Section by Section

DATA BREACH NOTIFICATION

Sec. 1. Definitions.

Establishes definitions for key terms under this Title. In pertinent part, section 101 defines:

- A "business entity" as any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture whether or not established to make a profit.
- A "security breach" as 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, (1) the unauthorized acquisition of sensitive personally identifiable information (SPII); or (2) access to SPII that is unauthorized or in excess of authorization.

Notably, lawfully authorized investigative, protective, or intelligence activities of a law enforcement agency of the federal, state, or local government are excluded from the definition of "security breach." The section also defines with particularity "sensitive personally identifiable information" and authorizes the Federal Trade Commission to amend this definition as needed through the rulemaking process.

Sec. 101. Notice to Individuals.

Sets forth customer notification requirements for certain business entities. Following the discovery of a security breach, such entities must notify any individual whose SPII has been, or is reasonably believed to have been, accessed or acquired, unless there is no reasonable risk of harm. Business entities covered by this section are those that use, access, transmit, store, dispose of, or collect SPII about more than 10,000 individuals during any 12-month period. Business entities are required to notify owners and licensees of SPII in the event of a security breach, and owners and licensees in such situations are charged with the responsibility of making required notifications.

Notification must be made without unreasonable delay. A reasonable delay is one of 60 days or less, unless the business entity seeking additional time demonstrates to the Federal Trade Commission that such time is reasonably necessary under a multi-factor standard; in such instances, the Commission may extend the period of reasonable delay in 30-day increments.

If a Federal law enforcement agency determines that the notification required would impede a criminal investigation or national security activity, notification shall be delayed upon written notice from such Federal law enforcement agency to the business entity that experienced the breach. 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.

Sec. 102. Exemptions From Notice To Individuals.

Sets forth exemptions from notice to individuals. If the United States Secret Service or Federal Bureau of Investigation determines that notification could be expected to reveal sensitive sources and methods or similarly impede the ability of the agency to conduct law enforcement investigations, such notification is not required. Similarly, if the FBI determines that notification of the security breach could be expected to cause damage to the national security, such notification is not required.

Section 102 also establishes a "safe harbor" exemption in which a business entity is exempt from notice to individuals if 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 SPII was subject to the security breach. It also establishes a presumption that no reasonable risk exists where data that was rendered unusable, unreadable, or indecipherable through a security technology or methodology generally accepted by experts in the field of information security. In order to invoke this "safe harbor," a business entity must notify the Federal Trade Commission within 45 days of the results of the risk assessment and its invocation of the "safe harbor". The section establishes requirements for risk assessments that may be used to invoke the "safe harbor".

For security breaches involving a limited subset of SPII, another exemption relieves a business entity from the notice requirement. A business entity need not notify if it utilizes or participates in a security program that effectively blocks the use of the SPII to initiate unauthorized financial transactions before they are charged to the account of the individual, and it provides for notice to affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

Sec. 103. Methods of Notice to Individuals.

Sets forth requirements for notice of individuals, permitting notification by mail, telephone, or email (if the individual has consented to receipt by email). It requires media notice in addition to personal notice where the number of affected individuals in any one state exceeds 5,000.

Sec. 104. Content of Notice to Individuals.

Sets forth requirements for the content of notifications, which includes a description of the SPII at risk, several contact toll-free telephone numbers (including one to assist with consumer

inquiries concerning the security breach), and the name of the business entity that has a direct business relationship with the individual.

Sec. 105. Coordination of Notification with Credit Reporting Agencies.

Requires that in breaches involving the SPII of more than 5,000 individuals, a business entity must notify all consumer reporting agencies 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. Reasonable delay shall not exceed 60 days, unless the business entity seeking additional time demonstrates to the Federal Trade Commission that such time is reasonably necessary under a multi-factor standard; in such instances, the Commission may extend the period of reasonable delay in 30-day increments.

Sec. 106. Notice For Law Enforcement and Other Purposes.

Requires business entities to notify the a DHS entity identified by the Secretary of Homeland Security if the security breach involves (1) the SPII of more than 5,000 individuals; (2) a database or other data system containing SPII of more than 500,000 individuals nationwide; (3) databases owned by the Federal Government; or (4) primarily the SPII of individuals known to be employees and contractors of the Federal Government involved in national security or law enforcement. The DHS entity that receives the reports shall then promptly notify and provide that same information to the United States Secret Service, the Federal Bureau of Investigation, and the Federal Trade 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.

This section also requires the Federal Trade Commission to promulgate regulations defining what these specified information notifications must contain. The Commission may also adjust as necessary the thresholds for notice to law enforcement, after consultation with the Attorney General.

The notice required under this section shall be provided as promptly as possible, but must occur 72 hours before notification of an individual or 10 days after discovery of the events requiring notice, whichever comes first.

Sec. 107. Enforcement.

Compliance with the requirements of this shall be enforced under the Federal Trade Commission Act by the Federal Trade Commission with respect to business entities subject to this Title. A violation of any requirement or prohibition imposed under this Title will constitute an unfair or deceptive act or practice in commerce and shall be subject to enforcement by the Commission, irrespective of whether that business entity is engaged in commerce or meets any other

jurisdictional tests in the Federal Trade Commission Act. In enforcing compliance with the requirements imposed by the Title, the Commission can use all its functions and powers. Such investigations shall not be initiated without prior consultation with the Attorney General, and the Commission may issue such other regulations as it determines to be necessary to carry out this Title.

Sec. 108. Enforcement By State Attorneys General.

Permits enforcement by State attorneys general (or their local designees) when they have 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. The State attorney general (or local designee) 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 enjoin that practice, enforce compliance with this Title, or seek civil penalties of not more than $1,000 per day per individual whose sensitive SPII 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.

Before filing an action, written notice must be provided to the Attorney General and the Federal Trade Commission. The Commission may move to stay the action, intervene in the action, initiate its own action, and file petitions for appeal. Institution of an action by the Commission precludes the filing of subsequent parallel actions by State attorneys general. Federal venue for any action by a State attorney general (or local designee) is controlled by the general civil venue statute. Process may be served in such an action wherever the defendant is an inhabitant or is found.

Finally, section 108 makes clear that nothing in this Title establishes a private cause of action against a business entity for violation of any of its provisions.

Sec. 109. Effect On Federal And State Law.

States that the provisions of this Title shall supersede any state or local law relating to notification by a business entity engaged in interstate commerce of a security breach of computerized data, except to the extent that a State requires that notice to an individual shall also include information regarding victim protection assistance provided for by that State.

Sec. 110. Reporting On Security Breaches. – Requires the United States Secret Service, Federal Bureau of Investigation, and Federal Trade Commission to report to Congress not later than 18 months after the date of enactment of this Title on matters related to the Title's implementation within their area of expertise or control.

Sec. 111. Excluded Business Entities.

Exempts business entities from coverage under the Title to the extent that they act (1) as covered entities and business associates, or (2) as vendors of personal health records and third-party service providers, that are subject to the Health Information Technology for Economic and Clinical Health Act, including the data breach notification requirements and implementing regulations of that Act.

Sec. 112. Effective Date.

The effective date of the Title is 90 days after the date of enactment.