114TH CONGRESS
1ST SESSION

# S. 1158

To ensure the privacy and security of sensitive personal information, to prevent and mitigate identity theft, to provide notice of security breaches involving sensitive personal information, and to enhance law enforcement assistance and other protections against security breaches, fraudulent access, and misuse of personal information.

---

IN THE SENATE OF THE UNITED STATES

APRIL 30, 2015

Mr. LEAHY (for himself, Mr. FRANKEN, Ms. WARREN, Mr. BLUMENTHAL, Mr. WYDEN, and Mr. MARKEY) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

# A BILL

To ensure the privacy and security of sensitive personal information, to prevent and mitigate identity theft, to provide notice of security breaches involving sensitive personal information, and to enhance law enforcement assistance and other protections against security breaches, fraudulent access, and misuse of personal information.

*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 ''Consumer Privacy Protection Act of 2015''.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

**SEC. 2. FINDINGS.**

Congress finds that—

(1) databases of sensitive personally identifiable information are increasingly prime targets of hackers, identity thieves, rogue employees, and other criminals, including organized and sophisticated criminal operations;

(2) security breaches caused by such criminal acts are a serious threat to consumer privacy, consumer confidence, homeland security, national security, e-commerce, and economic stability;

(3) misuse of sensitive personally identifiable information has the potential to cause serious or irreparable harm to an individual's livelihood, privacy, and liberty and undermine efficient and effective business and government operations;

(4) identity theft is a serious threat to the Nation's economic stability, national security, homeland security, cybersecurity, the development of e-commerce, and the privacy rights of Americans;

(5) it is important for business entities that own, use, store, or license sensitive personally identifiable information to adopt reasonable policies and procedures to help ensure the security and privacy of sensitive personally identifiable information; and

(6) individuals whose personal information has been compromised or who have been victims of identity theft should receive the necessary information and assistance to mitigate any potential damage.

**SEC. 3. DEFINITIONS.**

In this Act, the following definitions shall apply:

(1) AFFILIATE.—The term ''affiliate'' means persons related by common ownership or by corporate control.

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

(3) BUSINESS ENTITY.—The term ''business entity'' means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture established to make a profit, or a nonprofit organization.

(4) CONSUMER PRIVACY AND DATA SECURITY PROGRAM.—The term ''consumer privacy and data security program'' means the program described in section 202(a).

(5) COVERED ENTITY.—The term ''covered entity'' means any business entity, other than a service provider, that collects, uses, accesses, transmits,

stores, or disposes of sensitive personally identifiable information.

(6) DESIGNATED ENTITY.—The term ''designated entity'' means the Federal Government entity designated by the Secretary of Homeland Security under section 217(a).

(7) ENCRYPTION.—The term ''encryption''—

(A) means the protection of data in electronic form, in storage or in transit, using an encryption technology that has been generally accepted by experts in the field of information security that renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and

(B) includes appropriate management and safeguards of such cryptographic keys so as to protect the integrity of the encryption.

(8) IDENTITY THEFT.—The term ''identity theft'' means a violation of section 1028(a)(7) of title 18, United States Code.

(9) SECURITY BREACH.—

(A) IN GENERAL.—The term ''security breach'' means compromise of the privacy or security of computerized data that results in, or

that there is a reasonable basis to conclude has resulted in, unauthorized access to or acquisition of sensitive personally identifiable information.

(B) EXCLUSION.—The term ''security breach'' does not include—

(i) a good faith access or acquisition of sensitive personally identifiable information by a business entity, or an employee or agent of a business entity, if the sensitive personally identifiable information is not subject to further unauthorized disclosure;

(ii) the release of a public record not otherwise subject to confidentiality or nondisclosure requirements; or

(iii) any lawfully authorized investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the United States, a State, or a political subdivision of a State.

(10) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term ''sensitive personally identifiable information'' means any information or com-

pilation of information, in electronic or digital form that includes the following:

(A) A non-truncated social security number, a driver's license number, passport number, or alien registration number or other government-issued unique identification number.

(B) A financial account number or credit or debit card number in combination with any security code, access code, or password if required for an individual to obtain credit, withdraw funds, or engage in financial transactions.

(C) A unique electronic account identifier, including an online user name or email address, in combination with any security code, access code, password, or security question and answer, if required for an individual to obtain money, goods, services, access to digital photographs, digital videos or electronic communications, or any other thing of value.

(D) Unique biometric data, such as faceprint, fingerprint, voice print, a retina or iris image, or any other unique physical representation.

(E) An individual's first and last name or first initial and last name in combination with

any information that relates to the individual's past, present, or future physical or mental health or condition, or to the provision of health care to or diagnosis of the individual, including health insurance information such as a health insurance policy number or subscriber identification number, or any information in an individual's health insurance application and claims history.

(F) Information about an individual's geographic location generated by or derived from the operation or use of an electronic communications device that is sufficient to identify the street and name of the city or town in which the device is located, excluding telephone numbers or network or Internet protocol addresses.

(G) Password-protected digital photographs and digital videos not otherwise available to the public.

(11) SERVICE PROVIDER.—The term ''service provider'' means a business entity that provides electronic data transmission, routing, intermediate and transient storage, or connections to its system or network, where the business entity providing such services does not select or modify the content of the

electronic data, is not the sender or the intended recipient of the data, and the business entity transmits, routes, or provides connections for sensitive personally identifiable information in a manner that sensitive personally identifiable information is undifferentiated from other types of data that such business entity transmits, routes, or provides connections. Any such business 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.

# TITLE I—PUNISHMENT FOR CONCEALMENT OF SECURITY BREACHES AND TOOLS TO COMBAT CYBERCRIME

## SEC. 101. CONCEALMENT OF SECURITY BREACHES INVOLVING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following:

**"§ 1041. Concealment of security breaches involving sensitive personally identifiable information**

''(a) IN GENERAL.—Whoever, having knowledge of a security breach and of the fact that notice of such security breach is required under title II of the Consumer Privacy Protection Act of 2015, intentionally and willfully conceals the fact of such security breach, shall, in the event that such security breach results in economic harm to any individual in the amount of $1,000 or more, be fined under this title or imprisoned for not more than 5 years, or both.

''(b) PERSON DEFINED.—For purposes of subsection (a), the term 'person' has the meaning given the term in section 1030(e)(12).''.

(b) CONFORMING AND TECHNICAL AMENDMENTS.—The table of sections for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''1041. Concealment of security breaches involving sensitive personally identifiable information.''.

(c) ENFORCEMENT AUTHORITY.—

(1) IN GENERAL.—The United States Secret Service and Federal Bureau of Investigation shall have the authority to investigate offenses under section 1041 of title 18, United States Code, as added by subsection (a).

(2) NONEXCLUSIVITY.—The authority granted in paragraph (1) shall not be exclusive of any existing authority held by any other Federal agency.

**SEC. 102. REPORTING OF CERTAIN CYBERCRIMES.**

Section 1030 of title 18, United States Code, is amended by striking subsection (h) and inserting the following:

''(h) REPORTING CERTAIN CRIMINAL CASES.—Not later than 1 year after the date of the enactment of this subsection, and annually thereafter, the Attorney General shall report to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives the number of criminal cases brought under subsection (a) that involve conduct in which—

''(1) the defendant—

''(A) exceeded authorized access to a non-governmental computer; or

''(B) accessed a non-governmental computer without authorization; and

''(2) the sole basis for the Government determining that access to the non-governmental computer was unauthorized, or in excess of authorization, was that the defendant violated a contractual obligation or agreement with a service provider or

employer, such as an acceptable use policy or terms of service agreement.''.

**SEC. 103. AUTHORITY TO SHUT DOWN BOTNETS.**

(a) AMENDMENT.—Section 1345 of title 18, United States Code, is amended—

(1) in the heading, by inserting ''**and abuse**'' after ''**fraud**'';

(2) in subsection (a)—

(A) in paragraph (1)—

(i) in subparagraph (B), by striking ''or'' at the end;

(ii) in subparagraph (C), by inserting ''or'' after the semicolon; and

(iii) by inserting after subparagraph (C) the following:

''(D) violating section 1030(a)(5) where such conduct would damage (as defined in section 1030), 100 or more protected computers (as defined in section 1030) during any 1-year period, including by denying access to or operation of the computers, installing unwanted software on the computers, using the computers without authorization, or obtaining information from the computers without authorization;''; and

(B) in paragraph (2), by inserting ", a violation of section 1030(a)(5) as described in subsection (a)(1)(D)," before "or a Federal";

(3) in subsection (b), by adding ", except in the case of a person violating section 1030(a)(5) in the manner described in subsection (a)(1)(D)," before "take such other action"; and

(4) by adding at the end the following:

"(c) A restraining order or prohibition described in subsection (b), if issued in circumstances described in subsection (a)(1)(D)—

"(1) may only authorize action that solely affects persons violating section 1030 in the manner described in subsection (a)(1)(D); and

"(2) may, upon application of the Attorney General—

"(A) specify that no cause of action shall lie in any court against a person for complying with the restraining order, prohibition, or other action; and

"(B) provide that the United States shall pay to such person a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in complying

with the restraining order, prohibition, or other action.

''(d) There are authorized to be appropriated to the Department of Justice, the Department of Homeland Security, and the Department of the Treasury such sums as are necessary to implement this section, including payments made by the United States of a fee for reimbursement.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of section for chapter 63 is amended by striking the item relating to section 1345 and inserting the following:

''1345. Injunctions against fraud and abuse.''.

**SEC. 104. DETERRING THE DEVELOPMENT AND SALE OF COMPUTER AND CELL PHONE SPYING DEVICES.**

Section 1956(c)(7)(D) of title 18, United States Code, is amended by inserting ''section 2512 (relating to the manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices),'' before ''section 46502''.

# TITLE II—CONSUMER PRIVACY AND SECURITY OF SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION

## Subtitle A—Consumer Privacy and Data Security Program

### SEC. 201. PURPOSE AND APPLICABILITY OF CONSUMER PRIVACY AND DATA SECURITY PROGRAM.

(a) PURPOSE.—The purpose of this subtitle is to ensure standards for developing and implementing administrative, technical, and physical safeguards to protect the security of sensitive personally identifiable information.

(b) APPLICABILITY.—A covered entity engaging in interstate commerce that collects, uses, accesses, transmits, stores, or disposes of sensitive personally identifiable information in electronic or digital form of not less than 10,000 United States persons during any 12-month period is subject to the requirements for a consumer privacy and data security program for protecting sensitive personally identifiable information.

(c) LIMITATIONS.—Notwithstanding any other obligation under this subtitle, this subtitle does not apply to the following:

(1) FINANCIAL INSTITUTIONS.—Financial institutions—

(A) subject to and in compliance with the data security requirements and standards under section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)); and

(B) subject to the jurisdiction of an agency or authority described in section 505(a) of the Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)).

(2) HIPAA AND HITECH REGULATED ENTITIES.—An entity that is subject to and in compliance with the data security requirements of the following, with respect to data that is subject to such requirements:

(A) Section 13401 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931).

(B) Part 160 or 164 of title 45, Code of Federal Regulations (or any successor regulations).

(C) The regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note).

(D) In the case of a business associate, as defined in section 13400 of the Health Information Technology for Economic and Clinical

Health Act (42 U.S.C. 17921), the applicable privacy and data security requirements of part 1 of subtitle D of title XIII of division A of the American Reinvestment and Recovery Act of 2009 (42 U.S.C. 17931 et seq.).

(3) SERVICE PROVIDERS.—A service provider for any electronic communication by a third-party, to the extent that the service provider is engaged solely in the transmission, routing, or temporary, intermediate, or transient storage of that communication.

**SEC. 202. REQUIREMENTS FOR CONSUMER PRIVACY AND DATA SECURITY PROGRAM.**

(a) CONSUMER PRIVACY AND DATA SECURITY PROGRAM.—A covered entity subject to this subtitle shall comply with the following safeguards and any other administrative, technical, or physical safeguards identified by the Federal Trade Commission in a rulemaking process pursuant to section 553 of title 5, United States Code, for the protection of sensitive personally identifiable information:

(1) SCOPE.—A covered entity shall implement a comprehensive consumer privacy and data security program that includes administrative, technical, and physical safeguards appropriate to the size and com-

plexity, and the nature and scope, of the activities of the covered entity.

(2) DESIGN.—The consumer privacy and data security program shall be designed to—

(A) ensure the privacy and security of sensitive personally identifying information;

(B) protect against any anticipated vulnerabilities to the privacy and security of sensitive personally identifying information; and

(C) protect against unauthorized access, acquisition, disclosure, or use of sensitive personally identifying information.

(3) RISK ASSESSMENT.—A covered entity shall—

(A) identify reasonably foreseeable internal and external vulnerabilities and internal and external threats that could result in unauthorized access, disclosure, or use of sensitive personally identifiable information or of systems containing sensitive personally identifiable information;

(B) assess the likelihood of and potential damage from unauthorized access, acquisition, disclosure, or use of sensitive personally identifiable information;

(C) assess the sufficiency of its technical, physical, and administrative controls in place to control and minimize risks from unauthorized access, acquisition, disclosure, or use of sensitive personally identifiable information; and

(D) assess the vulnerability of sensitive personally identifiable information during destruction and disposal of such information, including through the disposal or retirement of hardware.

(4) RISK MANAGEMENT AND CONTROL.—Each covered entity shall—

(A) design its consumer privacy and data security program to control the risks identified under paragraph (3);

(B) adopt measures commensurate with the sensitivity of the data as well as the size, complexity, nature, and scope of the activities of the covered entity that—

(i) controls access to sensitive personally identifiable information, including controls to authenticate and permit access only to authorized individuals;

(ii) detect, record, and preserve information relevant to actual and attempted

fraudulent, unlawful, or unauthorized access, acquisition, disclosure, or use of sensitive personally identifiable information, including by employees and other individuals otherwise authorized to have access;

(iii) protect sensitive personally identifiable information during use, transmission, storage, and disposal by encryption, redaction, disclosure limitation methodologies, or access controls, that are widely accepted as an effective industry practice or industry standard, or other reasonable means;

(iv) ensure that sensitive personally identifiable information is properly destroyed and disposed of, including during the destruction of computers and other electronic media that contain sensitive personally identifiable information; and

(v) ensure that no third party is authorized to access or acquire sensitive personally identifiable information in its possession without the covered entity first performing sufficient due diligence to ascertain, with reasonable certainty, that such

information is being sought for a valid legal purpose; and

(C) establish a plan and procedures for minimizing the amount of sensitive personally identifiable information maintained by the covered entity, which shall provide for the retention of sensitive personally identifiable information only as reasonably needed for the business purposes of such business entity or as necessary to comply with any legal obligation.

(5) LIMITATION.—Nothing in this subsection shall be construed to permit, and nothing does permit, the Federal Trade Commission to issue regulations requiring, or according greater legal status to, the implementation of or application of a specific technology or technological specifications for meeting the requirements of this title.

(b) TRAINING.—Covered entities subject to this subtitle shall take steps to ensure employee training and supervision for implementation of the consumer privacy and data security program of the covered entity.

(c) VULNERABILITY TESTING.—

(1) IN GENERAL.—Covered entities subject to this subtitle shall take steps to ensure regular testing of key technical, physical, and administrative

controls for information and information systems of the consumer privacy and data security program to detect, prevent, and respond to attacks or intrusions, or other system failures.

(2) FREQUENCY.—The frequency and nature of the tests required under paragraph (1) shall be determined by the risk assessment of the covered entity under subsection (a)(3).

(d) RELATIONSHIP TO CERTAIN PROVIDERS OF SERVICES.—In the event a covered entity subject to this subtitle engages a person or entity not subject to this subtitle (other than a service provider) to receive sensitive personally identifiable information in performing services or functions (other than the services or functions provided by a service provider) on behalf of and under the instruction of such covered entity, the covered entity shall—

(1) exercise appropriate due diligence in selecting the person or entity for responsibilities related to sensitive personally identifiable information, and take reasonable steps to select and retain a person or entity that is capable of maintaining appropriate controls for the privacy and security of the sensitive personally identifiable information at issue; and

(2) require the person or entity by contract to implement and maintain appropriate measures de-

signed to meet the objectives and requirements governing subtitle A.

(e) PERIODIC ASSESSMENT AND CONSUMER PRIVACY AND DATA SECURITY MODERNIZATION.—Each covered entity subject to this subtitle shall on a regular basis monitor, evaluate, and adjust, as appropriate its consumer privacy and data security program in light of any relevant changes in—

(1) technology;

(2) internal or external threats and vulnerabilities to sensitive personally identifiable information; and

(3) the changing business arrangements of the covered entity, such as—

(A) mergers and acquisitions;

(B) alliances and joint ventures;

(C) outsourcing arrangements;

(D) bankruptcy; and

(E) changes to sensitive personally identifiable information systems.

(f) IMPLEMENTATION TIMELINE.—Not later than 1 year after the date of enactment of this Act, a covered entity subject to the provisions of this subtitle shall implement a consumer privacy and data security program pursuant to this subtitle.

**SEC. 203. FEDERAL ENFORCEMENT.**

(a) IN GENERAL.—The Attorney General and the Federal Trade Commission may enforce civil violations of section 201 or 202.

(b) CIVIL ACTIONS BY THE ATTORNEY GENERAL OF THE UNITED STATES.—

(1) IN GENERAL.—The Attorney General may bring a civil action in the appropriate United States district court against any covered entity that engages in conduct constituting a violation of this subtitle and, upon proof of such conduct by a preponderance of the evidence, such covered entity shall be subject to a civil penalty in an amount that is not greater than the product of the number of individuals whose sensitive personally identifiable information was placed at risk as a result of the violation and $16,500.

(2) PENALTY LIMITATION.—Notwithstanding any other provision of law, the total amount of the civil penalty assessed against a covered entity for conduct involving the same or related acts or omissions that results in a violation of this subtitle may not exceed $5,000,000, unless such conduct is found to be willful or intentional.

(3) DETERMINATIONS.—The determination of whether a violation of a provision of this subtitle has

occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact. The determination of whether a violation of a provision of this subtitle was willful or intentional, and if so, the amount of the additional penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.

(4) ADDITIONAL PENALTY LIMIT.—If a court determines under paragraph (3) that a violation of a provision of this subtitle was willful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $5,000,000.

(c) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—If it appears that a covered entity has engaged, or is engaged, in any act or practice constituting a violation of this subtitle, the Attorney General may petition an appropriate district court of the United States for an order—

(A) enjoining such act or practice; or

(B) enforcing compliance with this subtitle.

(2) ISSUANCE OF ORDER.—A court may issue an order under paragraph (1), if the court finds that

the conduct in question constitutes a violation of this subtitle.

(d) CIVIL ACTIONS BY THE FEDERAL TRADE COMMISSION.—

(1) IN GENERAL.—Compliance with the requirements imposed under this subtitle may be enforced under the Federal Trade Commission Act (15 U.S.C. 41 et seq.) by the Federal Trade Commission with respect to business entities subject to this Act. All of the functions and powers of the Federal Trade Commission under the Federal Trade Commission Act are available to the Commission to enforce compliance by any person with the requirements imposed under this title.

(2) CIVIL PENALTIES.—

(A) IN GENERAL.—Any covered entity that violates the provisions of this subtitle shall be subject to a civil penalty in the amount that is not greater than the product of the number of individuals whose sensitive personally identifiable information was placed at risk as a result of the violation and $16,500.

(B) PENALTY LIMITATION.—Notwithstanding any other provision of law, the total amount of the civil penalty assessed against a

covered entity for conduct involving the same or related acts or omissions that results in a violation of this subtitle may not exceed $5,000,000, unless such conduct is found to be willful or intentional.

(C) DETERMINATIONS.—The determination of whether a violation of a provision of this subtitle has occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact. The determination of whether a violation of a provision of this subtitle was willful or intentional, and if so, the amount of the additional penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.

(D) ADDITIONAL PENALTY LIMIT.—If a court determines under subparagraph (C) that a violation of a provision of this subtitle was willful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $5,000,000.

(3) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—For the purpose of the exercise by the Federal Trade Commission of its functions and powers under the Federal Trade Commission Act, a viola-

tion of any requirement or prohibition imposed under this title shall constitute an unfair or deceptive act or practice in commerce in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(I)(B)) regarding unfair or deceptive acts or practices and shall be subject to enforcement by the Federal Trade Commission under that Act with respect to any business entity, irrespective of whether that business entity is engaged in commerce or meets any other jurisdictional tests in the Federal Trade Commission Act.

(e) COORDINATION OF ENFORCEMENT.—

(1) IN GENERAL.—When opening an investigation, the Federal Trade Commission shall consult with the Attorney General.

(2) LIMITATION.—The Federal Trade Commission may initiate investigations under this subsection unless the Attorney General determines that such an investigation would impede an ongoing criminal investigation or national security activity.

(3) COORDINATION AGREEMENT.—

(A) IN GENERAL.—In order to avoid conflicts and promote consistency regarding the enforcement and litigation of matters under this

Act, not later than 180 days after the date of enactment of this Act, the Attorney General and the Federal Trade Commission shall enter into an agreement for coordination regarding the enforcement of this Act.

(B) REQUIREMENT.—The coordination agreement entered into under subparagraph (A) shall include provisions to ensure that parallel investigations and proceedings under this section are conducted in a manner that avoids conflicts and does not impede the ability of the Attorney General to prosecute violations of Federal criminal laws.

(f) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this section are cumulative and shall not affect any other rights and remedies available under law.

**SEC. 204. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

(a) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that a covered entity has violated section 201 or 202, the

State, as parens patriae, may bring a civil action on behalf of the residents of that State to—

(A) enjoin that act or practice;

(B) enforce compliance with section 201 or 202; or

(C) impose a civil penalty in an amount that is not greater than the product of the number of individuals whose sensitive personally identifiable information was placed at risk as a result of the violation and $16,500.

(2) PENALTY LIMITATION.—

(A) IN GENERAL.—Notwithstanding any other provision of law, the total sum of civil penalties assessed against a covered entity for all violations of the provisions of this subtitle resulting from the same or related acts or omissions may not exceed $5,000,000, unless such conduct is found to be willful or intentional.

(B) DETERMINATIONS.—The determination of whether a violation of a provision of this subtitle has occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact. The determination of whether a violation of a provision of this subtitle was willful or intentional,

and if so, the amount of the additional penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.

(C) ADDITIONAL PENALTY LIMIT.—If a court determines under subparagraph (B) that a violation of a provision of this subtitle was willful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $5,000,000.

(3) NOTICE.—

(A) IN GENERAL.—Before filing an action under this subsection, the attorney general of the State involved shall provide to the Attorney General of the United States and the Federal Trade Commission—

(i) a written notice of that action; and

(ii) a copy of the complaint for that action.

(B) EXCEPTION.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general of a State determines that it is not feasible to provide the notice described in this subparagraph before the filing of the action.

(C) NOTIFICATION WHEN PRACTICABLE.—In an action described under subparagraph (B), the attorney general of a State shall provide the written notice and the copy of the complaint to the Attorney General of the United States and the Federal Trade Commission as soon after the filing of the complaint as practicable.

(4) FEDERAL PROCEEDINGS.—Upon receiving notice under paragraph (2), the Attorney General of the United States and the Federal Trade Commission shall have the right to—

(A) move to stay the action, pending the final disposition of a pending Federal proceeding or action as described in section 203;

(B) initiate an action in the appropriate United States district court under section 203 and move to consolidate all pending actions, including State actions, in such court;

(C) intervene in an action brought under paragraph (1); and

(D) file petitions for appeal.

(5) PENDING PROCEEDINGS.—If the Attorney General of the United States or the Federal Trade Commission initiates a Federal civil action for a violation of this subtitle, or any regulations thereunder,

no attorney general of a State may bring an action for a violation of this subtitle that resulted from the same or related acts or omissions against a defendant named in the Federal civil action initiated by the Attorney General of the United States or the Federal Trade Commission.

(6) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1) nothing in this subtitle 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 and affirmations; or

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

(7) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under subsection (a) may be brought in—

(i) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(ii) another court of competent jurisdiction.

(B) SERVICE OF PROCESS.—In an action brought under subsection (a), process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

(b) NO PRIVATE CAUSE OF ACTION.—Nothing in this subtitle establishes a private cause of action against a business entity for violation of any provision of this subtitle.

**SEC. 205. RELATION TO OTHER LAWS.**

(a) PREEMPTION.—For any covered entity that is subject to this subtitle, the provisions of this subtitle shall supersede any other provision of Federal law, or any provisions of the law of any State or political subdivision of a State requiring data security practices that are less stringent than the requirements of this subtitle.

(b) CONSUMER PROTECTION LAWS.—Except as provided in subsection (a), this section 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.—Nothing in this Act shall be construed to preempt the applicability of—

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

(2) any other State law to the extent that the law relates to acts of fraud.

(d) PRESERVATION OF FTC AUTHORITY.—Nothing in this Act may be construed in any way to limit the authority of the Federal Trade Commission under any other provision of law.

# Subtitle B—Security Breach Notification

**SEC. 211. NOTICE TO INDIVIDUALS.**

(a) IN GENERAL.—Except as provided in section 212, a covered entity shall, following the discovery of a security breach of such information, notify any resident of the United States whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed or acquired.

(b) OBLIGATION OF THIRD PARTY ENTITIES.—

(1) IN GENERAL.—In the event of a breach of security of a system maintained by a third party entity that has been contracted to maintain or process data in electronic form containing sensitive personally identifiable information on behalf of a covered entity who owns or possesses such data, the third party entity shall notify the covered entity of the breach of security. Upon receiving notification from

the third party entity, such covered entity shall provide the notification required under subsection (a).

(2) NOTICE BY THIRD PARTY ENTITIES.—Nothing in this subtitle shall prevent or abrogate an agreement between a covered entity required to give notice under this section and a third party entity that has been contracted to maintain or process data in electronic form containing sensitive personally identifiable information for a covered entity, to provide the notifications required under subsection (a).

(3) SERVICE PROVIDERS.—If a service provider becomes aware of a security breach containing sensitive personally identifiable information that is owned or possessed by a covered entity 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, the service provider shall be required to promptly notify the covered entity who initiated such connection, transmission, routing, or storage of the security breach if the covered entity can be reasonably identified. Upon receiving such notification from a service provider, the covered entity shall be required to provide the notification required under subsection (a).

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—All notifications required under this section shall be made as expediently as possible and without unreasonable delay following the discovery by the covered entity of a security breach.

(2) REASONABLE DELAY.—Reasonable delay under this subsection may include any reasonable time necessary to determine the scope of the security breach, prevent further disclosures, and provide notice to law enforcement when required. Except as provided in subsection (d), delay of notification shall not exceed 30 days following the discovery of a security breach.

(3) BURDEN OF PRODUCTION.—The covered entity required to provide notice under this subtitle shall, upon the request of the Attorney General of the United States or the Federal Trade Commission provide records or other evidence of the notifications required under this subtitle, including to the extent applicable, the reasons for any delay of notification.

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

(1) IN GENERAL.—If a Federal law enforcement agency or intelligence agency determines that

the notification required under this section would impede a criminal investigation, or national security activity, such notification shall be delayed upon written notice from a Federal law enforcement agency or intelligence agency to the covered entity that experienced the security breach. The notification from a Federal law enforcement agency or intelligence agency shall specify in writing the period of delay requested for law enforcement or national security purposes.

(2) EXTENDED DELAY OF NOTIFICATION.—If the notification required under subsection (a) is delayed pursuant to paragraph (1), a covered entity shall give notice 15 days after the day such law enforcement or national security delay was invoked unless a Federal law enforcement or intelligence agency provides written notification that further delay is necessary.

(3) LAW ENFORCEMENT IMMUNITY.—No nonconstitutional cause of action shall lie in any court against any agency for acts relating to the delay of notification for law enforcement or national security purposes under this subtitle.

(e) LIMITATIONS.—Notwithstanding any other obligation under this subtitle, this subtitle does not apply to the following:

(1) FINANCIAL INSTITUTIONS.—Financial institutions—

(A) subject to and in compliance with the data security requirements and standards under section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)); and

(B) subject to the jurisdiction of an agency or authority described in section 505(a) of the Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)).

(2) HIPAA AND HITECH REGULATED ENTITIES.—An entity that is subject to and in compliance with the data breach notification of the following, with respect to data that is subject to such requirements:

(A) Section 13401 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931).

(B) Part 160 or 164 of title 45, Code of Federal Regulations (or any successor regulations).

(C) The regulations promulgated under section 264(c) of the Health Insurance Port-

ability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note).

(D) In the case of a business entity, the applicable data breach notification requirements of part 1 of subtitle D of title XIII of division A of the American Reinvestment and Recovery Act of 2009 (42 U.S.C. 17931 et seq.), if such business entity is acting as a covered entity, a business associate, or a vendor of personal health records, as those terms are defined in section 13400 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17921).

(E) In the case of and third party service provider, section 13407 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17937).

**SEC. 212. EXEMPTIONS.**

(a) NATIONAL SECURITY AND LAW ENFORCEMENT EXEMPTION.—

(1) IN GENERAL.—Section 211 shall not apply to a covered entity if a Federal law enforcement agency or intelligence agency—

(A) determines that notification of the security breach—

(i) could be expected to reveal sensitive sources and methods or similarly impede the ability of the Government to conduct law enforcement investigations; or

(ii) could be expected to cause damage to the national security;

(B) communicates the determination made under subparagraph (A) to the covered entity; and

(C) orders that notification required under section 211 not be made.

(2) IMMUNITY.—No non-constitutional cause of action shall lie in any court against any Federal agency for acts relating to the exemption from notification for law enforcement or national security purposes under this title.

(b) SAFE HARBOR EXEMPTION.—A covered entity shall be exempt from the notice requirements under section 211 if the covered entity reasonably determines that sensitive personally identifiable information is rendered unusable, unreadable, or indecipherable through data security technology or methodology, including encryption or redaction, that is generally accepted by experts in the field of information security, such that there is no reasonable

likelihood that a security breach has resulted in, or will result in, the misuse of data.

**SEC. 213. METHODS OF NOTICE.**

A covered entity shall be in compliance with section 211 if it provides the following:

(1) INDIVIDUAL NOTICE.—Notice to individuals by 1 of the following means if the method of notification selected can most likely be expected to reach the intended individual:

(A) Written notification to the last known home mailing address of the individual in the records of the covered entity.

(B) Telephone notice to the individual personally, provided that the telephone notice is made directly to each affected consumer, and is not made through a prerecorded message.

(C) E-mail notice, if—

(i)(I) the covered entity's primary method of communication with the individual is by e-mail; or

(II) the individual has consented to receive such notice and the notice is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in

Global and National Commerce Act (15 U.S.C. 7001); and

(ii) the e-mail notice does not request, or contain a hypertext link to a request, that the consumer provide personal information in response to the notice.

(2) MEDIA AND WEBSITE NOTICE.—In the event notice is required to more than 5,000 individuals in 1 State and individual notice is not feasible due to lack of sufficient contact information for the individuals required to be notified, a covered entity shall—

(A) provide notice to the major media outlets serving the State or jurisdiction of the individuals believed to be affected; and

(B) place notice in a clear and conspicuous place on the website of the covered entity if the covered entity operates a website.

**SEC. 214. CONTENT OF NOTIFICATION.**

(a) IN GENERAL.—Regardless of the method by which notice is provided to individuals under section 213, such notice shall include, to the extent possible—

(1) a general description of the incident and the date or estimated date of the security breach and

the date range during which the sensitive personally identifiable information was compromised;

(2) a description of the categories of sensitive personally identifiable information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person;

(3) the acts the covered entity, or the agent of the covered entity, has taken to protect sensitive personally identifiable information from further security breach;

(4) a toll-free number—

(A) that the individual may use to contact the covered entity, or the agent of the covered entity; and

(B) from which the individual may learn what types of sensitive personally identifiable information the covered entity maintained about that individual; and

(5) the toll-free contact telephone numbers and addresses for the major credit reporting agencies if the sensitive personally identifiable information that was breached could be used to commit financial fraud or identity theft.

(b) DIRECT BUSINESS RELATIONSHIP.—Regardless of whether a covered entity or a designated third party

provides the notice required pursuant to section 211(b), such notice shall include the name of the covered entity that has the most direct relationship with the individual being notified.

**SEC. 215. COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.**

If a covered entity is required to provide notification to more than 5,000 individuals under section 211(a) and the sensitive personally identifiable information that was breached could be used to commit financial fraud or identity theft, the covered entity shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis (as defined in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)) of the timing and distribution of the notices. Such notice shall be given to the consumer 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.

**SEC. 216. NOTICE TO THE FEDERAL TRADE COMMISSION.**

A covered entity required to provide notification under section 211(a) shall provide a copy of the notification to the Federal Trade Commission not later than the date on which notice is provided to individuals required to be notified. The Federal Trade Commission shall estab-

lish procedures to ensure the attorneys general of each State with affected residents receives a copy of the notice provided to it under this section.

**SEC. 217. NOTICE TO LAW ENFORCEMENT.**

(a) DESIGNATION OF GOVERNMENT ENTITY TO RECEIVE NOTICE.—

(1) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, the Secretary of Homeland Security, in consultation with the Attorney General, shall designate a Federal Government entity to receive the notices required under section 211 and this section.

(2) RESPONSIBILITIES OF THE DESIGNATED ENTITY.—The designated entity shall—

(A) promptly provide the information that it receives to the United States Secret Service or the Federal Bureau of Investigation for law enforcement purposes; and

(B) provide the information described in subparagraph (A) as appropriate to other Federal agencies for law enforcement, national security, or data security purposes.

(b) NOTICE.—A covered entity shall notify the designated entity of the fact that a security breach has occurred if—

(1) the number of individuals whose sensitive personally identifying information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person exceeds 5,000;

(2) the security breach involves a database, networked or integrated databases, or other data system containing the sensitive personally identifiable information of more than 500,000 individuals nationwide;

(3) the security breach involves databases owned by the Federal Government; or

(4) the security breach involves primarily sensitive personally identifiable information of individuals known to the covered entity to be employees and contractors of the Federal Government involved in national security or law enforcement.

(c) DEPARTMENT OF JUSTICE REVIEW OF THRESHOLDS FOR NOTICE.—The Attorney General, in consultation with the Secretary of Homeland Security, after notice and the opportunity for public comment, and in a manner consistent with this section, shall promulgate regulations, as necessary, under section 553 of title 5, United States Code, to adjust the thresholds for notice to law enforcement and national security authorities under subsection (a) and to facilitate the purposes of this section.

(d) TIMING.—The notice required under subsection (b) shall be provided as promptly as possible, but such notice must be provided not less than 72 hours before notice is provided to an individual pursuant to section 211, or not later than 10 days after the discovery of the events requiring notice, whichever occurs first. For each breach requiring notice under this subsection, a copy of the notice to individuals required under section 211 shall also be provided to the designated entity not later than the date on which the notice is provided to affected individuals.

**SEC. 218. FEDERAL ENFORCEMENT.**

(a) IN GENERAL.—The Attorney General and the Federal Trade Commission may enforce civil violations of this subtitle.

(b) CIVIL ACTIONS BY THE ATTORNEY GENERAL OF THE UNITED STATES.—

(1) IN GENERAL.—The Attorney General may bring a civil action in the appropriate United States district court against any covered entity that engages in conduct constituting a violation of this subtitle and, upon proof of such conduct by a preponderance of the evidence, the covered entity shall be subject to a civil penalty in an amount not greater than the product of the number of violations of this subtitle and $16,500. Each failure to provide notifi-

cation to an individual as required under this subtitle shall be treated as a separate violation.

(2) PENALTY LIMITATION.—Notwithstanding any other provision of law, the total amount of the civil penalty assessed against a covered entity for conduct involving the same or related acts or omissions that results in a violation of this subtitle may not exceed $5,000,000, unless such conduct is found to be willful or intentional.

(3) DETERMINATIONS.—The determination of whether a violation of a provision of this subtitle has occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact. The determination of whether a violation of a provision of this subtitle was willful or intentional, and if so, the amount of the additional penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.

(4) ADDITIONAL PENALTY LIMIT.—If a court determines under paragraph (3) that a violation of a provision of this subtitle was willful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $5,000,000.

(c) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—If it appears that a covered entity has engaged, or is engaged, in any act or practice constituting a violation of this subtitle, the Attorney General may petition an appropriate district court of the United States for an order—

(A) enjoining such act or practice; or

(B) enforcing compliance with this subtitle.

(2) ISSUANCE OF ORDER.—A court may issue an order under paragraph (1), if the court finds that the conduct in question constitutes a violation of this subtitle.

(d) CIVIL ACTIONS BY THE FEDERAL TRADE COMMISSION.—

(1) IN GENERAL.—Compliance with the requirements imposed under this subtitle may be enforced under the Federal Trade Commission Act (15 U.S.C. 41 et seq.) by the Federal Trade Commission with respect to business entities subject to this Act. All of the functions and powers of the Federal Trade Commission under the Federal Trade Commission Act are available to the Commission to enforce compliance by any person with the requirements imposed under this title.

(2) CIVIL PENALTIES.—

(A) IN GENERAL.—Any covered entity that violates this subtitle shall be subject to a civil penalty in the amount that is not greater than the product of the number of violations of this subtitle and $16,500. Each failure to provide notification to an individual as required under this subtitle shall be treated as a separate violation.

(B) PENALTY LIMITATION.—Notwithstanding any other provision of law, the total sum of civil penalties assessed against a covered entity for all violations of the provisions of this subtitle resulting from the same or related acts or omissions may not exceed $5,000,000, unless such conduct is found to be willful or intentional.

(C) DETERMINATIONS.—The determination of whether a violation of a provision of this subtitle has occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact. The determination of whether a violation of a provision of this subtitle was willful or intentional, and if so, the amount of the additional penalty

to be imposed, if any, shall be made by the court sitting as the finder of fact.

(D) ADDITIONAL PENALTY LIMIT.—If a court determines under subparagraph (C) that a violation of a provision of this subtitle was willful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $5,000,000.

(3) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—For the purpose of the exercise by the Federal Trade Commission of its functions and powers under the Federal Trade Commission Act, a violation of any requirement or prohibition imposed under this title shall constitute an unfair or deceptive act or practice in commerce in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(I)(B)) regarding unfair or deceptive acts or practices and shall be subject to enforcement by the Federal Trade Commission under that Act with respect to any business entity, irrespective of whether that business entity is engaged in commerce or meets any other jurisdictional tests in the Federal Trade Commission Act.

(e) COORDINATION OF ENFORCEMENT.—

(1) IN GENERAL.—When opening an investigation, the Federal Trade Commission shall consult with the Attorney General.

(2) LIMITATION.—The Federal Trade Commission may initiate investigations under this subsection unless the Attorney General determines that such an investigation would impede an ongoing criminal investigation or national security activity.

(3) COORDINATION AGREEMENT.—

(A) IN GENERAL.—In order to avoid conflicts and promote consistency regarding the enforcement and litigation of matters under this Act, not later than 180 days after the enactment of this Act, the Attorney General and the Federal Trade Commission shall enter into an agreement for coordination regarding the enforcement of this Act.

(B) REQUIREMENT.—The coordination agreement entered into under subparagraph (A) shall include provisions to ensure that parallel investigations and proceedings under this section are conducted in a manner that avoids conflicts and does not impede the ability of the Attorney General to prosecute violations of Federal criminal laws.

(f) RULEMAKING.—The Federal Trade Commission may, in consultation with the Attorney General, issue such other regulations as it determines to be necessary to carry out this subtitle. All regulations promulgated under this Act shall be issued in accordance with section 553 of title 5, United States Code.

(g) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this subtitle are cumulative and shall not affect any other rights and remedies available under law.

(h) FRAUD ALERT.—Section 605A(b)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681c–1(b)(1)) is amended by inserting ", or evidence that the consumer has received notice that the consumer's financial information has or may have been compromised," after "identity theft report".

**SEC. 219. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

(a) IN GENERAL.—

(1) CIVIL ACTIONS.—

(A) IN GENERAL.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that a covered entity has

violated this subtitle, the State, as parens patriae, may bring a civil action on behalf of the residents of the State to—

(i) enjoin that practice;

(ii) enforce compliance with this subtitle; or

(iii) impose a civil penalty in an amount not greater than the product of the number of violations of this subtitle and $16,500.

(B) FAILURE TO PROVIDE NOTIFICATION.—For purposes of subparagraph (A)(iii), each failure to provide notification to an individual as required under this subtitle shall be treated as a separate violation.

(2) PENALTY LIMITATION.—

(A) IN GENERAL.—Notwithstanding any other provision of law, the total sum of civil penalties assessed against a covered entity for all violations of the provisions of this subtitle resulting from the same or related acts or omissions may not exceed $5,000,000, unless such conduct is found to be willful or intentional.

(B) DETERMINATIONS.—The determination of whether a violation of a provision of this

subtitle has occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact. The determination of whether a violation of a provision of this subtitle was willful or intentional, and if so, the amount of the additional penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.

(C) ADDITIONAL PENALTY LIMIT.—If a court determines under subparagraph (B) that a violation of a provision of this subtitle was willful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $5,000,000.

(3) NOTICE.—

(A) IN GENERAL.—Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Attorney General of the United States and the Federal Trade Commission—

(i) written notice of the action; and

(ii) a copy of the complaint for the action.

(B) EXEMPTION.—

(i) IN GENERAL.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subtitle, if the State attorney general determines that it is not feasible to provide the notice described in such subparagraph before the filing of the action.

(ii) NOTIFICATION.—In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the Attorney General of the United States and the Federal Trade Commission at the time the State attorney general files the action.

(b) FEDERAL PROCEEDINGS.—Upon receiving notice under subsection (a)(2), the Attorney General and the Federal Trade Commission shall have the right to—

(1) move to stay the action, pending the final disposition of a pending Federal proceeding or action;

(2) initiate an action in the appropriate United States district court under section 218 and move to consolidate all pending actions, including State actions, in such court;

(3) intervene in an action brought under subsection (a)(2); and

(4) file petitions for appeal.

(c) PENDING PROCEEDINGS.—If the Attorney General or the Federal Trade Commission initiates a criminal proceeding or civil action for a violation of a provision of this subtitle, or any regulations thereunder, no attorney general of a State may bring an action for a violation of a provision of this subtitle against a defendant named in the Federal criminal proceeding or civil action.

(d) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this subtitle regarding notification shall be construed to prevent an attorney general of a State from exercising the powers conferred on such attorney general by the laws of that State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

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

(e) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in—

(A) the district court of the United States that meets applicable requirements relating to

venue under section 1391 of title 28, United States Code; or

(B) another court of competent jurisdiction.

(2) SERVICE OF PROCESS.—In an action brought under subsection (a), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

(f) NO PRIVATE CAUSE OF ACTION.—Nothing in this subtitle establishes a private cause of action against a business entity for violation of any provision of this subtitle.

**SEC. 220. EFFECT ON FEDERAL AND STATE LAW.**

(a) PREEMPTION.—For a covered entity that is subject to this subtitle, the provisions of this subtitle shall supersede any other provision of Federal law, or any provisions of the law of any State or political subdivision of a State requiring notification of a security breach of sensitive personally identifiable information that are less stringent than the requirements of this subtitle.

(b) CONSUMER PROTECTION LAWS.—Except as provided in subsection (a), this section 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.—Nothing in this Act shall be construed to preempt the applicability of—

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

(2) any other State law to the extent that the law relates to acts of fraud.

(d) PRESERVATION OF FTC AUTHORITY.—Nothing in this Act may be construed in any way to limit the authority of the Federal Trade Commission under any other provision of law.

(e) PRESERVATION OF FCC AUTHORITY.—Nothing in this Act may be construed in any way to limit the authority of the Federal Communications Commission under any other provision of law.

**SEC. 221. REPORTING ON EXEMPTIONS.**

Not later than 18 months after the date of enactment of this Act, and upon the request by Congress thereafter, the Attorney General, in consultation with the Secretary of Homeland Security, shall submit a report to Congress on the number and nature of security breaches subject to the national security and law enforcement exemptions under section 212(a).

**SEC. 222. EFFECTIVE DATE.**

This subtitle shall take effect on the expiration of the date that is 90 days after the date of enactment of this Act.

# TITLE III—COMPLIANCE WITH STATUTORY PAY-AS-YOU-GO ACT

**SEC. 301. BUDGET COMPLIANCE.**

The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement titled ''Budgetary Effects of PAYGO Legislation'' for this Act, submitted for printing in the Congressional Record by the Chairman of the Senate Budget Committee, provided that such statement has been submitted prior to the vote on passage.

○