Tulsa Data Privacy Attorney Aaron Tifft for the Journal Record - What Businesses Need to Know About Oklahoma's New Data Breach Law

August 21, 2025

By: Aaron C. Tifft

The Journal Record

https://journalrecord.com/2025/08/20/gavel-to-gavel-what-businesses-need-to-know-about-oklahomas-new-data-breach-law/

On January 1, 2026, Oklahoma's updated data breach law takes effect. Businesses should prepare now or face higher compliance risks later.

Senate Bill 626 expands Oklahoma's approach to cybersecurity, recognizing that businesses of every size now collect and store sensitive customer information. From retailers to oilfield service companies, no one is exempt from the potential fallout of a breach.

The law expands the scope of protected information by broadening what qualifies as "personal information." Beyond names, Social Security numbers, and financial accounts, the law now covers biometric identifiers (such as fingerprints or retinal scans), government-issued unique identifiers, and additional banking details. If your business collects any of these data points, you fall under the new rules.

Previously, breach notices were limited to affected individuals. Beginning in 2026, businesses must also notify state regulators when an incident impacting more than 500 Oklahoma residents occurs. This new step will likely trigger additional oversight and state scrutiny. Businesses should expect follow-up inquiries, especially in large-scale events or when reporting delays occur.

The Safe Harbor Provision

The new law does provide an upside for businesses. SB 626 creates a safe harbor for companies that utilize "reasonable safeguards." These safeguards are defined as, "conducting risk assessments, implementing technical and physical layered defenses, employee training on handling personal information, and establishing an incident response plan." This can be accomplished by utilizing data encryption, multi-factor authentication, regular training, and conducting risk assessments. Doing so, businesses will limit their susceptibility to attack and liability after a breach. This incentive rewards proactive investment in data security rather than punishment after the fact.

Preparation Checklist

To prepare for the upcoming changes to the law, Oklahoma businesses should:

- **Review data inventories.** Know what specific types of information you collect and where it's stored.
- **Enact technical safeguards.** Ensure your business is encrypting personal information and utilizing multi-factor authentication for access.
- **Update incident response plans.** Ensure you have clear procedures for containing breaches, investigating quickly, and issuing notices to impacted individuals and the state.
- **Train employees.** Many breaches stem from phishing or human error. Ongoing training reduces risk and is a necessary "reasonable safeguard."
- **Engage with vendors.** If you outsource services that utilize personal information you collect, confirm that contracts adequately address breach notification and security standards.
- **Review insurance coverage.** Cyber policies can cover response costs, regulatory investigations, and litigation.

SB 626 raises the bar for data protection in Oklahoma. The cost of ignoring compliance is no longer just reputational damage, it could be legal exposure and regulatory action. By treating data protection as a business priority now, companies can reduce risk and take advantage of the law's safe harbor protections.

Attorneys

- Aaron C. Tifft

Practices

- Cybersecurity & Data Privacy