Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Nevada

Nev. Rev. Stat. § **603A.010** ***et seq.*****, 242.183**

S.B. 347 (signed into law June 17, 2005, Chapter 485)

Effective October 1, 2005 and January 1, 2006:

S.B. No. 186 (signed into law June 15, 2011)

Effective October 1, 2011

A.B. 179 (Signed into law May 13, 2015)

Effective July 1, 2015

Application. Any governmental agency, institution of higher education, corporation, financial institution or retail operator, or any other type of business entity or association (collectively, Entity), that owns or licenses computerized data that includes PI.

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

- Good-faith acquisition of PI by an employee or agent of the Entity for the legitimate purposes of the Entity is not a breach of the security of the system if the PI is not otherwise 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 data to any resident of NV whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Notification to Consumer Reporting Agencies. If an Entity determines that notification is required to be given to more than 1,000 persons at any one time, the Entity shall also notify, without unreasonable delay, all nationwide consumer reporting agencies of the timing and content of the notice.

Third-Party Data Notification. If an Entity maintains computerized data that includes PI that the Entity does not own, the Entity must notify the owner or licensee of that PI of any breach of the security of the system 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 shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data.

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 name and data elements are not encrypted:

- Social Security number;

- Driver's license number, driver authorization card number or identification card number;
- 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;
- A medical identification number or a health insurance identification number; or
- A username, unique identifier, or email address in combination with a password, access code, or security question and answer that would permit access to an online account.

PI does not include the last four digits of a Social Security number, the last four digits of a driver's license or driver authorization card number, or the last four digits of an identification card number or publicly available information that is lawfully made available to the general public from federal, state, or local governmental records.

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, 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 policies and procedures as part of an information security policy for the treatment of PI that is otherwise consistent with the timing requirements of the statute shall be deemed in compliance with the notification requirements of the statute if it notifies subject persons in accordance with its policies and procedures in the event of a security breach.

Exception: Compliance with Other Laws.

- **Gramm-Leach-Bliley Act.** An Entity that is subject to and complies with the privacy and security provisions of the Gramm-Leach-Bliley Act shall be deemed to be in compliance with the notification requirements.

Other Key Provisions:

- **Delay for Law Enforcement.** The notification required by the statute may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification must be made after the law enforcement agency determines that the notification will not compromise the investigation.
- **Attorney General Enforcement.** If the state Attorney General or a district attorney of any county has reason to believe that any person is violating, proposes to violate, or has violated the provisions of the statute, he or she may bring an action against that person to obtain a temporary or permanent injunction against the violation.
- **Right of Action for Data Collector.** A data collector that provides the requisite notice may commence an action for damages against a person that unlawfully obtained or benefited from PI obtained from records maintained by the data collector.

- **Special Notification Obligations for Government Agencies and Elected Officers.** *See* Rev. Stat. § 242.181.
- **Special Rules Applicable to Electronic Health Records.** *See* Rev. Stat. §§ 439, 603A.100.
- Waiver Not Permitted.