Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Tennessee

Tenn. Code § 47-18-2107

(Scroll down to Title 47, Chapter 18, Part 21)

H.B. 2170 (signed into law June 8, 2005, Chapter 473)

Effective July 1, 2005

S.B. 2005 (signed into law March 24, 2016)

Effective July 1, 2016

S.B. 547 (signed into law April 4, 2017)

Effective April 4, 2017

Application. Any person or business that conducts business in TN, or any agency of TN or any of its political subdivisions (collectively, Entity), that owns or licenses computerized data that includes PI.

Security Breach Definition. Acquisition of:

(i) unencrypted computerized data; or

(ii) encrypted computerized data and the encryption key

by an unauthorized person that materially compromises the security, confidentiality, or integrity of PI maintained by the Entity. "Encrypted" means computerized data that is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key and in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2.

- Good-faith acquisition of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of the security of the system to any resident of TN whose PI was, or is reasonably believed to have been, acquired by an unauthorized person. "Unauthorized person" includes an employee of the Entity who is discovered by the Entity to have obtained personal information and intentionally used it for an unlawful purpose.

Notification to Consumer Reporting Agencies. If an Entity is required to notify more than 1,000 persons at one time, the person shall also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices.

Third-Party Data Notification. Any Entity that maintains computerized data that includes PI that the Entity does not own shall notify the owner or licensee of the information of any breach of the security of the data if the

PI was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than 45 days from the discovery or notification of the breach, unless a longer period of time is required due to the legitimate needs of law enforcement.

Timing of Notification. The disclosure shall be made immediately, but no later than 45 days from the discovery or notification of the breach, unless a longer period of time is required due to the legitimate needs of law enforcement.

Personal Information Definition. An individual's first name or first initial and last name, in combination with any one or more of the following data elements:

- Social Security number;
- Driver's license number; or
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

PI does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted or otherwise made unusable.

Notice Required. Notice may be provided by one of the following methods:

- Written notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act).

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

- Email notice when the Entity has email addresses for the subject persons;
- Conspicuous posting of the notice on the Entity's website if the Entity maintains one; and
- Notification to major statewide media.

Exception: Own Notification Policy. An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and is otherwise consistent with the timing requirements of the statute shall be deemed to be in compliance with the notification requirements of the statute if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Exception: Compliance with Other Laws. The provisions of this statute shall not apply to any Entity that is subject to:

- The provisions of Title V of the Gramm-Leach-Bliley Act; and/or
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. § 1320d), as expanded by the Health Information Technology for Clinical and Economic Health Act;

Other Key Provisions:

- **Delay for Law Enforcement.** The notification required may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made no later than 45 days after the law enforcement agency determines that it will not compromise the investigation.

- Private Right of Action.