Publications
June 01, 2014

# SECURITY BREACH NOTIFICATION CHART - Oklahoma

**24 Okla. Stat. § 161 *et seq.*, § 74-3113.1**

H.B. 2245 (signed into law April 28, 2008)

Effective November 1, 2008

---

**Application.** Any corporations, or any other legal or government entity, whether for profit or not-for-profit (collectively, Entity) that owns or licenses computerized data that includes PI of OK residents.

**Security Breach Definition.** Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of PI maintained by an Entity as part of a database of PI regarding multiple individuals and that causes, or the Entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of OK.

- Good-faith acquisition of PI by an employee or agent of an Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used for a purpose other than a lawful purpose of the Entity 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 OK whose unencrypted and unredacted PI was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of OK.

- An Entity must disclose the breach if encrypted information is accessed and acquired in an unencrypted form or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of OK.

**Third-Party Data Notification.** An Entity that maintains computerized data that includes PI that the Entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the PI was or if the Entity reasonably believes was accessed and acquired by an unauthorized person.

**Timing of Notification.** Without unreasonable delay consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system.

**Personal Information Definition.** The first name or first initial and last name of an individual in combination with and linked to any one or more of the following data elements that relate to a resident of OK, when the data elements are neither encrypted nor redacted:

- Social Security number;
- Driver's license or state identification card number issued in lieu of a driver license; 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 financial accounts.

PI shall not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

**Notice Required.** Notice means one of the following methods:

- Written notice to the postal address in the records of the Entity;
- Telephonic notice; or
- Electronic notice.

**Substitute Notice Available.** If an Entity demonstrates that the cost of providing notice would exceed $50,000, the affected class of residents to be notified exceeds 100,000, or the Entity does not have sufficient contact information or consent to provide notice. Substitute notice consists of any two of the following:

- Email notice, if the Entity has email addresses for the members of the affected class of residents;
- Conspicuous posting of the notice on the Entity's website if the Entity maintains one; or
- Notification to major statewide media.

**Exception: Own Notification Policy.** An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of PI and that are 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 residents of OK in accordance with its procedures in the event of a breach of security of the system.

**Exception: Compliance with Other Laws.**

- **Interagency Guidance.** A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with the provisions of the statute.
- **Primary Regulator.** An Entity that complies with the notification requirements or procedures pursuant to the rules, regulation, procedures, or guidelines established by the primary or functional federal regulator of the Entity shall be deemed to be in compliance with the provisions of the statute.

**Penalties.** The state Attorney General or a district attorney shall have exclusive authority to bring an action and may obtain either actual damages for a violation of the statute or a civil penalty not to exceed $150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

**Other Key Provisions:**

- **Delay for Law Enforcement.** Notice required may be delayed if a law enforcement agency determines and advises the Entity that the notice will impede a criminal or civil investigation or homeland or national security. Notice required must be made without unreasonable delay after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security.