Publications
June 01, 2014

SECURITY BREACH NOTIFICATION CHART - Kentucky

KY Rev. Stat. §365.732

H.B. 232 (signed into law April 10, 2014)

Effective July 15, 2014

H.B. 5 (signed into law April 10, 2014)

Effective January 1, 2015KY Rev. Stat. §61.931 *et seq*.

Effective January 1, 2015

Application. "Information Holder" is defined as any person or business entity that conducts business in Kentucky (collectively, Entity).

- Obligations for state agencies *and private parties that receive, collect or maintain* data from state agencies are different and more detailed than those described below. *See* KY Rev. Stat. §61.931 et seq.

Security Breach Definition. The unauthorized acquisition of unencrypted, unredacted computerized data that compromises the security, confidentiality, or integrity of PI maintained by the Entity as part of a database regarding multiple individuals that actually causes or leads the Entity to believe has caused or will cause, identity theft or fraud against any KY resident.

- 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 if the PI is not used or subject to further unauthorized disclosures.

Notification Obligation. An Entity to which the statute applies must, upon discovery or notification of breach in the security system, notify any KY resident whose unencrypted information was or is reasonably believed to have been acquired by an unauthorized person.

Notification to Consumer Reporting Agencies. If an Entity is required by this section to notify more than 1,000 persons, 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 shall notify the owner or licensee of the information of any breach of the security of the data as soon as reasonably practicable following discovery, if the PI was or is reasonably believed to have been acquired by an unauthorized person.

- Special note that under the state agency provisions in 61.932-.933, a private company contracting with a state agency must notify its contracting agency or institution in the most expedient time possible and without unreasonable delay, within 72 hours of determining that a breach occurred. The contracting agency or institution bears the responsibility of notifying any affected individuals and the state attorney

general.

Timing of Notification.

- Notice should occur in the most expedient time possible and without unreasonable delay, subject to the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach 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 one or more of the following data elements when the name or data element is not redacted:

- Social Security number;
- Driver's license 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.

Obligations under these statutes apply only to unencrypted, unredacted computerized data.

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

- Written notice; or
- Electronic notice, if the notice is provided 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 can demonstrate that the cost of providing notice would exceed $250,000, that the number of individuals to be notified exceeds 500,000, or that they do not have sufficient contact information for those affected. Substitute notice shall consist of all of the following:

- Email notification if the Entity has email addresses for the affected individuals;
- Conspicuous posting regarding the incident on the Entity's website, if the Entity maintains a website; 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 is otherwise consistent with the timing requirements of this section, shall be deemed to be in compliance with the notification requirements of this section, if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Exception: Compliance with Other Laws.

- **Federal Laws.** The provisions of this statute do not apply to any Entity subject to the provisions of Title V of the Gramm-Leach-Bliley Act, the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- **State Agencie** This statute does not apply to any KY agency, or any KY local governments or political subdivisions. (*But see* KY Rev. Stat. §61.931 *et seq*.)

Other Key Provisions:

- **Delay for Law Enforcement.** An Entity's notice may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.