THE JOURNAL RECORD

December 17,2015

GAVEL TO GAVEL

Data breaches

While every business owner should understand the importance of protecting the personal information of customers and employees, the legal obligations resulting from a data breach may not always be clear.

Although the issue has been discussed and debated for nearly 20 years, there is no federal data breach law to provide uniform guidance. Because of this federal void, business owners must look to state statutes to find legislation that specifically addresses their responsibilities following a data breach.

DIANA TATE VERMEIRE

Oklahoma joins 46 other states that have incorporated data breach language into their statutes. The definition of "breach" and "personal information" can vary from state to state, as can the notice requirements. It's important to know that the applicable law under which a business must comply is based upon the jurisdiction of residency of the individual affected, not the physical location of the breached company.

Oklahoma's Security Breach Notification Act defines, in part, a breach of the security system as "the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity ... as part of a database ... and that causes ... or will cause, identity theft or other fraud to any resident of this state."

The act defines personal information as an individual's first name or initial and last name combined with the individual's Social Security number, driver's license number and/or financial account number, credit card or debit card in combination with any required security code, access code or password.

But, what is required of a company following a data breach? Under Oklahoma law, any resident whose unencrypted/unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person when there is a reasonable belief that identity theft or other fraud may occur must be notified as soon as practicable following discovery.

Additionally, notification is required if encrypted information is accessed in an unencrypted form or if the breach involves a person with access to the encryption key. In Oklahoma, there is no de minimis for exclusion from coverage, so the act applies even if only one person's data was exposed.

While preventing a breach is always the preferred outcome, knowledge of and compliance with Oklahoma's data breach statute can help limit the financial and reputational damage that can follow should a data breach occur.

Diana Tate Vermeire is a shareholder with the law firm of GableGotwals.