

Texas' Amended Data Breach Notification Law Is Expansive

Texas amended its existing data breach notification law which became effective on September 1, 2012. The relevant section of the law is titled "Notification Required Following Breach of Security of Computerized Data" and is found at [Section 521.053 of the Texas Business and Commerce Code](#). This is one of the most expansive state breach notification laws in the country as it applies to not only Texas citizens, but to citizens of other states that do not have a breach notification law.

The main body of the law provides as follows:

(b) A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made as quickly as possible, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

What is a "breach of system security"?

The law defines "breach of system security" as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data."

What is "sensitive personal information"?

The law has a fairly detailed definition of "sensitive personal information" that should be read carefully. A couple of general points will provide an overview of what is and is not protected:

- Information that is lawfully made available to the public from a federal, state, or local governmental body is not considered sensitive personal information
- Sensitive personal information does include "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 in the items are not encrypted:" Social

Security number, driver's license number or other government issued identification number, account or card numbers in combination with the required access or security codes

- Also included is information that at that identifies an individual and is related to their health condition, provision of healthcare, or payment for healthcare

Who does the law apply to?

The law applies to any person (which includes entities) who conducts business in Texas and owns or licenses computerized data that includes sensitive personal information.

Who must be notified?

The law requires notification to "any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person." This is an incredibly broad class of individuals that is certainly not limited to only Texas citizens and, quite possibly, is not even limited to citizens of the United States.

When must the notification be given?

The notification must be given as quickly as possible after it has been determined that an individual's sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. However, the notification may be delayed as necessary to determine the scope of the breach and restore the reasonable integrity of the data system or at the request of law enforcement to avoid compromising an investigation.

What is the penalty for failure notify?

Section 151.151 of the law provides for a penalty for failing to comply with this notification requirement is a civil penalty of up to \$100.00 per individual per day for the delayed time but is not to exceed \$250,000 for a single breach.

If you have any questions about data breaches, breach notification, privacy or data security, please feel free to contact me to discuss.

Shawn E. Tuma
direct: 469.635.1335
stuma@brittontuma.com