To strengthen data protection and safeguards, require data breach notification, and further prevent identity theft.

IN THE SENATE OF THE UNITED STATES

APRIL 20, 2007

Mr. INOUYE (for himself, Mr. STEVENS, Mr. PRYOR, and Mr. SMITH) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To strengthen data protection and safeguards, require data breach notification, and further prevent identity theft.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) Short Title.—This Act may be cited as the “Identity Theft Prevention Act”.

(b) Table of Contents.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Protection of sensitive personal information.
Sec. 3. Notification of security breach risk.
Sec. 4. Security freeze.
Sec. 5. Information security and consumer privacy advisory committee.
Sec. 6. Related crime study.
SEC. 2. PROTECTION OF SENSITIVE PERSONAL INFORMATION.

(a) IN GENERAL.—A covered entity shall develop, implement, maintain, and enforce a written program for the security of sensitive personal information the entity collects, maintains, sells, transfers, or disposes of, containing administrative, technical, and physical safeguards—

(1) to ensure the security and confidentiality of such data;

(2) to protect against any anticipated threats or hazards to the security or integrity of such data; and

(3) to protect against unauthorized access to, or use of, such data that could result in substantial harm to any individual.

(b) COMPLIANCE WITH FTC STANDARDS REQUIRED.—A covered entity that is in full compliance with the requirements of the Commission’s rules on Standards for Safeguarding Customer Information and Disposal of Consumer Report Information and Records is deemed to be in compliance with the requirements of subsection (a).

(c) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall pro-
mulgate regulations, in accordance with section 553 of title 5, United States Code, that require procedures for authenticating the credentials of any third party to which sensitive personal information is to be transferred or sold by a covered entity.

SEC. 3. NOTIFICATION OF SECURITY BREACH RISK.

(a) Security Breaches Affecting 1,000 or More Individuals.—

(1) In general.—If a covered entity discovers a breach of security that affects 1,000 or more individuals, then, before conducting the notification required by subsection (c), it shall—

(A) report the breach to the Commission (or other appropriate Federal regulator under section 8); and

(B) notify all consumer reporting agencies described in section 603(p)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)(1)) of the breach.

(2) FTC Website Publication.—Whenever the Commission receives a report under paragraph (1)(A), after the notification required by subsection (e) has begun, it shall post a report of the breach of security on its website without disclosing any sen-
sitive personal information pertaining to the individuals affected (including their names).

(3) CONTENTS OF REPORT.—The report described in paragraph (2) shall include—
   
   (A) the number of individuals impacted by the breach of security; and
   
   (B) confirmation that the covered entity has taken action to comply with the requirements of subsection (c).

(b) SECURITY BREACHES AFFECTING FEWER THAN 1,000 INDIVIDUALS.—

   (1) IN GENERAL.—If a covered entity discovers a breach of security that affects the sensitive personal information of fewer than 1,000 individuals and determines that the breach of security does not create a reasonable risk of identity theft, it shall report the breach to the Commission (or other appropriate Federal regulator under section 8).

   (2) REPORT CONTENTS.—The report shall contain the number of individuals affected and the type of information that was exposed because of the breach of security.

   (3) LIMITATION ON COMMISSION RESPONSE.—With respect to a report under paragraph (1) re-
ceived by the Commission, the Commission may not—

(A) disclose any sensitive personal information relating to the individuals (including their names); or

(B) publish such a report on its website.

(4) Determination of Reasonable Risk of Identity Theft.—

(A) In general.—If a covered entity cannot make a determination as to whether the breach of security creates a reasonable risk of identity theft, it may request guidance from the Commission in writing as to a suggested course of action that may be required under this Act.

(B) Time and Manner of Response.—The Commission shall respond to a request from a covered entity under subparagraph (A) in writing within 5 business days after the date on which it receives the request.

(c) Notification of Consumers.—

(1) In general.—A covered entity shall use due diligence to investigate any suspected breach of security affecting sensitive personal information maintained by that covered entity. If, after the exercise of such due diligence, the covered entity dis-
covers a breach of security and determines that the breach of security creates a reasonable risk of identity theft, the covered entity shall notify each such individual. In determining whether a reasonable risk of identity theft exists, a covered entity shall consider such factors as whether—

(A) data containing sensitive personal information is usable or could be made usable by an unauthorized third party; and

(B) the data is in the possession and control of an unauthorized third party.

(2) Direct relationship with consumer required.—The notice required by paragraph (1) must be provided by the entity which has a direct relationship with the parties whose information was subject to the breach. Unless there is an agreement to the contrary, the entity providing the notice shall be compensated for the cost of the notice required by the covered entity subject to the breach of security.

(d) Methods of notification; notice content.—

(1) In general.—A covered entity shall provide notice pursuant to subsection (c) by—

(A) written notice;
(B) electronic notice, if such notice is consistent with the provisions of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.); or

(C) substitute notice, if the covered entity does not have sufficient contact information for the individuals to be notified, consisting of—

(i) notice by electronic mail when the covered entity has an electronic mail address for affected individuals;

(ii) conspicuous posting of the security breach on the Internet website of the covered entity for a reasonable period, if the covered entity maintains a website (except that the information posted may not disclose any sensitive personal information pertaining to the affected individuals (including their names)); and

(iii) notification to major statewide media of the breach of security.

(2) CONTENT OF NOTICE.—The notice required under paragraphs (1)(A) and (B) shall consist of—

(A) the name of the individual whose information was the subject of the breach of security;
(B) the name of the covered entity that
was the subject of the breach of security;

(C) a description of the categories of sen-
sitive personal information of the individual
that were the subject of the breach of security;

(D) the date of discovery of such breach of
security; and

(E) the toll-free numbers necessary to con-
tact—

(i) each covered entity that was the
subject of the breach of security;

(ii) each nationwide credit reporting
agency; and

(iii) the Commission.

(e) TIMING OF NOTIFICATION.—

(1) IN GENERAL.—Except as provided in para-
graph (2), notice required by subsection (c) shall be
given—

(A) in a manner that is consistent with
any measures necessary to determine the scope
of the breach and restore the security and in-
tegrity of the data system; and

(B) in the most expeditious manner prac-
ticable, but not later than 25 business days
after the date on which the breach of security
was discovered by the covered entity.

(2) LAW ENFORCEMENT AND NATIONAL OR
HOMELAND SECURITY RELATED DELAYS.—Notwith-
standing paragraph (1), the giving of notice as re-
quired by that paragraph may be delayed for a rea-
sonable period of time if—

(A) a Federal or State law enforcement
agency determines that the timely giving of no-
tice under subsections (a) and (c), as required
by paragraph (1), would materially impede a
civil or criminal investigation; or

(B) a Federal national security or home-
land security agency determines that such time-
ly giving of notice would threaten national or
homeland security.

(f) CERTAIN SERVICE PROVIDERS.—Section 2 and
subsections (a), (b), and (c) of this section do not apply
to electronic communication of a third party stored by a
cable operator, information service, or telecommunications
carrier in the network of such operator, service or carrier
in the course of transferring or transmitting such commu-
nication. Any term used in this subsection that is defined
in the Communications Act of 1934 (47 U.S.C. 151 et
seq.) has the meaning given it in that Act.
SEC. 4. SECURITY FREEZE.

(a) In General.—

(1) Emplacement.—A consumer may place a security freeze on the consumer’s credit report by making a request to a consumer credit reporting agency in writing, by telephone, or through a secure electronic connection if such a connection is made available by the consumer credit reporting agency.

(2) Consumer Disclosure.—If a consumer requests a security freeze, the consumer credit reporting agency shall disclose to the consumer the process of placing and removing the security freeze. A consumer credit reporting agency may not imply or inform a consumer that the placement or presence of a security freeze on the consumer’s credit report may negatively affect the consumer’s credit score.

(b) Effect of Security Freeze.—

(1) Release of Information Blocked.—If a security freeze is in place on a consumer’s credit report, a consumer credit reporting agency may not release the credit report for consumer credit review purposes to a third party without prior express authorization from the consumer.

(2) Information Provided to Third Parties.—Paragraph (1) does not prevent a consumer
credit reporting agency from advising a third party that a security freeze is in effect with respect to the consumer’s credit report. If a third party, in connection with a request for information in any circumstance under which a consumer credit reporting agency may furnish a consumer report under section 604(a) of the Fair Credit Reporting Act (15 U.S.C. 1681b), requests access to a consumer credit report on which a security freeze is in place, the third party may treat any application associated with the request as incomplete.

(3) Consumer Credit Score Not Affected.—The placement of a security freeze on a credit report may not be taken into account for any purpose in determining the credit score of the consumer to whom the account relates.

(c) Removal; Temporary Suspension.—

(1) In General.—Except as provided in paragraphs (2)(B) and (4), a security freeze shall remain in place until the consumer requests that the security freeze be removed. A consumer may remove a security freeze on the consumer’s credit report by making a request to a consumer credit reporting agency in writing, by telephone, or through a secure
electronic connection made available by the consumer credit reporting agency.

(2) CONDITIONS.—A consumer credit reporting agency may remove a security freeze placed on a consumer’s credit report only—

(A) upon the consumer’s request, pursuant to paragraph (1); or

(B) if the agency determines that the consumer’s credit report was frozen due to a material misrepresentation of fact by the consumer.

(3) NOTIFICATION TO CONSUMER.—If a consumer credit reporting agency intends to remove a freeze upon a consumer’s credit report pursuant to paragraph (2)(B) or (4), the consumer credit reporting agency shall notify the consumer in writing prior to removing the freeze on the consumer’s credit report.

(4) TEMPORARY SUSPENSION.—A consumer may have a security freeze on the consumer’s credit report temporarily suspended by making a request to a consumer credit reporting agency in writing or through a secure electronic connection made available by the consumer credit reporting agency and—

(A) specifying beginning and ending dates for the period during which the security freeze
is not to apply to that consumer’s credit report;

or

(B) specifying a specific third party to which access to the credit report may be granted notwithstanding the freeze.

(d) Response Times; Notification of Other Entities.—

(1) In general.—A consumer credit reporting agency shall—

(A) place a security freeze on a consumer’s credit report under subsection (a) no later than 3 business days after receiving a request from the consumer under subsection (a)(1);

(B) remove a security freeze within 3 business days after receiving a request for removal from the consumer under subsection (c); and

(C) temporarily suspend a security freeze within 1 business day after receiving a request under subsection (c)(4).

(2) Notification of other covered entities.—If the consumer requests in writing, by telephone, or by secure electronic connection that other covered entities be notified of the request, the consumer credit reporting agency shall notify all other consumer credit reporting agencies described in sec-
tion 603(p)(1) of the Fair Credit Reporting Act (15
U.S.C. 1681a(p)(1)) of the request within 1 day of
receiving the request.

(3) IMPLEMENTATION BY OTHER COVERED EN-
TITIES.—A consumer credit reporting agency that is
notified of a request under paragraph (2) to place,
remove, or temporarily suspend a security freeze on
a consumer’s credit report shall—

(A) ensure the validity of the request, in-
cluding verifying the identity of the requesting
consumer, within 3 business days after receiv-
ing the notification; and

(B) place, remove, or temporarily suspend
the security freeze on that credit report within
3 business days after validating the request, in-
cluding verifying the identity of the requesting
consumer and securing the fee under subsection
(h)(1), if applicable.

(c) CONFIRMATION.—Except as provided in sub-
section (e)(3), whenever a consumer credit reporting agen-
cy places, removes, or temporarily suspends a security
freeze on a consumer’s credit report at the request of that
consumer under subsection (a) or (e), respectively, it shall
send a written confirmation thereof to the consumer with-
in 10 business days after placing, removing, or temporarily
suspending the security freeze on the credit report. This subsection does not apply to the placement, removal, or temporary suspension of a security freeze by a consumer credit reporting agency because of a notification received under subsection (d)(2).

(f) ID REQUIRED.—A consumer credit reporting agency may not place, remove, or temporarily suspend a security freeze on a consumer’s credit report at the consumer’s request unless the consumer provides proper identification (within the meaning of section 610(a)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681(h)(a)(1)) and the regulations thereunder.

(g) EXCEPTIONS.—This section does not apply to the use of a consumer credit report by any of the following:

(1) A person or entity, or a subsidiary, affiliate, or agent of that person or entity, or an assignee of a financial obligation owing by the consumer to that person or entity, or a prospective assignee of a financial obligation owing by the consumer to that person or entity in conjunction with the proposed purchase of the financial obligation, with which the consumer has or had prior to assignment an account or contract, including a demand deposit account, or to whom the consumer issued a negotiable instrument, for the purposes of reviewing the account or
collecting the financial obligation owing for the account, contract, or negotiable instrument.

(2) Any Federal, State or local agency, law enforcement agency, trial court, or private collection agency acting pursuant to a court order, warrant, subpoena, or other compulsory process.

(3) A child support agency or its agents or assigns acting pursuant to subtitle D of title IV of the Social Security Act (42 U.S.C. et seq.) or similar State law.

(4) The Department of Health and Human Services, a similar State agency, or the agents or assigns of the Federal or State agency acting to investigate medicare or medicaid fraud.

(5) The Internal Revenue Service or a State or municipal taxing authority, or a State department of motor vehicles, or any of the agents or assigns of these Federal, State, or municipal agencies acting to investigate or collect delinquent taxes or unpaid court orders or to fulfill any of their other statutory responsibilities.

(6) Any person or entity administering a credit file monitoring subscription to which the consumer has subscribed.
(7) Any person or entity for the purpose of providing a consumer with a copy of the consumer’s credit report or credit score upon the consumer’s request.

(8) Except when access is restricted to a specific third party during a temporary suspension of a security freeze under subsection (e)(4)(B), any person who seeks access during the time period that a security freeze is temporarily suspended for the purpose of facilitating the extension of credit or another permissible use.

(h) FEES.—

(1) IN GENERAL.—Except as provided in paragraph (2), a consumer credit reporting agency may charge a fee, not in excess of $10, for placing a security freeze on a consumer’s credit report. A consumer reporting agency may not charge a consumer for up to 2 requests per year per credit reporting agency for temporary suspension of a security freeze. If the consumer requests more than 2 temporary suspensions of a security freeze from a credit reporting agency within a year, then that consumer credit reporting agency may charge the consumer a fee for each such additional request, but that consumer credit reporting agency may not charge in ex-
cess of $5 per request. A consumer credit reporting agency may not charge a consumer for removing a security freeze.

(2) FEES PROHIBITED.—

(A) ID THEFT VICTIMS.—A consumer credit reporting agency may not charge a fee for placing, removing, or temporarily suspending a security freeze on a consumer’s credit report if—

(i) the consumer is a victim of identity theft;

(ii) the consumer requests the security freeze in writing;

(iii) the consumer has filed a police report with respect to the theft, or an identity theft report (as defined in section 603(q)(4) of the Fair Credit Reporting Act (15 U.S.C. 1681a(q)(4))), within 180 days after the theft occurred or was discovered by the consumer; and

(iv) the consumer provides a copy of the report to the credit reporting agency.

(B) CATEGORICAL CLASSES.—A consumer credit reporting agency may not charge a fee for placing, removing, or temporarily sus-
pending a credit freeze on a consumer’s credit report if the consumer requesting it—

(i) has attained the age of 65 years;

(ii) is on active duty or in the ready reserve component of an armed force of the United States; or

(iii) is the spouse of an individual described in clause (ii).

(i) Limitation on Information Changes in Frozen Reports.—

(1) In General.—If a security freeze is in place on a consumer’s credit report, a consumer credit reporting agency may not change any of the following official information in that credit report without sending a written confirmation of the change to the consumer within 30 days after the change is made:

(A) Name.

(B) Date of birth.

(C) Social security account number.

(D) Address.

(2) Confirmation.—Paragraph (1) does not require written confirmation for technical modifications of a consumer’s official information, including name and street abbreviations, complete spellings, or
transposition of numbers or letters. In the case of an
address change, the written confirmation shall be
sent to both the new address and to the former ad-
dress.

(j) Certain Entity Exemptions.—

(1) Resellers and Other Agencies.—

(A) In general.—Except as provided in
subparagraph (B), the provisions of this Act do
not apply to a consumer credit reporting agency
that acts only as a reseller of credit information
by assembling and merging information con-
tained in the data base of another consumer
credit reporting agency or multiple consumer
credit reporting agencies, and does not main-
tain a permanent data base of credit informa-
tion from which new consumer credit reports
are produced.

(B) Reseller to Honor Freezes
placed by consumer reporting agen-
cies.—Section 4(b), and, to the extent applica-
ble, section 8 of this Act apply to a consumer
credit reporting agency described in subpara-
graph (A).
(2) Other exempted entities.—The following entities are not required to place a security freeze in a credit report:

(A) A check services or fraud prevention services company, which issues reports on incidents of fraud or authorizations for the purpose of approving or processing negotiable instruments, electronic funds transfers, or similar methods of payments.

(B) A deposit account information service company, which issues reports regarding account closures due to fraud, substantial overdrafts, ATM abuse, or similar negative information regarding a consumer, to inquiring banks or other financial institutions for use only in reviewing a consumer request for a deposit account at the inquiring bank or financial institution.

SEC. 5. INFORMATION SECURITY AND CONSUMER PRIVACY ADVISORY COMMITTEE.

(a) Establishment.—Not later than 90 days after the date of enactment of this Act, the Chairman of the Commission shall establish the Information Security and Consumer Privacy Advisory Committee.
(b) Membership.—The Advisory Committee shall consist of 5 members appointed by the Chairman after appropriate consultations with relevant interested parties. Of the 5 members, the Advisory Committee shall contain at least 1 member from each of the following groups:

1. A non-profit consumer advocacy group.
2. A business organization that collects personally identifiable information.
3. A state Attorney General’s office.

(c) Chairperson.—The Advisory Committee members shall elect 1 member to serve as chairperson of the Advisory Committee.

(d) Functions.—The Advisory Committee shall collect, review, disseminate, and advise on best practices for covered entities to protect sensitive personal information stored and transferred.

(e) Report.—Not later than 12 months after the date on which the Advisory Committee is established under subsection (a) and annually thereafter, the Advisory Committee shall submit to Congress a report on its findings.

(f) No Termination.—Section 14(a)(2) of the Federal Advisory Committee Act (5 U.S.C. App 14(a)(2)) shall not apply to the Advisory Committee.
SEC. 6. RELATED CRIME STUDY.

(a) IN GENERAL.—The Federal Trade Commission, in conjunction with the Department of Justice and other Federal agencies, shall undertake a study of—

(1) the correlation between methamphetamine use and identity theft crimes;

(2) the needs of law enforcement to address methamphetamine crimes related to identity theft, including production, trafficking, and the purchase of precursor chemicals; and

(3) the Federal Government’s role in addressing and deterring identity theft crimes.

(b) REPORT.—Not later than 18 months after the date of enactment of this Act, the Commission shall submit a report of its findings and recommendations to the Congress that includes—

(1) a detailed analysis of the correlation between methamphetamine use and identity theft crimes;

(2) the needs of law enforcement to address methamphetamine crimes related to identity theft including production, trafficking, and the purchase of precursor chemicals related to methamphetamine;

(3) the Federal Government’s role in addressing and deterring identity theft crimes; and
(4) specific recommendations for means of reducing and preventing crimes involving methamphetamine and identity theft, including recommendations for best practices for local law enforcement agencies.

SEC. 7. PROHIBITION ON TECHNOLOGY MANDATES.

Nothing in this Act shall be construed to permit the Commission to issue regulations that require or impose a specific technology, product, technological standards, or solution.

SEC. 8. ENFORCEMENT.

(a) Enforcement by Commission.—Except as provided in subsection (e), this Act shall be enforced by the Commission.

(b) Violation Is Unfair or Deceptive Act or Practice.—The violation of any provision of this Act shall be treated as an unfair or deceptive act or practice proscribed under a rule issued under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(c) Enforcement by Certain Other Agencies.—Compliance with this Act shall be enforced exclusively under—

(1) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), in the case of—
(A) national banks, and Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers), by the Office of the Comptroller of the Currency;

(B) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 and 611), and bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies and investment advisers), by the Board of Governors of the Federal Reserve System;

(C) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System), insured State branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, per-
sons providing insurance, investment companies
and investment advisers), by the Board of Di-
rectors of the Federal Deposit Insurance Cor-
poration; and

(D) savings associations the deposits of
which are insured by the Federal Deposit In-
surance Corporation, and any subsidiaries of
such savings associations (except brokers, deal-
ers, persons providing insurance, investment
companies and investment advisers), by the Di-
rector of the Office of Thrift Supervision;

(2) the Federal Credit Union Act (12 U.S.C.
1751 et seq.) by the Board of the National Credit
Union Administration Board with respect to any
Federal credit union and any subsidiaries of such a
credit union;

(3) the Securities and Exchange Act of 1934
(15 U.S.C. 78a et seq.) by the Securities and Ex-
change Commission with respect to—

(A) a broker or dealer subject to that Act;

(B) an investment company subject to the
Investment Company Act of 1940 (15 U.S.C.
80a–1 et seq.); and
(C) an investment advisor subject to the Investment Advisers Act of 1940 (15 U.S.C. 80b–1 et seq.); and

(4) State insurance law, in the case of any person engaged in providing insurance, by the applicable State insurance authority of the State in which the person is domiciled.

(d) Exercise of Certain Powers.—For the purpose of the exercise by any agency referred to in subsection (c) of its powers under any Act referred to in that subsection, a violation of this Act is deemed to be a violation of a requirement imposed under that Act. In addition to its powers under any provision of law specifically referred to in subsection (c), each of the agencies referred to in that subsection may exercise, for the purpose of enforcing compliance with any requirement imposed under this Act, any other authority conferred on it by law.

(e) Other Authority Not Affected.—Nothing in this Act shall be construed to limit or affect in any way the Commission’s authority to bring enforcement actions or take any other measure under the Federal Trade Commission Act (15 U.S.C. 41 et seq.) or any other provision of law.

(f) Compliance With Gramm-Leach-Bliley Act.—
(1) **NOTICE.**—Any covered entity that is subject to the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), and gives notice in compliance with the notification requirements established for such covered entities under title V of that Act is deemed to be in compliance with section 3 of this Act.

(2) **SAFEGUARDS.**—Any covered entity that is subject to the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), and fulfills the information protection requirements established for such entities under title V of the Act and under section 607(a) of the Fair Credit Reporting Act (15 U.S.C. 1681e(a)) to protect sensitive personal information shall be deemed to be in compliance with section 2 of this Act.

**SEC. 9. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

(a) **IN GENERAL.**—Except as provided in section 8(c), a State, as parens patriae, may bring a civil action on behalf of its residents in an appropriate state or district court of the United States to enforce the provisions of this Act, to obtain damages, restitution, or other compensation on behalf of such residents, or to obtain such further and other relief as the court may deem appropriate, whenever the attorney general of the State has reason to believe that the interests of the residents of the State have been or
are being threatened or adversely affected by a covered entity that violates this Act or a regulation under this Act.

(b) NOTICE.—The State shall serve written notice to the Commission (or other appropriate Federal regulator under section 8) of any civil action under subsection (a) at least 60 days prior to initiating such civil action. The notice shall include a copy of the complaint to be filed to initiate such civil action, except that if it is not feasible for the State to provide such prior notice, the State shall provide such notice immediately upon instituting such civil action.

(c) AUTHORITY TO INTERVENE.—Upon receiving the notice required by subsection (b), the Commission (or other appropriate Federal regulator under section 8) may intervene in such civil action and upon intervening—

(1) be heard on all matters arising in such civil action; and

(2) file petitions for appeal of a decision in such civil action.

(d) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this section shall prevent the attorney general of a State from exercising the powers conferred on the attorney general by the laws of such State to conduct investigations or to administer oaths or affirmations or to compel the attendance
of witnesses or the production of documentary and other
evidence.

(e) Venue; Service of Process.—In a civil action
brought under subsection (a)—

(1) the venue shall be a judicial district in
which—

(A) the covered entity operates; or

(B) the covered entity was authorized to do
business;

(2) process may be served without regard to the
territorial limits of the district or of the State in
which the civil action is instituted; and

(3) a person who participated with a covered
entity in an alleged violation that is being litigated
in the civil action may be joined in the civil action
without regard to the residence of the person.

(f) Limitation on State Action While Federal
Action Is Pending.—If the Commission (or other appro-
priate Federal agency under section 8) has instituted a
civil action or an administrative 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 or the other agency
for any violation of this Act alleged in the complaint.
SEC. 10. PREEMPTION OF STATE LAW.

(a) NOTICE.—This Act preempts any State or local law, regulation, or rule that requires a covered entity to notify individuals of breaches of security pertaining to them.

(b) INFORMATION SECURITY PROGRAMS.—This Act preempts any State or local law, regulation, or rule that requires a covered entity to develop, implement, maintain, or enforce information security programs to which this Act applies.

(c) SECURITY FREEZE.—

(1) IN GENERAL.—This Act shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State with regards to consumer credit reporting agencies compliance with a consumer’s request to place, remove, or temporarily suspend the prohibition on the release by a credit reporting agency of information from its files on that consumer, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this Act, and then only to the extent of the inconsistency.

(2) GREATER PROTECTION UNDER STATE LAW.—For purposes of this section, a State statute, regulation, order, or interpretation is not incon-
sistent with the provisions of this subtitle if the pro-
tection of such statute, regulation, order, or inter-
pretation affords any person is greater than the pro-
tection provided under this Act in regards to credit
reporting agencies compliance with a consumer’s re-
quest to place, remove, or temporarily suspend the
prohibition on the release by a consumer credit re-
porting agency of information from its files on that
consumer.

(d) LIMITATION OF PREEMPTION.—Federal preemp-
tion under this Act shall only apply to matters expressly
described in subsection (a) or (b) of this section, and shall
have no effect on other State or local laws, regulations,
or rules over covered entities.

SEC. 11. DEFINITIONS.

In this Act:

(1) BREACH OF SECURITY.—The term “breach
of security” means unauthorized access to and ac-
quision of data in any form or format containing
sensitive personal information that compromises the
security or confidentiality of such information.

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

(3) CONSUMER CREDIT REPORTING AGENCY.—
The term “consumer credit reporting agency” means
any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing credit reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing credit reports.

(4) COVERED ENTITY.—The term “covered entity” means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity, and any charitable, educational, or nonprofit organization, that acquires, maintains, or utilizes sensitive personal information.

(5) CREDIT REPORT.—The term “credit report” means a consumer report, as defined in section 603(d) of the Federal Fair Credit Reporting Act (15 U.S.C. 1681a(p)), as well as any associated credit score that is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing a consumer’s eligibility for credit for personal, family or household purposes.

(6) IDENTITY THEFT.—The term “identity theft” means the unauthorized acquisition, purchase,
sale, or use by any person of an individual’s sensitive personal information that—

(A) violates section 1028 of title 18, United States Code, or any provision of State law in pari materia; or

(B) results in harm to the individual whose sensitive personal information was used.

(7) REASONABLE RISK OF IDENTITY THEFT.—

The term “reasonable risk of identity theft” means that the preponderance of the evidence available to the covered entity that has experienced a breach of security establishes that identity theft for 1 or more individuals from the breach of security is foreseeable.

(8) REVIEWING THE ACCOUNT.—The term “reviewing the account” includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

(9) SENSITIVE PERSONAL INFORMATION.—

(A) IN GENERAL.—Except as provided in subparagraphs (B), (C), and (D), the term “sensitive personal information” means an individual’s name, address, or telephone number combined with 1 or more of the following data elements related to that individual:
(i) Social security account number or an employer identification number that is the same as or is derived from the social security account number of that individual.

(ii) Financial account number, or credit card or debit card number of such individual, combined with any required security code, access code, or password that would permit access to such individual’s account.

(iii) State driver’s license identification number or State resident identification number.

(B) PASSWORD ACCOUNTS.—An account identifier combined with a password, PIN, or security code to access the account, for any account from which any of the following can occur without further authentication after login:

(i) A financial transaction.

(ii) A purchase of goods or services.

(iii) A charge to a payment card or account.

(iv) A charge to a credit card or account.
(v) Access to the account that reveals sufficient information to engage in any activity described in clause (i), (ii), (iii), or (iv).

(C) FTC MODIFICATIONS.—The Commission may, through a rulemaking proceeding in accordance with section 553 of title 5, United States Code, designate other identifying information that may be used to effectuate identity theft as sensitive personal information for purposes of this Act and limit or exclude any information described in subparagraph (A) from the definition of sensitive personal information for purposes of this Act.

(D) EXCEPTION.—The term “sensitive personal information” does not include information that is obtained from—

(i) Federal, State, or local governments that has been made available to the general public; or

(ii) widely distributed media.

The exception provided by this subparagraph does not apply if the information obtained from Federal, State, or local government records or
widely distributed media is combined with information obtained from non-public sources.

(E) Public records.—Nothing in this Act prohibits a covered entity from obtaining, aggregating, or using sensitive personal information it lawfully obtains from public records in a manner that does not violate this Act.

SEC. 12. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Commission $2,000,000 for each of fiscal years 2007 through 2011 to carry out this Act.

SEC. 13. EFFECTIVE DATES.

(a) In general.—Except as provided in subsections (b) and (c), the provisions of this Act take effect upon its enactment.

(b) Implementation of security program.—A covered entity shall implement the program required by section 2(a) within 6 months after the date of enactment of this Act.

(c) Provisions requiring rulemaking.—The Commission shall initiate 1 or more rulemaking proceedings under sections 2(c), 3, and 4 (including a rulemaking proceeding to determine what constitutes proper identification within the meaning of section 610(a)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681(h)(a)(1)))
within 45 days after the date of enactment of this Act.
The Commission shall promulgate all final rules pursuant
to those rulemaking proceedings within 1 year after the
date of enactment of this Act. The provisions of sections
2(c), 3, and 4 shall take effect on the same date 6 months
after the date on which the Commission promulgates the
last final rule under the proceeding or proceedings com-
enced under the preceding sentence.
(d) PREEMPTION.—Section 10 shall take effect at the
same time as sections 2(c), 3, and 4 take effect.