114TH CONGRESS
1ST SESSION

S. _____

To require notice of data security breaches, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. WARNER introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To require notice of data security breaches, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Data Breach Notification Act of 2015''.

SEC. 2. DEFINITIONS.

For purposes of this Act, the following definitions shall apply:

(1) AFFILIATE.—The term ''affiliate'' means any company that controls, is controlled by, or is under common control with another company.

(2) AGENCY.—The term ''agency'' has the same meaning as in section 551(1) of title 5, United States Code.

(3) BREACH OF SECURITY.—

(A) IN GENERAL.—The term ''breach of security'' means the unauthorized acquisition of data in electronic form containing sensitive account information or sensitive personal information.

(B) EXCEPTION FOR DATA THAT IS NOT IN USABLE FORM.—

(i) IN GENERAL.—The term ''breach of security'' does not include the unauthorized acquisition of sensitive account information or sensitive personal information that is maintained or communicated in a manner that is not usable—

(I) to commit identity theft; or

(II) to make fraudulent transactions on financial accounts.

(ii) RULE OF CONSTRUCTION.—For purposes of this subparagraph, information that is maintained or communicated in a manner that is not usable includes any information that is maintained or commu-

nicated in an encrypted or redacted form, or secured by any other method or technology that renders the information unreadable, indecipherable, or incapable of either identifying a financial account or personally identifying a specific individual.

(4) CONSUMER REPORTING AGENCY THAT COMPILES AND MAINTAINS FILES ON CONSUMERS ON A NATIONWIDE BASIS.—The term ''consumer reporting agency that compiles and maintains files on consumers on a nationwide basis'' has the same meaning as in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

(5) COVERED ENTITY.—

(A) IN GENERAL.—The term ''covered entity'' means any—

(i) entity, the business of which is engaging in financial activities, as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k));

(ii) financial institution, including any institution described in section 313.3(k) of title 16, Code of Federal Regulations, as in effect on the date of enactment of this Act;

(iii) entity that maintains or otherwise possesses information that is subject to section 628 of the Fair Credit Reporting Act (15 U.S.C. 1681w); or

(iv) except as provided in subparagraph (B), other individual, partnership, sole proprietorship, corporation, nonprofit corporation, trust, estate, cooperative, association, institution, service provider or other entity that acquires, maintains, stores, utilizes, or communicates sensitive account information or sensitive personal information.

(B) EXCEPTION.—The term ''covered entity'' does not include—

(i) any agency or any other unit of Federal, State, or local government or any subdivision of the unit; or

(ii) any entity which is a covered entity for purposes of the regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) to the extent that such entity is subject to the re-

quirements of such regulations with respect to protected health information.

(6) DATA IN ELECTRONIC FORM.—The term ''data in electronic form'' means any sensitive account information or sensitive personal information stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

(7) FINANCIAL HARM.—

(A) IN GENERAL.—The term ''financial harm'' means material financial loss to, or civil or criminal penalties imposed on, an individual, due to the unauthorized use of sensitive account information or sensitive personal information relating to the individual.

(B) EXCEPTION.—The term ''financial harm'' does not include—

(i) changing a financial account number or closing a financial account; or

(ii) harm that does not result from identity theft or account fraud.

(8) FINANCIAL INSTITUTION.—The term ''financial institution'' has the same meaning as in section 509(3) of the Gramm-Leach-Bliley Act (15 U.S.C. 6809(3)).

(9) FUNCTIONAL REGULATOR.—The term ''Functional Regulator'' means the Federal department or agency, other than the Federal Trade Commission, that has jurisdiction to bring enforcement actions against covered entities—

(A) under section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), in the case of—

(i) national banks, Federal branches and Federal agencies of foreign banks, and Federal savings associations, by the Office of the Comptroller of the Currency;

(ii) 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, by the Board; and

(iii) banks insured by the Federal Deposit Insurance Corporation (other than

members of the Federal Reserve System), insured State branches of foreign banks, and State savings associations, by the Board of Directors of the Federal Deposit Insurance Corporation; and

(B) under the Federal Credit Union Act (12 U.S.C. 1751 et seq.) by the Board of the National Credit Union Administration with respect to any Federally insured credit union;

(C) under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.) by the Securities and Exchange Commission with respect to any broker or dealer;

(D) under the Investment Company Act of 1940 (15 U.S.C. 80a-1 et seq.) by the Securities and Exchange Commission with respect to investment companies;

(E) under the Investment Advisers Act of 1940 (15 U.S.C. 80b-1 et seq.) by the Securities and Exchange Commission with respect to investment advisers registered under that Act;

(F) under 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, sub-

ject to section 104 of the Gramm-Leach-Bliley Act (15 U.S.C. 6701), except that in any State in which the State insurance authority elects not to exercise this power, the enforcement authority pursuant to this Act shall be exercised by the Federal Trade Commission;

(G) under part A of subtitle VII of title 49, United States Code, by the Secretary of Transportation with respect to any air carrier or foreign air carrier subject to that part;

(H) under the Packers and Stockyards Act, 1921 (7 U.S.C. 181 et seq.) (except as provided in section 406 of that Act (7 U.S.C. 226, 227)), by the Secretary of Agriculture with respect to any activities subject to that Act; and

(I) under the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.) by the Farm Credit Administration with respect to any Federal land bank, Federal land bank association, Federal intermediate credit bank, or production credit association.

(10) SENSITIVE ACCOUNT INFORMATION.—

(A) IN GENERAL.—The term ''sensitive account information'' means the first and last name, address, or telephone number of an indi-

vidual in combination with a financial account number relating to an individual, including a bank account number, credit card number, or debit card number, and any security code, access code, password, or other personal identification information that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account.

(B) EXCEPTION.—The term ''sensitive account information'' does not include a financial account number that is encrypted, redacted, or secured by any other method or technology that removes elements that identify a financial account or that otherwise renders the financial account information unusable.

(11) SENSITIVE PERSONAL INFORMATION.—

(A) IN GENERAL.—The term ''sensitive personal information'' means the first and last name, address, or telephone number of an individual, in combination with any of the following relating to the individual:

(i) Social security account number.

(ii) Driver's license number or equivalent State identification number, passport

number, military identification number, or other unique identification number issued on a government document and used to verify the identity of a specific individual.

(iii) Taxpayer identification number.

(B) EXCEPTION.—The term ''sensitive personal information'' does not include —

(i) publicly available information about an individual that is lawfully made available to the general public by a Federal, State, or local government entity or by widely distributed media; or

(ii) information that is encrypted, redacted, or secured by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

(12) SERVICE PROVIDER.—The term ''service provider'' means a covered entity that provides electronic data transmission, routing, and transient storage, or connections to its system or network, where such entity providing such services does not inspect or access the content of the electronic data, is not the sender or the intended recipient of the data, and does not differentiate sensitive account information

or sensitive personal information from other information that such entity transmits, routes, stores, or for which such entity provides connections. Any such entity shall be treated as a service provider under this Act only to the extent that it is engaged in the provision of such transmission, routing, transient storage, or connections.

SEC. 3. PROTECTION OF INFORMATION AND INVESTIGATION OF SECURITY BREACH.

(a) SECURITY PROCEDURES REQUIRED.—

(1) IN GENERAL.—Each covered entity shall implement, maintain, and enforce reasonable policies and procedures to protect the confidentiality and security of, sensitive account information and sensitive personal information that is maintained or is being communicated by, or on behalf of, a covered entity from the unauthorized use of the information that is reasonably likely to result in financial harm to the individual to whom the information relates.

(2) LIMITATION.—Any policy or procedure implemented or maintained under paragraph (1) shall be appropriate to—

(A) the size and complexity of the covered entity;

(B) the nature and scope of the activities of the covered entity; and

(C) the sensitivity of the information to be protected.

(b) INVESTIGATION REQUIRED.—

(1) IN GENERAL.—If a covered entity determines that a breach of security has or may have occurred in relation to sensitive account information or sensitive personal information that is maintained or is being communicated by, or on behalf of, the covered entity, the covered entity shall conduct an investigation to—

(A) assess the nature and scope of the breach;

(B) identify any sensitive account information or sensitive personal information that may have been involved in the breach, and the identity of any individuals to whom that information relates; and

(C) determine if the sensitive account information or sensitive personal information is reasonably likely to be, or has been, acquired by an unauthorized person, and is reasonably likely to have caused or will cause financial harm to the individuals to whom the information relates.

(2) NEURAL NETWORKS AND INFORMATION SECURITY PROGRAMS.—In determining the likelihood of misuse of sensitive account information under paragraph (1)(C), a covered entity shall consider whether any neural network or security program has detected, or is likely to detect or prevent, fraudulent transactions resulting from the breach of security.

(c) UNFAIR OR DECEPTIVE ACT OR PRACTICE.—It shall be an unfair or deceptive act or practice within the meaning of section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1)) for a covered entity, in connection with the protection of sensitive account information or sensitive personal information, to engage in a practice of failing to maintain reasonable security procedures.

SEC. 4. NOTIFICATION OF SECURITY BREACH.

(a) NOTIFICATION.—

(1) IN GENERAL.—A covered entity that owns or licenses data in electronic form containing sensitive account information or sensitive personal information shall give notice of any breach of security, following discovery by the covered entity of the breach of security, to each individual who is a citizen or resident of the United States whose data in electronic form was, or that the covered entity reasonably believes to have been, acquired by an unauthor-

ized person and that the covered entity reasonably believes has caused or will cause financial harm.

(2) LAW ENFORCEMENT.—A covered entity shall notify the United States Secret Service or the Federal Bureau of Investigation of the fact that a breach of security has occurred if the number of individuals whose personal information the covered entity reasonably believes to have been accessed and acquired by an unauthorized person exceeds 10,000.

(b) SPECIAL NOTIFICATION REQUIREMENTS.—

(1) NOTICE BY CONTRACTED COVERED ENTITIES.—

(A) IN GENERAL.—Subject to the exceptions in subparagraphs (B) and (C), in the event of a breach of security of a system maintained by a covered entity that has been directly contracted by another covered entity to maintain, store, transmit, or process data in electronic form containing sensitive account information or sensitive personal information on its behalf, the breached covered entity shall, as expeditiously as possible and without unreasonable delay following discovery of the breach of security, notify such other covered entity of the breach of security before, and in addition to,

providing notification as required under subsection (a).

(B) ELECTION BY COVERED ENTITY RECEIVING BREACH NOTICE FROM CONTRACTED COVERED ENTITY.—A covered entity that receives notification pursuant to subparagraph (A) from a contracted covered entity that incurred the breach of security may elect to provide notification to affected individuals that are its customers, clients, employees, or contractors under subsection (a) in place of notification to the same individuals by the contracted covered entity that incurred the breach of security, provided that the contracted covered entity that incurred the breach of security—

(i) is party to a valid and enforceable written contract under which it maintains, stores, transmits, or processes data in electronic form containing sensitive account information or sensitive personal information on behalf of the covered entity electing to provide notice;

(ii) has consented in the written contract described in clause (i) that the covered entity electing to provide notice has

the right to provide such notice in compliance with all of the requirements of subsection (a) in place of notification by the contracted covered entity that incurred the breach of security; and

(iii) maintains responsibility for providing notice with respect to any affected individuals not notified by the covered entity electing to provide notice.

(C) CONTRACTED COVERED ENTITY OBLIGATIONS AFTER ELECTION BY COVERED ENTITY RECEIVING BREACH NOTIFICATION.—

(i) AFFIRMATIVE OBLIGATIONS AND LIABILITY FOR NOTICE.—If a covered entity elects, pursuant to subparagraph (B), to provide notice, as required under subsection (a), in place of notification by the contracted covered entity that incurred the breach of security, the contracted covered entity that incurred the breach of security shall—

(I) ensure that the notification required under subsection (a) is made by the covered entity electing to provide notice in place of notification by

the covered entity that incurred the breach of security; and

(II) provide all required information about the breach of security to, and cooperate in all respects with, the covered entity electing to provide notice so that the notification is made as required under subsection (a).

(ii) RELIEF OF OBLIGATION TO PROVIDE NOTICE TO AFFECTED INDIVIDUALS.—A contracted covered entity that incurred the breach of security shall be relieved of its obligation to provide notification as required under subsection (a) with respect to the affected individuals notified by the covered entity electing to provide notice pursuant to subparagraph (B), provided that all of the following conditions have been met—

(I) notice to an affected covered entity has been made under subparagraph (A);

(II) an election to notify certain individuals has been made by an af-

fected covered entity under subparagraph (B); and

(III) the covered entity that incurred the breach has fulfilled all of its affirmative obligations under clause (i) of this subparagraph.

(D) EXCEPTION FOR SERVICE PROVIDERS.—In the event of a breach of security of a system or network maintained by a service provider, the obligations under subparagraphs (A), (B), and (C) for a contracted covered entity that incurred a breach of security shall not apply to such service provider, who shall be subject instead to the obligations set forth in paragraph (2) of this subsection.

(2) SERVICE PROVIDERS.—

(A) IN GENERAL.—Subject to the exception set forth in subparagraph (C), if a service provider discovers or otherwise becomes aware of a breach of security of its system or network involving data in electronic form that may contain sensitive account information or sensitive personal information that is owned or licensed by a covered entity that connects to or uses a system or network provided by the service pro-

vider for the purpose of transmitting, routing, or providing transient storage of such data, such service provider shall promptly notify the covered entity who initiated such connection, transmission, routing, or storage.

(B) SERVICE PROVIDER DUTY TO INVESTIGATE.—In addition to its obligations under section 3, a service provider that discovers or otherwise becomes aware of a breach of security as specified in subparagraph (A) shall use all best efforts to investigate and determine the identity of the covered entity who initiated such connection, transmission, routing, or storage.

(C) EXCEPTION FOR NON-IDENTIFICATION OF COVERED ENTITY WHO INITIATED SERVICE.—Notwithstanding subparagraphs (A) and (B), in the event a service provider cannot reasonably identify the covered entity who initiated such connection, transmission, routing, or storage, the service provider shall—

(i) provide the notification as required under subsection (a) by substitute notification pursuant to subsection (d)(2); and

(ii) promptly notify the United States Secret Service or Federal Bureau of Inves-

tigation, and the Federal Trade Commission, of the breach of security it has discovered or otherwise become aware.

(D) COVERED ENTITIES WHO RECEIVE NOTICE FROM SERVICE PROVIDERS.—A covered entity that owns or licenses sensitive account information or sensitive personal information that receives notification, pursuant to subparagraph (A), from a service provider that discovered or became aware of a breach of security of its system or network as specified under subparagraph (A), shall provide the notification required under subsection (a) on behalf of the service provider, provided that the service provider has first notified the covered entity that owns or licenses such information, and initiated the service, of the breach of security pursuant to subparagraph (A).

(E) SERVICE PROVIDER OBLIGATIONS TO PROVIDE INFORMATION TO COVERED ENTITIES.—For each covered entity obligated to provide notice on behalf of a service provider that incurred, discovered, or was made aware of a breach of security of its system pursuant to subparagraph (D), the service provider shall

provide all required content under subsection (d) about the breach of security to, and cooperate in all respects with, the covered entity providing the notification required under subsection (a).

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—Unless subject to a delay authorized under paragraph (3), a notification required under subsection (a) or (b) with respect to a breach of security shall be made as expeditiously as practicable and without unreasonable delay.

(2) REASONABLE DELAY.—For purposes of paragraph (1), a reasonable delay may include any time necessary for the purpose of allowing the covered entity to—

(A) determine the scope of the breach of security;

(B) identify individuals affected by the breach of security; and

(C) restore the reasonable integrity of the data system that was breached.

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

(A) LAW ENFORCEMENT.—If a Federal law enforcement agency determines that the notification required under subsection (a) would interfere with a criminal investigation, such notification shall be delayed upon the written request of the law enforcement agency for any period which the law enforcement agency determines is reasonably necessary. The law enforcement agency may, by a subsequent written request, revoke such delay or extend the period set forth in the original request made under this subparagraph by a subsequent request if further delay is necessary.

(B) NATIONAL SECURITY.—If a Federal national security agency or homeland security agency determines, following referral by a Federal law enforcement agency, that the notification required under this section would threaten national or homeland security, such notification may be delayed upon the written request of the national security agency or homeland security agency for any period which the national security agency or homeland security agency determines is reasonably necessary. A Federal national security agency or homeland security

agency may revoke such delay or extend the period set forth in the original request made under this subparagraph by a subsequent written request if further delay is necessary.

(d) METHOD AND CONTENT OF NOTIFICATION.—

(1) DIRECT NOTIFICATION.—

(A) METHOD OF NOTIFICATION.—A covered entity required to provide notification to an individual under subsection (a) or (b) shall be in compliance with such requirement if the covered entity provides such notice by 1 of the following methods:

(i) Written notification, sent to the postal address of the individual in the records of the covered entity.

(ii) Telephone.

(iii) Email or other electronic means.

(B) CONTENT OF NOTIFICATION.—Regardless of the method by which notification is provided to an individual under subparagraph (A) with respect to a breach of security, such notification, to the extent practicable, shall include—

(i) the date, estimated date, or estimated date range of the breach of security;

(ii) a description of the type of sensitive account information or sensitive personal information that was accessed and acquired, or reasonably believed to have been accessed and acquired, by an unauthorized person as a part of the breach of security; and

(iii) information that the individual can use to contact the covered entity to inquire about—

(I) the breach of security; or

(II) the sensitive account information or sensitive personal information about the consumer which the covered entity reasonably believes to have been acquired by an unauthorized person.

(2) SUBSTITUTE NOTIFICATION.—

(A) CIRCUMSTANCES GIVING RISE TO SUBSTITUTE NOTIFICATION.—A covered entity required to provide notification to an individual under subsection (a) may provide substitute notification in lieu of the direct notification required by paragraph (1) if such direct notification is not feasible due to—

(i) excessive cost to the covered entity required to provide such notification relative to the resources of such covered entity; or

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

(B) FORM OF SUBSTITUTE NOTIFICATION.—Such substitute notification shall include at least 1 of the following:

(i) A conspicuous notice on the Internet website of the covered entity (if such covered entity maintains such a website).

(ii) Notification in print and to broadcast media, including major media in metropolitan and rural areas where the individuals whose personal information was, or is reasonably believed to have been, acquired reside.

SEC. 5. ENFORCEMENT BY FUNCTIONAL REGULATORS.

(a) GENERAL APPLICATION.—Except as set forth in section 6 of this Act, notwithstanding any other provision of law, the requirements of section 3 and section 4 shall be enforced by each Functional Regulator of appropriate jurisdiction and apply to the following covered entities:

(1) Entities, the business of which is engaging in financial activities, as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial institutions, including any institution described in section 313.3(k) of title 16, Code of Federal Regulations, as in effect on the date of enactment of this Act.

(3) Entities that maintain or otherwise possesses information that is subject to section 628 of the Fair Credit Reporting Act (15 U.S.C. 1681w).

(b) ENFORCEMENT BY FUNCTIONAL REGULATORS.—

(1) VIOLATIONS.—For the purpose of the exercise by any Functional Regulator of its powers under any Act referred to in section 2(9)(A), violation of section 3 or 4 of this Act is deemed to be an unfair or deceptive act or practice prescribed under section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

(2) POWERS OF FUNCTIONAL REGULATORS.—

(A) IN GENERAL.—Except as provided in subsection (a), each Functional Regulator shall enforce this Act in the same manner, by the same means, and with the same powers and duties as though all applicable terms and provi-

sions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. In addition to its powers under any provision of law specifically referred to in section 2(9), each Functional Regulator may exercise, for the purpose of enforcing compliance with any requirement imposed under this Act, any other authority conferred on it by law.

(B) PRIVILEGES AND IMMUNITIES.—Any person who violates section 3 or 4 shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

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

(A) $5,000,000 for all violations of section 3 resulting from the same related act or omission; and

(B) $5,000,000 for all violations of section 4 resulting from a single breach of security.

SEC. 6. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) GENERAL APPLICATION.—For any covered entity not subject to enforcement under section 5 of this Act, the requirements of sections 3 and 4 shall be enforced by the Federal Trade Commission and apply to—

(1) those individuals, partnerships, corporations, trusts, estates, cooperatives, associations, institutions, service providers, and other entities over which the Federal Trade Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)); and

(2) notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.).

(b) ENFORCEMENT BY FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 3 or 4 of this Act is deemed to be an unfair or deceptive act or practice proscribed under section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

(2) POWERS OF FEDERAL TRADE COMMISSION.—

(A) IN GENERAL.—Except as provided in subsection (a), the Federal Trade Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act.

(B) PRIVILEGES AND IMMUNITIES.—Any person who violates section 3 or 4 shall be subject to the penalties and entitled to the privileges and immunities provided in such Act.

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

(A) $5,000,000 for all violations of section 3 resulting from the same related act or omission; and

(B) $5,000,000 for all violations of section 4 resulting from a single breach of security.

SEC. 7. COORDINATION OF ENFORCEMENT POLICIES, ACTIONS, AND PENALTIES.

(a) EQUIVALENT POLICIES, ACTIONS, AND PENALTIES FOR COVERED ENTITIES.—The Functional Regulators and the Federal Trade Commission shall coordinate their enforcement policies, actions, and penalties so that violations of this Act are enforced and penalized equivalently among covered entities.

(b) COORDINATION AMONG FUNCTIONAL REGULATORS AND FEDERAL TRADE COMMISSION.—In order to promote the development and application of fair, consistent, and equivalent enforcement actions and penalties to apply to covered entities for violations of this Act, the Functional Regulators and the Federal Trade Commission shall, within 180 days after the date of the enactment of this Act, enter into a single memorandum of understanding regarding the coordination of enforcement policies, procedures, and penalties in order to—

(1) ensure that the circumstances triggering enforcement actions and the imposition of penalties for violations of this Act are equivalent for all covered entities;

(2) ensure that the scope of penalties to be imposed against covered entities for violations of this Act are equivalent for all covered entities for similar violations of this Act; and

(3) ensure that enforcement actions are not pursued against the same covered entity for the same violation by more than one Federal department or agency, whether it is a Functional Regulator or the Federal Trade Commission.

SEC. 8. EFFECT ON OTHER LAWS.

(a) CONGRESSIONAL INTENT.—The purposes of this Act are to—

(1) establish uniform, national data security and breach notification standards; and

(2) expressly preempt related State laws and common law to ensure uniformity of this Act's standards and consistency of their application across jurisdictions, thereby eliminating the administrative costs and burdens placed on interstate commerce from varying standards.

(b) PREEMPTION OF STATE LAWS AND COMMON LAW.—No law, rule, regulation, requirement, standard, or other provision having the force and effect of law relating to data security or notification following a breach of data security shall be imposed by a State or political subdivision of a State on a person subject to this Act.

SEC. 9. EFFECTIVE DATE.

This Act shall take effect on the date that is 180 days after the date of enactment of this Act.