Publications
June 01, 2014

SECURITY BREACH NOTIFICATION CHART - Kansas

Kan. Stat. § 50-7a01 ***et seq.***

S.B. 196 (signed into law April 19, 2006)

Effective January 1, 2007

Application. Any individual, legal or government entity (collectively, Entity) that conducts business in KS and that owns or licenses computerized data that includes PI.

Security Breach Definition. Any unauthorized access to and acquisition of unencrypted or un-redacted computerized data that compromises the security, confidentiality, or integrity of PI maintained by an Entity and that causes, or such Entity reasonably believes has caused or will cause, identity theft to any consumer.

- 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 or is not subject to further unauthorized disclosure.

Notification Obligation. An Entity to which the statute applies shall, when it becomes aware of any breach of the security of the system, give notice as soon as possible to the affected KS resident.

- Notification is not required if after a good-faith, reasonable, and prompt investigation the Entity determines that the PI has not been and will not be misused.

Notification to Consumer Reporting Agencies. In the event that an Entity must notify more than 1,000 consumers at one time, the Entity shall also notify, without unreasonable delay, all nationwide consumer reporting agencies of the timing, distribution, and content of the notices.

Third-Party Data Notification. An Entity that maintains computerized data that includes PI that the Entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the data following discovery of a breach, if the PI was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.

Timing of Notification. Notice 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 and to restore the reasonable integrity of the computerized data system.

Personal Information Definition. A consumer's first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, when the data elements are neither encrypted nor redacted:

- Social Security number;
- Driver's license number or state identification card number; or

- Account number, credit card number, or debit card number, alone or in combination with any required security code, access code, or password that would permit access to a consumer'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; 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 required to provide notice demonstrates that the cost of providing notice will exceed $100,000, or that the affected class of consumers to be notified exceeds 5,000, or that the Entity does not have sufficient contact information to provide notice. Substitute notice shall consist of all of the following:

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

Exceptions:

- **Primary Regulator.** Notification pursuant to laws, rules, regulations, guidance, or guidelines established by an Entity's primary or functional state or federal regulator is sufficient.
- **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, is deemed to be in compliance with the notice requirements of the statute if the Entity notifies affected consumers in accordance with its policies

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 shall be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.
- **Attorney General Enforcement.** Allows the state Attorney General (or Insurance Commissioner in the case of an insurance company) to bring actions at law or equity to enforce compliance and enjoin future violations.