Published on *The National Law Review* https://natlawreview.com

Texas Joins Other States with New Texas Data Breach Notification Requirement: Is This a New Trend?

Article By:

Joseph J. Lazzarotti

Jason C. Gavejian

Rachel E. Ehlers

Maya Atrakchi

The Texas Legislature, which meets every other year, pushed a change to its data breach notification law at the end of the session in late May, and yesterday Governor Greg Abbott signed the bill into law. It follows a growing trend of changes to privacy and cybersecurity laws at the state level.

Texas House Bill 3746 will amend Texas Business and Commerce Code § 521.053, which requires notifications to individuals and the Texas Attorney General following certain data breaches. The amendment adds a requirement for the Texas Attorney General to post on its website a listing of data breach notifications received, when a breach involves 250 or more Texas residents. California has a similar requirement, although it is for breaches affecting 500 or more residents.

Specifically, the Texas amendment would require the Texas Attorney General to:

- Post on the Attorney General's public website a listing of notifications received, excluding any sensitive personal information, any information that may compromise a data system's security, and any other information reported to the Attorney General that is made confidential by law;
- Maintain an updated listing on the website, and update the list no later than every 30 days; and
- Remove data no later than one year following the date it was added, unless the entity notified the Attorney General of additional incidents.

The amendment also now requires that entities reporting a breach to the Texas Attorney General provide the number of Texas residents receiving notification of the breach, in addition to the current

requirements of:

- 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 residents affected by the breach;
- The measures taken by the person regarding the breach and any measures the person intends to take regarding the breach after notification; and
- Information regarding whether law enforcement is engaged in investigating the breach.

The Texas amendment may indicate a growing trend towards increased information sharing in an effort to prevent future data breaches. On the federal level, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has implemented several programs in the past year to promote information sharing and awareness. "Information sharing is essential to the protection of critical infrastructure and to furthering cybersecurity for the nation. As the lead federal department for the protection of critical infrastructure and the furthering of cybersecurity, the CISA has developed and implemented numerous information-sharing programs. Through these programs, CISA develops partnerships and shares substantive information with the private sector, which owns and operates the majority of the nation's critical infrastructure. CISA also shares information with state, local, tribal, and territorial governments and with international partners, as cybersecurity threat actors are not constrained by geographic boundaries", CISA states. More information on CISA information sharing and awareness programs is available here.

The updated Texas law will take effect September 1, 2021. With no shortage of large-scale breaches and heightened public awareness across the nation, organizations regardless of jurisdiction are advised to evaluate and enhance their data breach prevention and response capabilities.

National Law Review, Volume XI, Number 166