National Data Breach Notification/Incident Reporting Act

SEC. 101. NOTICE TO INDIVIDUALS.

(a) IN GENERAL.—Each covered entity shall, following the discovery and confirmation of a security breach involving sensitive personal information of a citizen or lawful permanent resident of the United States, notify each individual whose sensitive personal information (as defined in section 113) was, or is reasonably believed to have been, accessed or acquired as a result of the security breach.

(b) OBLIGATIONS OF AND TO OWNER OR LICENSEE.—

(1) NOTICE TO OWNER OR LICENSEE.—Any covered entity that uses, accesses, transmits, stores, disposes of, or collects sensitive personal information that the covered entity does not own or license shall notify the owner or licensee of the information following the discovery and confirmation of a security breach involving such information.

(2) NOTICE BY OWNER, LICENSEE, OR OTHER DESIGNATED THIRD PARTY.—Nothing in this title shall prevent or abrogate an agreement between a covered entity required to provide notice under this section and a designated third party, including an owner or licensee of the sensitive personal information subject to the security breach, to provide the notice required under subsection (a).

(3) COVERED ENTITY RELIEVED FROM PROVIDING NOTICE.—A covered entity obliged to provide notice under subsection (a) shall be relieved of such obligation if an owner or licensee of the sensitive personal information subject to the security breach, or other designated third party, provides such notice.

(c) OBLIGATIONS OF SERVICE PROVIDERS.— If a service provider becomes aware of a security breach involving sensitive personal 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 promptly notify the covered entity that initiated such connection, transmission, routing, or storage of the security breach if the covered entity can be reasonably identified and also notify the entity designated to receive notification pursuant to subsection 105(d).

(d) TIMELINESS OF NOTICE.—All notice required under this section shall be made within 30 days following the discovery and confirmation by the covered entity or service provider of a security breach, except as provided in subsections 101(e), 102(a), 106(a), or 106(b). A covered entity or service provider shall, upon the request of the Commission, provide records or other evidence of the notice required under this section.

(e) DELAY OR WAIVER OF NOTICE FOR LAW ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—

(1) IN GENERAL.— Upon written notification from a Federal law enforcement agency to the covered entity that experienced the breach, notice to individuals shall be delayed if a Federal law enforcement agency determines that such notice:

(A) would impede a criminal investigation or national security activity;

(B) could reveal sensitive sources and methods or similarly impede the ability of an agency or department to conduct criminal investigations or national security activities; or

(C) could cause damage to national security.

(2) EXTENDED DELAY OF NOTICE.—If the notice required under subsection (a) is delayed pursuant to paragraph (1), a covered entity shall give the notice 30 days after the day such delay was invoked unless the Federal law enforcement agency provides in its written notification that extended delay is necessary. Such notifications for extended delay shall specify a period of delay for up to one year, subject to renewal. The Federal law enforcement agency may revoke the delay by a subsequent written notification as appropriate.

(3) WAIVER OF NOTICE.—Notice to individuals shall not be required if the Attorney General, Director of National Intelligence, or head of a Federal law enforcement agency determines that such notice reasonably could be expected to cause damage to the national security or a department or agency's ability to conduct national security activities and provides written notification to the covered entity waiving such notice.

(4) IMMUNITY.—No cause of action shall lie in any court against any Federal agency or department or covered entity for acts relating to the delay or waiver of notice for law enforcement or national security purposes under this section.

SEC. 102. EXEMPTIONS FROM NOTIFICATIONS TO INDIVIDUALS.

(a) SAFE HARBOR. —

(1) IN GENERAL. —A business entity is exempt from the notification requirement under section 101, if the following requirements are met:

(A) RISK ASSESSMENT. —A risk assessment, in accordance with paragraph

(3), is conducted by or on behalf of the covered entity that concludes that there is no reasonable risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personal information was subject to the security breach.

(B) NOTICE TO COMMISSION. —Without unreasonable delay and not later than 30 days after the discovery and confirmation of a security breach, unless extended by the Commission or a Federal law enforcement agency under section 101 (in which case, before the extended deadline), the covered entity notifies the Commission, in writing, of—

(i) the results of the risk assessment; and

(ii) the decision by the covered entity to invoke the risk assessment exemption described under subparagraph (A).

(C) DETERMINATION BY COMMISSION. —During the period beginning on the date on which the notification described in subparagraph (B) is submitted and ending 10 days after such date, the Commission has not issued a determination in writing that a notification should be provided under section 101, the exemption shall be deemed to have been granted.

(D) DELEGATION.—The Commission may delegate authority pursuant to this section to the Federal Breach Notification Recipient or another Federal department or agency, designated by joint agreement with the Secretary of Homeland Security and the Attorney General, in consultation with the National Cyber Director.

(2) REBUTTABLE PRESUMPTION. —For purposes of paragraph (1) —

(A) the rendering of sensitive personal information at issue is unusable, unreadable, or indecipherable through a security technology generally accepted by experts in the field of information security shall establish a rebuttable presumption that such reasonable risk does not exist; and

(B) any such presumption shall be rebuttable by facts demonstrating the security technologies or methodologies in a specific case have been, or are reasonably likely to have been, compromised.

(3) RISK ASSESSMENT REQUIREMENTS. —A risk assessment is in accordance with this paragraph if the following requirements are met:

(A) PROPERLY CONDUCTED. —The risk assessment is conducted in a reasonable manner or according to standards generally accepted by experts in the field of information security.

(B) LOGGING DATA REQUIRED. —The risk assessment includes logging data, as applicable and to the extent available, for a period of at least six months before the discovery and confirmation of a security breach—

(i) for each communication or attempted communication with a database or data system containing sensitive personal information, the data system communication information for the communication or attempted communication, including any Internet addresses, and the data and time associated with the communication or attempted communication; and

(ii) all log-in information associated with databases or data systems containing sensitive personal information, including both administrator and user log-in information.

(C) FRAUDULENT OR MISLEADING INFORMATION. —The risk assessment does not contain fraudulent or deliberately misleading information.

(b) FINANCIAL FRAUD PREVENTION EXEMPTION. —

(1) IN GENERAL. —A business entity is exempt from the notification requirement under section 101 if the business entity uses or participates in a security program that—

(A) effectively blocks the use of the sensitive personal information to initiate unauthorized financial transactions before they are charged to the account of the individual; and

(B) provides notification to affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

(2) LIMITATION. —The exemption in paragraph (1) does not apply if the information subject to the breach includes the individual's first and last names or any other type of sensitive personal information other than a credit card number or credit card security code.

SEC. 103. METHODS OF NOTICE TO INDIVIDUALS.

(a) IN GENERAL.—Notice provided by a covered entity as required by section 101 shall be sufficient if it includes individual notice, web site or digital interface notice, and, if required, media notice, as described below.

(1) INDIVIDUAL NOTICE.—Notice to individuals shall be provided by one of the following means:

(A) written notice to the last known mailing address of the individual in the records of the covered entity;

(B) telephone notice reasonably calculated to notify the individual personally;

(C) e-mail notice, if 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 (section 7001 of title 15, United States Code); or

(D) if the covered entity does not have any of the means of contacting the individual specified in paragraphs (A), (B), or (C), a conspicuous message reasonably calculated to notify the individual personally through their account with the covered entity's website or other digital interface, such as a mobile application.

(2) WEB SITE OR DIGITAL INTERFACE NOTICE.—If a covered entity subject to the requirements of section 101 maintains a website or other digital interface, such as a mobile application, such entity shall post conspicuous notice on that website and interface for a period of not less than 90 days.

(3) MEDIA NOTICE.—If the number of residents of a State whose sensitive personal information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person exceeds 5,000, the covered entity shall provide notice to media reasonably calculated to reach such individuals, such as major media outlets serving the relevant State or jurisdiction.

(b) MODIFIED NOTICE BY RULEMAKING.—The Commission may, by rule promulgated under section 553 of title 5, United States Code, amend the method of notice required by this section in a manner that will accomplish the purposes of this title.

SEC. 104. CONTENT OF NOTICE TO INDIVIDUALS.

(a) IN GENERAL.—Regardless of the method by which notice is provided to individuals under section 103, such notice shall include—

(1) a description of the categories of sensitive personal information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, including the entity breached and, to the extent possible, the estimated date range of the security breach;

(2) contact information, including a telephone number and electronic mail address,—

(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 personal information the covered entity maintained about that individual;

(3) the toll-free contact telephone numbers and website addresses for the major credit reporting agencies and the Commission; and

(4) regardless of whether the covered entity or a designated third party provides notice pursuant to section 101 of this title, identification of the covered entity that initially collected the individual's sensitive personal information, as practicable.

(b) OBLIGATION TO PROVIDE CREDIT MONITORING.— If the breach involved sensitive personal information as defined in paragraph 113(d)(1) or subsequent rulemaking, the covered entity must ensure that the notice to individuals includes instructions for activating credit monitoring not otherwise freely available for at least two years without cost to the individual.

(c) ADDITIONAL CONTENT.—Notwithstanding section 108 of this title, a State may require that a notice under subsection (a) shall also include information regarding victim protection assistance provided for by that State.

(d) MODIFIED CONTENT BY RULEMAKING.—The Commission may, by rule promulgated under section 553 of title 5, United States Code, amend the content of notice required by this section in a manner that will accomplish the purposes of this title.

SEC. 105. COORDINATION OF NOTICE WITH CREDIT REPORTING AGENCIES.

Where a covered entity is required to provide notice to more than 5,000 individuals under section 101, the covered entity shall also notify all credit 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 (section 1681a(p) of title 15, United States Code)) of the timing and distribution of the notices. Such notification 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. 106. NOTIFICATION TO THE FEDERAL GOVERNMENT AND FOR OTHER PURPOSES.

(a) NOTIFICATION OF HIGH-RISK BREACHES OF SENSITIVE PERSONAL INFORMATION.

(1) IN GENERAL.—Any covered entity shall notify the Federal Breach Notification Recipient if a security breach—

(A) is reasonably believed to involve the access or acquisition of the sensitive personal information of more than 5,000 individuals;

(B) involves access to, or the integrity of, a database, networked or integrated databases, or other information system containing the sensitive personal
information of more than 500,000 individuals;

(2) COMMISSION RULEMAKING.—Not later than one year after the date of the enactment of this title—

(A) in consultation with the Attorney General, the Secretary of Homeland Security, and the National Cyber Director, the Commission shall promulgate regulations, as necessary, under section 553 of title 5, United States Code, defining what information about incidents, threats, and vulnerabilities notifications under subsection (a)(1) must contain; and

(B) in consultation with the Attorney General, the Secretary of Homeland Security, and the National Cyber Director, the Commission shall promulgate regulations, as necessary, under section 553 of title 5, United States Code, to adjust the thresholds for notification to the authorities under subsections (a)(1) and (b)(1) to ensure adequate information protection if any information required to be submitted under paragraph (a)(3)(A) is subject to information protection controls established by federal law or regulation apart from this title, and to otherwise facilitate the purposes of this section.

(b) NOTIFICATION OF OTHER SECURITY BREACHES WITH HEIGHTENED RISK.

(1) IN GENERAL.—Notwithstanding the notice and notification obligations under sections 101 and 106(a), any covered entity shall notify the Federal Breach Notification Recipient if a security breach is reasonably believed to involve—

(A) the access to or acquisition or integrity of:

(i) Controlled Technical Information; technical data designated on the United States Munitions List at 22 C.F.R. section 121.1;

(ii) information constituting items listed on the Commerce Control List at 15 C.F.R. part 774 supplement number 1;

(iii) Unclassified Controlled Nuclear Information under the Atomic Energy Act, section 2168 of title 42, United States Code, and 10 C.F.R. Part 1017;

(iv) information controlled under 10 C.F.R. Part 810;

(v) restricted or formerly restricted data under the Atomic Energy Act, section 2162 of title 42, United States Code;

(vi) special nuclear materials under section 128 of title 10, United States Code; or

(vii) aviation security information under the Federal Aviation Act, section 40119 of title 49, United States Code;

(B) inaccessibility of data due to a ransomware attack;

(C) unauthorized access to an operational technology network; or

(D) unauthorized access to a software build system, software development system, or any such other such system that develops, manages, or distributes software updates to proprietary hardware or software.

(2) CONTENT OF NOTIFICATION.—Notification required under this subsection shall include:

(A) a description of the security breach, including identification of the affected databases, information systems, or devices that were, or are reasonably believed to have been, accessed by an unauthorized person, and the estimated date range of the security breach;

(B) where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to accomplish the unauthorized access;

(C) where applicable, any identifying information related to the malicious actor;

(D) where applicable, identification of the category or categories of information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person; and

(E) contact information, such as a telephone number or electronic mail address, that the government may use to contact the covered entity or an agent of the covered entity;

(3) REGULATORY USE.—Information disclosed pursuant to subsection (b)(3) that is not otherwise available (including, but not limited to, any information in notices to individuals described in section 104), shall not be used by any Federal, state, local, tribal, or territorial government to sanction or otherwise punish the entity disclosing the information.

(4) PRESERVATION OF PRIVILEGE.—Disclosure of information pursuant to this subsection or by a covered entity to the Federal Breach Notification Recipient, the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, the United States Secret Service, or national security authorities for the purposes of furthering the prevention, detection, investigation, or prosecution of a security breach of their systems shall not waive any otherwise applicable privilege, immunity, or protection provided by law.

(5) EXEMPTION FROM DISCLOSURE.—Information disclosed pursuant to this subsection or by a covered entity for the purposes of furthering the prevention, detection, investigation, or prosecution of a security breach of their systems, shall be withheld, without discretion, from the public under section 552(b)(3)(B) of title 5, United States Code.

(6) EXCEPTION.—This subsection shall not apply if the covered entity discovered and confirmed the security breach through notification from the federal government. Federal government entities providing notification to covered entities of security breaches shall at the same time provide notification to the Federal Breach Notification Recipient.

(c) FEDERAL BREACH NOTIFICATION RECIPIENT.

(1) The Federal Breach Notification Recipient shall be an entity or mechanism within the Department of Justice or Department of Homeland Security and shall be designated by the National Cyber Director. The Attorney General and Secretary of Homeland Security, in consultation with the National Cyber Director, shall jointly develop and issue operating procedures for the Federal Breach Notification Recipient and, beginning with the date of inception of the Federal Breach Notification Recipient, biannually review such procedures and amend them as needed.

(2) Whenever the Federal Breach Notification Recipient receives a notification from a covered entity, service provider, or federal government entity under this title, it shall immediately notify and provide all information contained in the notification to the Federal Bureau of Investigation, the United States Secret Service, the Cybersecurity and Infrastructure Security Agency, and the National Cyber Director. The Federal Breach Notification Recipient shall also make such information available as appropriate to other Federal agencies for law enforcement, national security, or cyber security purposes.

(c) TIMING OF NOTIFICATION BY THE COVERED ENTITY.—

(1) IN GENERAL.—The notifications by the covered entity to the federal government required under this section shall be provided as promptly as possible, but must occur at least
72 hours before notice to an individual pursuant to subsection 101(d), or 10 days after discovery and confirmation of the security breach requiring notice, whichever comes first.

(d) EXTENSION FOR NOTICE TO INDIVIDUALS.—If a covered entity notifies federal law enforcement within 72 hours of discovery and confirmation of a security breach, notice to individuals under section 101 shall be made within 40 days of discovery and confirmation of the security breach, unless such notice to individuals is delayed pursuant to subsection 101(e).

(e) PRESERVATION OF EXISTING OBLIGATIONS.—Nothing in this title shall modify, prevent, or abrogate any notice or notification obligations under government contracts, enforceable agreements with the government, or other Federal law.

SEC. 107. ENFORCEMENT.

(a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—Compliance with the requirements imposed under this title shall be enforced under the Federal Trade Commission Act (sections 41 et seq. of title 15, United States Code) by the Commission with respect to covered entities subject to this title. For the purpose of the exercise by the 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 promulgated under section 18(a)(1)(B) of the Federal Trade Commission Act (section 57a(a)(1)(B) of title 15, United States Code) regarding unfair or deceptive acts or practices and shall be subject to enforcement by the Commission under that Act with respect to any covered entity.

(b) ENFORCEMENT.—All of the functions and powers of the 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. Notwithstanding sections 4, 5(a)(2), or 6 of the Federal Trade Commission Act (sections 44, 45(a)(2), or 46 of title 15, United States Code) or any jurisdictional limitation of the Commission, the Commission shall also enforce this title, in the same manner provided in this section, with respect to—

(1) organizations not organized to carry on business for their own profit or that of their members; and

(2) common carriers subject to the Communications Act of 1934 (section 151 of title 47, United States Code) and Acts amendatory thereof and supplementary thereto.

(c) COMMON CARRIERS.—Where enforcement relates to common carriers subject to the Communications Act of 1934 (sections 151 et seq. of title 47, United States Code) and Acts amendatory thereof and supplementary thereto, the Commission will coordinate with the Federal Communications Commission.

(d) FINANCIAL SERVICES.—Where enforcement relates to information associated with the provision of financial products or services by an entity that provides a consumer financial product or service as defined in section 1002 of the Consumer Financial Protection Act of 2010 (section 5481 of title 12, United States Code)), the Commission will notify the Consumer Financial Protection Bureau.

(e) NOTIFICATION.—Where enforcement relates to matters implicating the

jurisdiction or authorities of another Federal agency, the Commission will notify that agency as appropriate.

(f) DECONFLICTION.—The Commission and Attorney General shall jointly develop procedures to de-conflict investigations deriving from obligations under this title.

(g) CONSTRUCTION.—Nothing in this title shall be construed to limit the authority of the Federal Trade Commission under any other provision of law.

SEC. 108. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) IN GENERAL.—

(1) CIVIL ACTIONS.—In any case in which either 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 an interest of the residents of that State has been or is threatened or adversely affected by the engagement of a covered entity in a practice that is prohibited under this title or the failure to meet a requirement imposed under this title, the attorney general of the State, or the authorized State or local law enforcement agency on behalf of the residents of the agency's jurisdiction, may bring a civil action on behalf of the residents of the State or jurisdiction in a district court of the United States of appropriate jurisdiction or any other court of competent jurisdiction, including a State court, to—

(A) enjoin that practice;

(B) enforce compliance with this title; or

(C) impose civil penalties of not more than $1,000 per day per individual whose sensitive personal information was, or is reasonably believed to have been,
accessed or acquired without authorization, up to a maximum of $1,000,000 per violation unless such conduct is found to be willful or intentional.

(2) NOTICE.—At least 30 days before filing an action under paragraph (1), the attorney general of the State, or the State or local law enforcement agency, shall provide to the Attorney General and the Commission—

(A) written notice of the action; and

(B) the complaint for the action.

(3) LIMITATION.—Civil actions described in subsection (a) shall not be filed if the Attorney General certifies that the filing would impede a criminal investigation or national security activity.

(b) FEDERAL PROCEEDINGS.—Upon receiving notice under paragraph (a)(2), the Commission shall have the right to—

(1) move to intervene and 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 107 and move to consolidate all pending actions, including State actions, in such court;

(3) intervene in an action brought under paragraph (a)(2); or

(4) file petitions for appeal.

(c) PENDING PROCEEDINGS.—If the Commission has instituted a proceeding or action for a violation of this title or any regulations promulgated thereunder, no attorney general of a State or State or local law enforcement agency may, during the pendency of such proceeding or action, bring an action under this title against any defendant named in such civil action for any violation that is alleged in that proceeding or action.

(d) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this title regarding notice or notification shall be construed to prevent an attorney general of a State or a State or local law enforcement agency 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.

SEC. 109. EFFECT ON STATE LAW.

The provisions of this title shall supersede any provision of the law of any State, or a political subdivision thereof, to the extent such provision relates to notice to individuals by a covered entity of a security breach of digital data, except as provided in section 103(c).

SEC. 110. CONGRESSIONAL REPORTING

The Chairman of the Federal Trade Commission, in consultation with the Attorney General and Secretary of Homeland Security, shall report to Congress not later than 18 months after the date of enactment of this title, and upon the request by Congress thereafter, on the implementation of this title.

SEC. 111. EXCLUSIONS.

Nothing in this title shall apply to—

(a) covered entities to the extent that they act as covered entities and business associates subject to the Health Information Technology for Economic and Clinical Health Act (section 17932 of title 42,
United States Code), including the data breach notification requirements and implementing regulations of that Act;

(b) covered entities to the extent that they act as vendors of personal health records and third party service providers subject to the Health Information Technology for Economic and Clinical Health Act (section 17937 of title 42, United States Code), including the data breach notification requirements and implementing regulations of that Act;

(c) National Security Systems, as defined in section 3552 of title 44 of the United States Code, provided that in the event of a security breach of a National Security System operated by a covered entity on behalf of a United States Government agency or department, the covered entity shall notify the relevant agency or department as promptly as possible, and within no more than 15 days, and provide all relevant information. The content of such notification shall be consistent with Sec. 105(b)(2) of this Act. An agency or department receiving such a

notification from a covered entity shall comply with applicable reporting and notification requirements which may include policies, procedures, guidelines, instructions and standards levied in accordance with other applicable law, Executive order, and Presidential policy; and

(d) Intelligence Community "information technology," as defined in section 11101 of title 40 of the United States Code, provided that in the event of a security breach of Intelligence Community "information technology" operated by a covered entity on behalf of a United States Government agency or department, the covered entity shall notify the relevant agency or department as promptly as possible and within no more than 15 days, and provide all relevant information. The content of such notification shall be consistent with Sec. 105(b)(2) of this Act. An agency or department receiving such a notification from a covered entity shall comply with applicable reporting and notification requirements which may include policies, procedures, guidelines, instructions and standards levied in accordance with other applicable law, Executive order, and Presidential policy. . The definition of the term "Intelligence Community" is the same as set forth in section 3003 of title 50 of the United States Code.

SEC. 112. EFFECTIVE DATE.

This title shall take effect 90 days after the date of enactment.

SEC. 113. DEFINITIONS.

In this title, the following definitions shall apply:

(a) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(b) COVERED ENTITY.—The term "covered entity" means any non-governmental organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture, whether or not established to make a profit, other than a service provider as defined in this section, engaged in or affecting interstate commerce, that accesses, acquires, maintains, disposes of, uses, stores, sells, or communicates sensitive personal information in or through one or more electronic systems, networks, or services.

(c) SECURITY BREACH.—

> (1) IN GENERAL.—The term "security breach" means a compromise of the confidentiality, integrity, or availability of, or the loss of, digital data without or in excess of authorization.
>
> (2) EXCLUSION.—The term "security breach" does not include any lawfully authorized investigative, protective, or intelligence activity of, or voluntary disclosure to, an agency of the United States, a State, or a political subdivision of a State.

(d) SENSITIVE PERSONAL INFORMATION.—

(1) The term "sensitive personal information" means information or compilation of information, in electronic or digital form that includes one or more of the following—

(A) an individual's first and last name (or first initial and last name), address, or telephone number, in combination with a driver's license number or equivalent State identification number, passport number, military identification number, or
other unique identification number issued on a government document that is used to verify the identity of a specific individual;

(B) a financial account number, including bank account number, credit card
number, or debit card number, in combination with any security code, access code, password, expiration date, or other personal identification information necessary to access the financial account or conduct a transaction that will
credit or debit the financial account;

(C) any unique biometric data, such as a fingerprint, voice print, facial print, retina or iris image, genomic data, or other unique physical representation or digital representation of biometric data if such biometric data may be used to digitally verify the identity of a specific individual.

(E) the last four digits of a Social Security number in combination with an individual's first and last name (or first initial and last name);

(G) a username, electronic mail address, first and last name of an individual, or other account identifier, in combination with a password, access code, or
security question and answer that would permit access to an account.

(H) any combination of the following data elements:

(i) an individual's first and last name (or first initial and last name).

(ii) a unique account identifier, including a financial account number or credit or debit card number, electronic identification number, username, or routing code.

(iii) any security code, access code, or password, or source code that could be used to generate such codes or passwords.

(2) EXCLUSIONS.—

(A) PUBLIC RECORD INFORMATION.—sensitive personal information does not include information about an individual which has been:

(i) lawfully made publicly available by, and which the covered entity obtained from, a Federal, State, or local government entity; or

(ii) widely distributed by media.

(B) ENCRYPTED OR SECURED DATA.—sensitive personal information does not include information that is encrypted or secured by any method or technology generally accepted by experts in the field of information security that renders the data elements unusable, unreadable, or indecipherable by unauthorized persons. This exclusion does not apply if any cryptographic keys necessary to enable decryption of such data are also reasonably believed to have been accessed or acquired without authorization.

(3) MODIFIED DEFINITION BY RULEMAKING.—The Commission may, by rule promulgated under section 553 of title 5, United States Code, amend the definition of "sensitive personal information" to the extent that such amendment will not unreasonably impede interstate commerce and will accomplish the purposes of this Act. In amending the definition, the Commission may determine—

(A) that any particular combination of information are sensitive personal information; or

(B) that any particular piece of information, on its own, is sensitive personal information.

(e) RANSOMWARE ATTACK.—A security breach where an attacker gains unauthorized access to a system or network, encrypts the data it contains, and threatens to expose the

victim's data or perpetually render it inaccessible if a ransom is not paid.

(f) OPERATIONAL TECHNOLOGY. —Software, hardware, or information system that detects or causes change through direct monitoring or control of industrial equipment.

(g) SERVICE PROVIDER.—The term "service provider" means a nongovernmental organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture, whether or not established to make a profit, that provides digital data transmission, routing, storage, or connections to its system or network, where the entity providing such services does not select or modify the content of the digital data and is not the sender or the intended recipient of the data, and the entity transmits, routes, or provides connections for sensitive personal information in a manner that sensitive personal information is undifferentiated from other types of data that such entity transmits, routes, or provides connections. Any such entity shall be treated as a service provider under this title only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage, or connections. Such entities are nevertheless covered entities under this title to the extent they access, acquire, maintain, dispose of, store, sell, or otherwise use digital data for their own purposes. *******