Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Minnesota

Minn. Stat. § 325E.61 and 325E.64

H.F. 2121 (signed into law June 2, 2005, Chapter 167)

Effective January 1, 2006

Application. Any person or business that conducts business in MN (collectively, Entity), and that owns or licenses data that includes PI.

Security Breach Definition. An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI maintained by the Entity.

- 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. An Entity to which the statute applies shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of MN whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Notification to Consumer Reporting Agencies. If an Entity notifies more than 500 persons at one time, the Entity shall also notify, within 48 hours, all nationwide consumer reporting agencies of the timing, distribution, and content of the notices.

Third-Party Data Notification. Any Entity that maintains 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 immediately following discovery, if the PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.

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, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired:

- Social Security number;
- Driver's license number or state identification card 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 publicly available information that is lawfully made available to the general public from federal, state, or local government records.

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

- Written notice to the most recent available address the Entity has in its records; or
- Electronic notice, if the Entity's primary method of communication with the individual is by electronic means, or 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 Entity has to provide notice to more than 500,000 residents, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

- Email notice, if 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 whose procedures are otherwise consistent with the timing requirements of the statute, shall be deemed to be in compliance with the notification requirements of the statute, if the Entity notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Other Key Provisions:

- **Delay for Law Enforcement.** Notice may be delayed to a date certain if a law enforcement agency determines that the notice will impede a criminal investigation.
- Attorney General Enforcement.
- Private Right of Action.
- Waiver Not Permitted.
- Does not apply to any "financial institution," as defined by 15 U.S.C. § 6809(3).