Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Texas

Tex. Bus. & Com. Code §§ 521.002, 521.053

Acts 2007, 80th Leg., ch. 885, § 2.01. Amended by Acts 2009, 81st Leg., ch. 419, § 3.

Effective April 1, 2009

Acts 2011, 82nd Leg., ch. 1126, § 14 (H.B. No. 300).

Effective Sept. 1, 2012

S.B. 1610 (signed into law June 14, 2013)

Effective June 14, 2013

H.B. 4390 (signed into law June 14, 2019)

Effective January 1, 2020

H.B. 3529 (signed into law May 26, 2021)

Effective September 1, 2021

H.B. 3746 (signed into law June 14, 2021)

Effective September 1, 2021

S.B. 768 (signed into law May 27, 2023)

Effective September 1, 2023

Application. A person (Entity) that conducts business in TX and owns or licenses computerized data that includes sensitive PI.

Security Breach Definition. Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive PI maintained by an Entity, including data that is encrypted if the person accessing the data has the key required to decrypt the data.

- Good-faith acquisition of sensitive PI by an employee or agent of the Entity for the purposes of the Entity is not a breach of system security unless the sensitive PI is used or disclosed by the person in an unauthorized manner.

Notification Obligation. An Entity to which the statute applies shall disclose any breach of system security to any person, including nonresidents, whose sensitive PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Attorney General Notification. Any Entity that is required to provide notification of a security breach to at least 250 Texas residents, shall notify the attorney general of that breach as soon as practicable and not later than

30 days after the Entity determines that a breach has occurred. The notification must include:

- A detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach;
- The number of Texas residents affected by the breach at the time of notification;
- The number of affected residents that have been sent a disclosure of the breach by mail or other direct method of communication at the time of notification;
- The measures taken by the Entity regarding the breach;
- Any measures the Entity intends to take regarding the breach after notification; and
- Information regarding whether law enforcement is investigating the breach.

Businesses must submit a detailed description of the breach in addition to other required information using an electronic form accessed through the attorney general's website.

Notification to Consumer Reporting Agencies. If an Entity is required by this section to notify at one time more than 10,000 persons of a breach of system security, 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. Any Entity that maintains computerized data that includes sensitive PI that the Entity does not own shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. Notice to individuals shall be made as soon as practicable and in each case not later than the 60th day after the date on which the person determines that the breach occurred, consistent with the legitimate needs of law enforcement, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

- Notification to the Attorney General must be made in 30 days.

Sensitive Personal Information Definition. An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

- Social Security number;
- Driver's license number or government-issued ID 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.

Sensitive PI also includes information that identifies an individual and relates to:

- The physical or mental health or condition of the individual;
- The provision of health care to the individual; or
- Payment for the provision of health care to the individual.

Sensitive PI does not include publicly available information that is lawfully made available to the general public from the federal government or a state or local government.

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

- Written notice at the last known address of the individual; or

- Electronic notice, if the notice is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act).

However, if the affected person is a resident of a state that has its own breach notification requirement, the Entity may provide notice under that state's law or under Texas's law.

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the Entity does not have sufficient contact information, the notice may be given by any of the following:

- Email notice when the Entity has email addresses for the affected persons;
- Conspicuous posting of the notice on the Entity's website; or
- Notice published in or broadcast on 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 sensitive PI that complies with the timing requirements for notice under this section complies with this section if the Entity notifies affected persons in accordance with that policy.

Other Key Provisions:

- **Delay for Law Enforcement.** An Entity may delay providing notice as required at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The required notification shall be made as soon as the law enforcement agency determines that the required notice will not compromise the investigation.
- **Attorney General Website.** The attorney general will post on its publicly accessible website a listing of the notifications it receives under the statute of any system security breach. Such notices will be posted no later than thirty days after the attorney general receives the notification. The listing of the notice will be removed no later than the first anniversary of its posting if the person who provided the notification has not notified the attorney general of any additional breaches during that period.
- **Attorney General Enforcement.** Remedies include injunctive relief and civil penalties of at least $2,000 but not more than $50,000 for each violation.
- Civil penalties for failure to comply with notification requirements are raised to up to $100 per person to whom notification is due, per day, not to exceed $250,000 per breach.