# PUBLICATION

## Important Notice Regarding Amendments to Tennessee's Breach Notification Statute

**Authors: Alisa L. Chestler**
**April 2016**

All companies with Tennessee employees or customers need to revise their data incident policies and procedures. Tennessee has revised their breach notification statute to remove the encryption safe harbor, which previously obviated the need to notify individuals when encrypted assets containing personal information were lost, stolen or compromised. Tennessee is the first state in the nation to remove the safe harbor.

Despite the removal of the safe harbor, the statute still permits an organization to perform an analysis to determine whether an incident requiring notification has occurred. Specifically, that analysis requires an organization to determine whether an unauthorized acquisition of data "materially compromises the security, confidentiality, or integrity of personal information." Arguably, if the information is undecipherable or inaccessible to a bad actor because it is encrypted, the information has likely not been "materially" compromised. Even so, regardless of the level of encryption, organizations are cautioned to still approach every incident on case-by-case basis and work with counsel and their security vendors to determine whether a reportable incident has occurred.

This is not the only newsworthy aspect of the amendment. Tennessee has also amended its data breach notification statute to require organizations to notify Tennessee residents within ***45 days*** after discovery of a breach. Previously, the law contained a requirement that businesses were to notify individuals in the most expedient time possible and without unreasonable delay.

The law also amends the statute to clarify when an unauthorized disclosure has occurred. The amendment now specifies that an "unauthorized person" includes an employee of the organization who is discovered to have obtained personal information and intentionally used it for an unlawful purpose.

The Tennessee law takes effect July 1, 2016.

**Key Takeaways:**

- Organizations holding personal information of Tennessee residents need to amend their incident policies and procedures to reflect the removal of the encryption safe harbor. Employees should also be retrained regarding their immediate obligation to report any lost or stolen IT assets, including BYOD devices which contain personal information.
- Given the new 45-day timeframe, businesses must have working incident response and breach notification policies and procedures in place. Failure to have policies and procedures in place – with key stakeholders' contacts in place for legal, insurance, law enforcement, regulatory, computer forensics, PR, *etc.* – will likely result in reporting outside of the statutorily mandated timeframe. Companies should also routinely test their incident response policies to ensure timely action with the 45-day period.
- Businesses should take this opportunity to dust off their access control policies to ensure that employees are not accessing databases or files without authorization and that employees only have access to the minimum amount of information necessary to complete their tasks. Should an employee

access files or databases without authorization, the business must conduct an investigation as to the motives, if any, of the individual who obtained the access to personal information and make a determination whether the use was for an "unlawful purpose."

For more information about how this amendment may affect your business or for assistance with your breach preparedness and response needs, contact any member of the Firm's Privacy and Information Security Team.