Legislative Language

Data Breach Notification

“ SEC. 1. DEFINITIONS.

“ In this title, the following definitions shall apply:

“ (a) AFFILIATE.—The term “affiliate” means persons related by common ownership or by corporate control.

“ (b) BUSINESS ENTITY.—The term “business entity” means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture, whether or not established to make a profit.

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

“ (d) DATA SYSTEM COMMUNICATION INFORMATION.—The term “data system communication information” means dialing, routing, addressing or signaling information that identifies the origin, direction, destination, processing, transmission, or termination of each communication initiated, attempted, or received.

“ (e) DATE AND TIME.—The term “date and time” includes the date, time, and specification of the time zone offset from Coordinated Universal Time (UTC).

“ (f) INTERNET ADDRESS.—The term “Internet address” means an Internet Protocol address as specified by the Internet Protocol version 4 or 6 protocol, or any successor protocol or any unique number for a specific host on the Internet.

“ (g) SECURITY BREACH.—

> “ (1) IN GENERAL.—The term “security breach” means a compromise of the security, confidentiality, or integrity of, or the loss of, computerized data that results in, or there is a reasonable basis to conclude has resulted in –
>
> > “ (A) the unauthorized acquisition of sensitive personally identifiable information; or
> >
> > “ (B) access to sensitive personally identifiable information that is for an unauthorized purpose, or in excess of authorization.
>
> “ (2) EXCLUSION.—The term “security breach” does not include any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

“ (h) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term “sensitive personally identifiable information” means any information or compilation of information, in electronic or digital form that includes—

“ (1) an individual’s first and last name or first initial and last name in combination with any two of the following data elements:

“ (A) home address or telephone number;“ (B) Mother’s maiden name;

“ (C) month, day, and year of birth;

“ (2) a non-truncated social security number, driver’s license number, passport number, or alien registration number or other government-issued unique identification number;

“ (3) unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation;

“ (4) a unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code; or

“ (5) any combination of the following data elements:

“ (A) an individual’s first and last name or first initial and last name;

“ (B) a unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code; or

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

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

“ (A) that any particular combinations of information are sensitive personally identifiable information, or

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

“ SEC. 101. NOTICE TO INDIVIDUALS.

“ (a) IN GENERAL.—Any business entity engaged in or affecting interstate commerce, that uses, accesses, transmits, stores, disposes of or collects sensitive personally identifiable information about more than 10,000 individuals during any 12-month period shall, following the discovery of a security breach of such information, notify any individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed or acquired, unless there is no reasonable risk of harm or fraud to such individual.

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

> “ (1) NOTICE TO OWNER OR LICENSEE.—Any business entity engaged in or affecting interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information that the business entity does not own or license shall notify the owner or licensee of the information following the discovery of a security breach involving such information, unless there is no reasonable risk of harm or fraud to such owner or licensee.
>
> “ (2) NOTICE BY OWNER, LICENSEE OR OTHER DESIGNATED THIRD PARTY.—Nothing in this title shall prevent or abrogate an agreement between a business entity required to give notice under this section and a designated third party, including an owner or licensee of the sensitive personally identifiable information subject to the security breach, to provide the notifications required under subsection (a).
>
> “ (3) BUSINESS ENTITY RELIEVED FROM GIVING NOTICE.—A business entity obligated to give notice under subsection (a) shall be relieved of such obligation if an owner or licensee of the sensitive personally identifiable information subject to the security breach, or other designated third party, provides such notification.

“ (c) TIMELINESS OF NOTIFICATION.—

> “ (1) IN GENERAL.—All notifications required under this section shall be made without unreasonable delay following the discovery by the business entity of a security breach. A business entity shall, upon the request of the Commission, provide records or other evidence of the notifications required under this section.
>
> “ (2) REASONABLE DELAY.—Reasonable delay under this subsection shall not exceed 60 days, except as provided in section 101(d) or unless the business entity seeking additional time demonstrates to the Commission that additional time is reasonably necessary to determine the scope of the security breach, prevent further disclosures, conduct the risk assessment, restore the reasonable integrity of the data system, and provide notice to an entity designated by the Secretary of Homeland Security to receive reports and information about information security incidents, threats, and vulnerabilities when required. If the Commission determines that additional delay is necessary the agency may extend the time period for notification for additional periods of up to 30 days each. Any such extension shall be provided in writing.

" (3) BURDEN OF PRODUCTION.— If a business entity requires additional time under paragraph (2), it shall provide the Commission with records or other evidence of the reasons necessitating delay of notification.

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

" (1) IN GENERAL.—If a Federal law enforcement 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 such Federal law enforcement agency to the business entity that experienced the breach.

" (2) EXTENDED DELAY OF NOTIFICATION.—If the notification required under subsection (a) is delayed pursuant to paragraph (1), a business entity shall give notice 30 days after the day such delay was invoked unless a Federal law enforcement agency provides written notification that further delay is necessary. Written notifications for further delay shall specify the period of delay to which they apply.

" (3) IMMUNITY.—No non-constitutional cause of action shall lie in any court against any federal agency for acts relating to the delay of notification for law enforcement or national security purposes under this section.

" SEC. 102. EXEMPTIONS FROM NOTICE TO INDIVIDUALS.

" (a) EXEMPTION FOR NATIONAL SECURITY AND LAW ENFORCEMENT.—

" (1) IN GENERAL.— If the United States Secret Service or Federal Bureau of Investigation determines that notification of the security breach could be expected to reveal sensitive sources and methods or similarly impede the ability of the agency to conduct law enforcement investigations, or if the Federal Bureau of Investigation determines that notification of the security breach could be expected to cause damage to the national security, notification under section 101 is not required.

" (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.—

" (1) IN GENERAL.— A business entity will be exempt from the notice requirements under section 101, if—

" (A) a risk assessment conducted by or on behalf of the business entity concludes that there is no reasonable risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach. If the data at issue was rendered

unusable, unreadable, or indecipherable through a security technology or methodology generally accepted by experts in the field of information security, there shall be a presumption that no reasonable risk exists. Any such presumption shall be rebuttable by facts demonstrating that the security technologies or methodologies in a specific case have been, or are reasonably likely to have been, compromised; and

" (B) without unreasonable delay, but not later than 45 days after the discovery of a security breach, unless extended by the Commission, the business entity notifies the Commission, in writing, of—

" (i) the results of the risk assessment; and

" (ii) its decision to invoke the risk assessment exemption.

" (2) RISK ASSESSMENTS.—

" (A) failure to conduct the risk assessment in a reasonable manner or according to standards generally accepted by experts in the field of information security shall constitute a violation of this section.

" (B) a risk assessment must include logging data, as applicable and to the extent available, for a period of at least six months prior to submitting the risk assessment—

" (1) for each communication or attempted communication with a database or data system containing sensitive personally identifiable information, the data system communication information for the communication or attempted communication, including any Internet addresses, and the date and time associated with the communication or attempted communication; and

" (2) all log-in information associated with databases or data systems containing sensitive personally identifiable information, including both administrator and user log-in information.

" (C) submitting a risk assessment containing fraudulent or deliberately misleading information shall constitute a violation of this section.

" (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

" (1) IN GENERAL.—A business entity will be exempt from the notice requirement under section 101 if the business entity utilizes or participates in a security program that—

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

" (B) provides for notice 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 security breach includes the individual's first and last name or any other type of sensitive personally identifiable information other than a credit card number or credit card security code.

" SEC. 103. METHODS OF NOTICE TO INDIVIDUALS.

" A business entity shall be in compliance with section 101 if it provides both—

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

" (A) written notification to the last known home mailing address of the individual in the records of the business entity;

" (B) telephone notice to the individual personally; or

" (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).

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

" 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, to the extent possible—

" (1) 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;

" (2) a toll-free number—

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

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

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

" (b) DIRECT BUSINESS RELATIONSHIP. —Regardless of whether the business entity or a designated third party provides notice pursuant to section 101(b) of this Act, such notice shall identify the business entity that has a direct business relationship with the individual.

" (c) ADDITIONAL CONTENT.—Notwithstanding section 109, a State may require that a notice under subsection (a) shall also include information regarding victim protection assistance provided for by that State.

" SEC. 105. COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.

" (a) Where a business entity is required to provide notification to more than 5,000 individuals under section 101, the business 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 (section 1681a(p) of title 15, United States Code) 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.

" (b) Reasonable delay under subsection (a) shall not exceed 60 days, except as provided in section 101(d) and 102(a) or unless the business entity providing notice can demonstrate to the Commission that additional time is reasonably necessary to determine the scope of the security breach, prevent further disclosures, conduct the risk assessment, restore the reasonable integrity of the data system, and provide notice to an entity designated by the Secretary of Homeland Security to receive reports and information about information security incidents, threats, and vulnerabilities when required. If the Commission determines that additional delay is necessary, the agency may extend the time period for notification for additional periods of up to 30 days each. Any such extension shall be provided in writing.

" SEC. 106. NOTICE FOR LAW ENFORCEMENT AND OTHER PURPOSES.

" (a) NOTICE TO LAW ENFORCEMENT AND NATIONAL SECURITY AUTHORITIES.— Any business entity shall notify an entity designated by the Secretary of Homeland Security to receive reports and information about information security incidents, threats, and vulnerabilities, and such agency shall promptly notify and provide that same information to the United States Secret Service, the Federal Bureau of Investigation, and the Commission for civil law enforcement purposes, and shall make it available as appropriate to other federal agencies for law enforcement, national security, or computer security purposes, if—

" (1) the number of individuals whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person exceeds 5000;

" (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 business entity to be employees and contractors of the Federal Government involved in national security or law enforcement.

" (b) COMMISSION RULEMAKING. – Not later than one year after the date of the enactment of this Act, in consultation with the Attorney General and the Secretary of Homeland Security, the Commission shall promulgate regulations defining what information notifications under subsection (a) must contain. In addition, in consultation with the Attorney General, the Commission 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.

" (c) TIMING OF NOTICE.—The notice required under this section shall be provided as promptly as possible, but must occur 72 hours before notification of an individual pursuant to section 101 or 10 days after discovery of the events requiring notice, whichever comes first.

" 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 business entities subject to this Act. 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 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 business entity, irrespective of whether that business entity is engaged in commerce or meets any other jurisdictional tests in the Federal Trade Commission Act. 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. Where enforcement relates to customer proprietary network information, enforcement actions by the Commission will be coordinated with the Federal Communications Commission.

" (b) Before opening an investigation, the Commission must consult with the Attorney General. The 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.

" (c) RULEMAKING.—The Commission may, in addition to the specific rulemakings required or authorized by this title, issue such other regulations as it determines to be necessary to carry out this title. All regulations promulgated under this title shall be issued in accordance with section 553 of title 5, United States Code. Where regulations relate to customer proprietary network information, the promulgation of such regulations will be coordinated with the Federal Communications Commission.

" SEC. 108. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

" (a) IN GENERAL.—

" (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 an interest of the residents of that State has been or is threatened or adversely affected by the engagement of a business 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 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 personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $1,000,000 per violation unless such conduct is found to be willful or intentional.

" (2) NOTICE.— 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—

" (i) written notice of the action; and

" (ii) a copy of the complaint for the action. Such actions 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 subsection (a)(2), the 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 107 and move to consolidate all pending actions, including State actions, in such court;

" (3) intervene in an action brought under subsection (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 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 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.

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

“ SEC. 109. EFFECT ON FEDERAL AND STATE LAW.

“ The provisions of this title shall supersede any provision of the law of any State, or a political subdivision thereof, relating to notification by a business entity engaged in interstate commerce of a security breach of computerized data, except as provided in section 104(c).

“ SEC. 110. REPORTING ON SECURITY BREACHES.

“ (a) The United States Secret Service and Federal Bureau of Investigation 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 number and nature of security breaches subject to the national security and law enforcement exemptions under section 102(a).

“ (b) The Commission shall report to Congress not later than 18 months after the date of enactment of this title, and upon the request of Congress thereafter, on the number and nature of the security breaches described in the notices filed by those business entities invoking the risk assessment exemption under section 102(b) and the response of the Commission to such notices.

“ SEC. 111. EXCLUDED BUSINESS ENTITIES.

Nothing in this Act shall apply to—

“ (a) business 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; and

“ (b) business 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.

“ SEC. 112. EFFECTIVE DATE.

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