# Tennessee Legislature Amends Data Breach Notification Statute - Encryption is No Longer an Automatic Safe Harbor

Miller & Martin Alert PLLC | June 14, 2016
by ***Leah Gerbitz***

On March 24, 2016, Governor Haslam signed S.B. 2005 which amends Tennessee's data breach notice statute. The amended statute will go into effect on July 1, 2016.The new Tennessee breach notice requirements are triggered by the unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the information holder. The key consideration to determine when notice must be provided regarding a data breach is whether the integrity of the personal information has been compromised by the unauthorized access. There are two significant changes in the amended statute: 1) there is no longer a safe harbor to breach notice if the data was encrypted and 2) breach notice must be given within 45 days.

**Encryption is No Longer an Automatic Safe Harbor**

The amended statute makes Tennessee the first state to potentially require breach notice even if the data is encrypted. To date, all other breach notification laws do not require notice if the data is encrypted. The amendment reflects a concern expressed by legislators that theft of encrypted data remains a cyber threat. Generally, encryption of data has been considered the gold standard for data security. While encryption of any type is more secure than leaving the data in plain text, some encryption methods are too simple and can be decrypted fairly easily. The amended statute requires a review of the relative strength and complexity of the encryption employed with each data breach rather than applying an automatic safe harbor when any encryption is in place. It is important to note that the amended statute only requires breach notice when the unauthorized acquisition materially compromises security, confidentiality or integrity of the data. Thus, if it is determined the encryption is sufficiently protective, notice is not necessarily required.

It should be noted that the legislative discussions regarding this amendment occurred close in time to when the United States Department of Justice filed its motion to require Apple to break the encryption on the iPhone related to the San Bernadina terrorist attack. The Legislators' doubts as to the effectiveness of some encryption programs may have led to the enactment of this amendment. However, it is also possible the amended language is not significant because the statute still generally defines the "breach of personal information" that triggers the notice requirement to only include unencrypted personal information. This statutory ambiguity may be a legislative oversight?time will tell. For the time being, the prudent course is to interpret the amended statute to no longer have an encryption safe harbor for breach notices.

**Notice Must be Given No Later Than 45 Days After Breach**

The amended statute now requires notification to any Tennessee resident immediately but no later than 45 days from discovery or notice of a data breach. Previously the law required breach notice within the most expedient time possible. Tennessee joins 9 other states in mandating a defined period of time for notice. Tennessee's breach notice statute is one of the more demanding in the nation as it does not permit delays in notice for remediation or investigation of the breach unless a law enforcement agency determines the notice will impede a criminal investigation.

The amendments also clarify that breach notification is required when an authorized employee of the information holder acquires personal information and intentionally misuses it for unlawful purposes.

Finally, the amendment provides an exemption to any information holder governed by the requirements of Gramm-Leach-Bliley and/or HIPAA.

If you have any questions about the amendment or how it may affect your company, please contact Leah Gerbitz.