Publications
June 01, 2014

SECURITY BREACH NOTIFICATION CHART - Arkansas

Ark. Code § 4-110-101 ***et seq.***

(Go to the Arkansas Code Search page, Title 4, Subtitle 7, Chapter 110)

S.B. 1167 (signed into law March 31, 2005, Act 1526)

Effective August 12, 2005

H.B. 1943 (signed into law on April 15, 2019, Act 1030)

Effective July 23, 2019

Application. Any person, business or state agency (collectively, Entity) that acquires, owns, or licenses computerized data that includes PI.

Security Breach Definition. An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI maintained by an 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 to any resident of AR whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person.

- Notification is not required if after a reasonable investigation the Entity determines there is no reasonable likelihood of harm to consumers.

Third-Party Data Notification. If an Entity maintains computerized data that includes PI that the Entity does not own, that Entity shall notify the owner or licensee of the information of any breach of the security of the system 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 and manner possible and without unreasonable delay, subject to any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

Personal Information Definition. An individual's first name, or first initial and his or her last name, in combination with any one or more of the following data elements when either the name or the data element is not encrypted or redacted:

- Social Security number;

- Driver's license number or state 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; or
- Medical information (any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional).
- Biometric data (data generated by automatic measurements of an individual's biological characteristics) and any other unique biological characteristics of an individual if used to uniquely authenticate the individual's identity for access to a system of account.

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

- Written notice; or
- Email 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 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 website of the Entity, if the Entity maintains one; and
- Notification to statewide media.

Attorney General Notification. If the affected class of persons to be notified exceeds 1,000, the Entity must disclose the breach to the Attorney General. Notice must be provided at the same time the Entity notifies the affected class, or 45 days after it determines there is a reasonable likelihood of harm to individuals, whichever is first. **Exception: Own Notification Policy.** Any 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 the Entity notifies affected persons in accordance with its policies in the event of a security breach.

Other Key Provisions:

- **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by the statute must be made after the law enforcement agency determines that notification will no longer impede the investigation.
- Attorney General Enforcement.
- **Records Retention.** An Entity must retain a copy of the determination of the breach and any supporting documentation for five years from the date the breach was determined.