pursuant to section 3(a). Section 3(b)(1) should not inhibit or supersede the parties' ability to contract for responsibility in the event of a data breach, therefore, a third party agent's duty is to notify only the owner of the data in the event of a breach, and not the owner's customers or consumers. Notice of a breach from both a third party agent and the owner of the data would be duplicative and may cause confusion for a consumer who neither recognizes nor has a direct relationship with the third party agent.

Section 3(b)(2) is a limited exception for service providers when acting solely as a conduit of personal information that is owned or possessed by another person. Section 3(b)(2) provides that if a service provider becomes aware of a breach of security of personal information that is owned or possessed by another person who uses the service provider's system or network for the purpose of transmitting, routing, or providing intermediate or transient storage of such data, the service provider only is required to notify the person who initiated the connection or transmission. Notice is required only in those cases where such person reasonably can be identified. Upon receiving notification from a service provider, such person must provide the notice required under subsection (a). Thus, section 3(b)(2) recognizes that in many cases a breach of security, during the course of transmission of information, may not always be discovered and that even when a breach is discovered, a service provider may not always be able to identify the nature of the data being transmitted or the identity of the sender of the information. To the extent a service provider otherwise experiences a breach of security, such service provider must comply with all the requirements of section 3.

Section 3(c) provides that, subject to paragraph (2), notice must be provided not later than 60 days following the discovery of the breach unless it can be shown that providing notice within 60 days is not feasible due to extraordinary circumstances necessary to prevent further breach or unauthorized disclosures and reasonably restore the integrity of the data system. In those circumstances, notice shall be provided as promptly as possible and the person providing notice shall have the burden of proving that the extraordinary circumstances warranted the delay. Paragraph (2) provides for a delay of notification for law enforcement or national security

purposes upon receipt of a written request from a law enforcement or national security agency.

Section 3(d)(1) provides for the method and content of notification. Section 3(d)(2) sets forth the circumstances under which a person may provide substitute notification in lieu of direct notification required under section 3(d)(1). This provision recognizes that small businesses may not have the resources or the ability to comply with the direct notification requirements.

Section 3(d)(3) requires the FTC to issue regulations concerning substitute notification. As part of the regulations, the FTC may identify other circumstances where substitute notification would be appropriate for any person, regardless of size or the amount of personal information held by that person, including circumstances under which the cost of providing notification exceeds the benefits to consumers.

Section 3(e) requires a person that provides notice to individuals under subsection (a) to provide or arrange for the provision of consumer credit reports, a credit monitoring service, or other service that enables consumers to detect the misuse of their personal information. An individual shall receive these services upon request, at no cost to the individual, and the services must begin not later than 60 days following the request and continue for a period of 2 years thereafter. This provision recognizes that there are a variety of products and services available that may help consumers following a breach of security and provide effective protection for consumers from the risks of identity theft, fraud, or other unlawful conduct. The requirement is limited to providing affected individuals one service, not multiple services. The Committee recognizes, however, that some services available in the marketplace may provide only minimal, if any, benefit to consumers, or may provide benefits in limited circumstances. To address the concern that a person providing notice would provide the least expensive service regardless of its efficacy or benefit to consumers, section 3(e)(3) directs the FTC to determine, through rulemaking, the circumstances under which a person must provide consumer credit reports, credit monitoring, or other service.

Section 3(f) provides an exemption from the requirements of section 3 under limited circumstances. Pursuant to paragraph (1), a person will not be required to provide notice if following a breach of security a person determines that there is no reasonable risk of identity theft, fraud, or other unlawful conduct. The Committee expects that these determinations will require a fact-specific analysis of a particular incident that will take into account the types of information that have been compromised, the cause of the breach, the identity of the party who may have accessed or acquired the information (if known), the usability of the compromised information, and other factors.

Section 3(f)(2)(A) establishes a presumption that there is no reasonable risk of identity theft, fraud, or other unlawful conduct in a particular breach of security if the personal information that was the subject of the breach is unusable, unreadable, or indecipherable to an unauthorized third party. The method of rendering information unusable, unreadable, or indecipherable must be generally accepted by experts in the information security field. As of the date of this report, December 2009, encryption is one such method. How-

ever, while the statute recognizes encryption as a generally accepted method, it should not be interpreted as to require the use of "end to end" encryption. The presumption, of no reasonable risk of identity theft, fraud, or other unlawful conduct, may be rebutted by facts demonstrating that in a particular case the security technologies or methodologies have been, or are reasonably likely to be compromised.

Section 3(f)(2)(B) requires the FTC to issue rules or guidance identifying security methodologies or technologies which render data unusable, unreadable, or indecipherable for the purpose of establishing the rebuttable presumption. FTC rules or guidance must be issued one year after the enactment of H.R. 2221 and biannually thereafter. This biannual requirement will ensure that FTC guidance remains relevant, up-to-date, and reflects changes in technology and methodologies over time. Because certain technologies and methodologies will likely become outdated or no longer considered to be an effective information security tool by experts in the information security field, the FTC will update its guidance or regulations to reflect that fact. The FTC could, at any time through this rulemaking process, determine that encryption or any other technology or methodology previously identified in FTC guidance no longer receives a presumption. Importantly, in issuing these rules or guidance, the FTC is required to consult with relevant industries, consumer organizations, data security experts, identity theft prevention experts, and established standard setting bodies.

By establishing this rebuttable presumption, the Committee does not intend to deem any technology as the only, preferred or most effective method or technology for securing personal information. To the contrary, the provision expressly recognizes that there may be many technologies and methodologies that render data unusable, unreadable, or indecipherable for the purpose of establishing the rebuttable presumption. The Committee expects that during the rulemaking or guidance process mandated by this paragraph, those stakeholders that the FTC is required to consult with will identify, and the FTC will consider, a broad range of technologies and methodologies including, but not limited to, access controls, data association, data masking, encryption, non-persistent storage on devices, physical anti-tamper devices, redaction, and remotely triggered kill-pill technologies. This ongoing process is intended to encourage innovation and foster the development and adoption of new, information security technologies and methodologies.

Section 3(g) provides the FTC with the discretion to place a notice of a breach of security it has received pursuant to section 3(a)(2) on its website if the FTC finds that such notice would be in the public interest or for the protection of consumers. In making a determination, the FTC should consider not only the benefits to consumers and the public interest, but also any possible harm that could result from such publication, including the possible facilitation of phishing attacks or the causing of undue consumer concern and confusion.

Section 3(h) requires the FTC to conduct a study on the practicality and cost effectiveness of requiring notice to be provided in a language in addition to English to individuals known to speak only a language other than English.

Section 3(i) provides the FTC with discretionary rulemaking authority to issue rules necessary for the FTC to effectively enforce section 3.

Section 3(j) provides that the FTC shall determine through rulemaking which other federal laws that require persons subject to H.R. 2221 to provide notice to individuals following a breach of security provide protections substantially similar to, or greater than, those required under section 3. Any person, who is in compliance with the identified federal law, shall be deemed to be in compliance with section 3 and the implementing regulations of the FTC. It is the intent of the Committee to avoid the imposition of duplicative, inconsistent, or overlapping regulations while ensuring that consumers receive notification of information security breaches.

Section 4. Application and enforcement

Section 4(a) provides that sections 2 and 3 only apply to those persons, partnerships, or corporations over which the FTC has authority pursuant to section 5(a)(2) of the FTC Act.

Section 4(b) provides for enforcement by the FTC and establishes that a violation of section 2 or 3 shall be treated as an unfair or deceptive act or practice in violation of a regulation under section 18 of the FTC Act. Section 4(b)(3) explicitly prohibits the FTC, when promulgating rules under this Act, from requiring the deployment or use of any specific products or technologies, including any specific hardware or software.

Section 4(c)(1) provides for enforcement by the attorney general of a state, or an official or agency of a state, for violations of section 2 and 3. Section 4(c)(2) sets out the specific methods for calculating civil penalties in actions brought by the attorney general of a state, or an official or agency of a state. Section 4(c)(2)(C) limits the maximum total liability for civil penalties. Section 4(c)(3) imposes specific obligations and limitations on state actions.

Section 4(d)(1) establishes an affirmative defense to an enforcement action brought under subsection 4(b), or a civil action brought under subsection 4(c), based on a violation of section 3, that all of the personal information compromised in a particular breach of security is public record information acquired from such public records. Section 4(d)(2) provides that the affirmative defense does not exempt any person from the requirement to notify the FTC of a breach of security as required under section 3(a).

Section 5. Definitions

Section 5 contains the definitions that apply to the Act.

Paragraph (1) defines "breach of security" to mean the unauthorized access to or acquisition of data in electronic form containing personal information.

Paragraph (2) defines the term "Commission" to mean the Federal Trade Commission.

Paragraph (3) defines the term "data in electronic form" to mean any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices. The definition includes data stored on removable media and portable storage devices.

Paragraph (4) defines the term "encryption" to mean 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 that renders data indecipherable in the absence of the cryptographic keys needed to decrypt the data. Such encryption must include the appropriate management and protection of the keys.

Paragraph (5) defines the term "identity theft" to mean the unauthorized use of another person's personal information for the purpose of engaging in commercial transactions under the name of that other person. While identity theft has predominantly involved account fraud, including the misuse of existing accounts and new account fraud, the term captures other equally harmful actions that occur in commerce that do not constitute account fraud.

Paragraph (6)(A) defines the term "information broker" to mean 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 that information or provide access to that information to any non-affiliated third party. This term includes entities who meet this definition as to any part of their overall business. Some entities may have other business lines under which they conduct transactions directly with individual customers. Any entity will be considered an information broker if any part of its business meets the definition.

Paragraph (6)(B) excludes from the definition of information broker a commercial entity to the extent that it processes information collected by and received from a nonaffiliated third party concerning individuals who are current or former customers or employees of that third party to enable that third party to (1) provide benefits for its employees or (2) directly transact business with its customers. This subparagraph clarifies that "information broker" does not include an entity where the collection or processing of information is incidental to its provision of other services, such as the provision of employee benefits. The phrase "collected by and received from a nonaffiliated third party" includes information collected on behalf of such nonaffiliated third party, received directly from the individual about whom the information relates. During the course of administration of an employee benefit plan, for example, an entity may, on behalf of the plan, directly collect and receive data (e.g. phone numbers, address updates, bank deposit/EFT instructions) from individual employees.

Paragraph (7) provides that the term "personal information" means an individual's first name or initial and last name, or address, or phone number, in combination with any one or more of the following data elements for that individual: Social Security number; driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity; 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. An individual's first name or initial and last name, or address, or phone number, in combination with a financial account number, or credit or debit card number alone, constitutes "personal information" for the purposes of this Act where such information, without a security code, access code, or password, could be used to commit identity theft, fraud, or other unlawful conduct. For example, information contained in the magnetic field

on the back of a credit card contains only the card holder's name and the card number, along with associated security data. For most credit cards, theft of this information, without a PIN or password, is adequate to duplicate the card and steal goods. Therefore, the definition of personal information includes the name and card number information contained in the magnetic fields of a credit card.

Pursuant to paragraph 7(B), the FTC may modify the definition of "personal information" through rulemaking, but only to the extent that modification will not unreasonably impede interstate commerce and will accomplish the purposes of this Act. In addition, for the purpose of section 3, the FTC must further find that modification is necessary to accommodate changes in technology or practices.

Paragraph (8) defines the term "public record information" to mean information about an individual that has been obtained originally from records of a federal, state, or local government entity that are available for public inspection.

Paragraph (9) defines the term "non-public information" to mean information about an individual that is of a private nature and neither available to the general public nor obtained from a public record.

Paragraph (10) defines the term "service provider" to mean an entity that provides to a user transmission, routing, intermediate and transient storage, or connections to its system or network, for electronic communications, between or among points specified by such user of material of the user's choosing, without modification to the content of the material as sent or received. Any such entity shall be treated as a service provider under this Act only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage, or connections. In this context, intermediate or transient storage is to be interpreted narrowly to only cover temporary storage in the course of transmission or routing. Furthermore, the term service provider only applies to those entities that serve as a conduit of information and only to the specific activities of providing transmission, routing, intermediate and transient storage or connections. The service provider does not treat personal information it is transmitting or routing any differently from any other data sent over its pipes. An entity that processes information, or serves as an intermediary for the transmission or processing of specific categories of information, such as a credit card processor receiving and forwarding credit card information, does not meet this definition.

Section 6. Effect on other laws

Section 6 provides that this Act preempts any provision of a state law to the extent a state law expressly requires information security practices and treatment of data containing personal information similar to any of those required under section 2; and requires notification to individuals of a breach of security resulting in unauthorized access to or acquisition of data in electronic form containing personal information. Section 6 further provides that no person other than a person specified in section 4(c) 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 provisions of this Act, but makes clear that this provision shall not be construed

to limit the enforcement of any state consumer protection law by an attorney general of a state.

Section 7. Effective date

Section 7 establishes the effective date as 1 year after enactment of this Act.

Section 8. Authorization of appropriations

Section 8 authorizes appropriations of $1 million for each fiscal year from 2010 to 2015 to carry out the provisions of this Act.

EXPLANATION OF AMENDMENTS

During the full Committee markup of H.R. 2221, Chairman Waxman offered an amendment in the nature of a substitute as a manager's amendment. The bipartisan amendment not only incorporated the changes made in Subcommittee, but also included several additional changes to the bill.

In section 2, the manager's amendment streamlined the ability of the FTC to conduct rulemaking concerning the destruction of paper documents. The manager's amendment also clarified that persons subject to security requirements under other relevant federal statutes will be deemed to be in compliance with the bill's security requirements provided that those safeguards are "substantially similar to or greater than" the requirements of this bill. In addition, the amendment clarified the telecommunications exemption in section 2 to ensure that certain service providers are exempt from the security requirements only to the extent they are serving as the conduit for the transmission of information.

With respect to the information broker provisions in section 2(b), the amendment: (1) clarified the exemption for fraud databases from the accuracy requirements under certain circumstances; (2) established a new procedure that permits information brokers to offer consumers the ability to prohibit the use of their information for marketing purposes in lieu of complying with the bill's access and correction provisions for marketing databases; and (3) further clarified that compliance with the Fair Credit Reporting Act constitutes compliance with the accuracy, access, and correction requirements of this Act.

The amendment deleted the provision in section 3 of the bill concerning breaches of health information; added a requirement that consumers be provided with notice not later than 60 days after the discovery of the breach; provided that in lieu of free credit reports for individuals who have experienced a breach, a breached entity may provide affected individuals with credit monitoring or other services that assist in the detection or prevention of the misuse of their personal information; and revised provisions concerning the presumption that there is no reasonable risk of identity theft so that the presumption is more technology neutral and remains current and relevant as technology evolves. In addition, as with section 2, the amendment clarified the scope and application of the limited telecommunications exemption in section 3 to ensure that such exception only applies to service providers when serving as the conduit for the transmission of information.

Further, the amendment clarified that the Act only applies to commercial entities subject to FTC jurisdiction and that the civil

penalty cap that applies to enforcement by the states may not exceed $5 million for each violation. Finally, the amendment added language to clarify the definition of information broker.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

There are no changes in existing federal law made by the bill, as reported.

○