WINSTON & STRAWN LLP

BLOG

Tennessee (Re)Amends its Data Breach Notification Law

MAY 1, 2017

Only a year after its last change, Tennessee has again amended its data breach notification law. Changes include adding back in the encryption exception, such that organizations are required to give notification to individuals as a result of a data breach only when the acquired information was unencrypted. However, as now drafted, the law contains a definition of encrypted data, namely that which follows the Federal Information Processing Standard (FIPS), something it did not have before. Tennessee is unique among the state breach notification laws in citing to FIPS as a reference for what constitutes encrypted data, but several agencies such as the U.S. Treasury and HHS use FIPS in their own industry-specific breach notification requirements.

The law now also requires vendors (third parties who experience a breach of information they are holding on behalf of another) to notify the data owner either within 45 days after discovery of the breach.

Finally, the amendment also clarified that notice can be made by email not only if the notice is consistent with the E-Sign Act, but also if the organization's primary method of communication with the individual was by electronic means. The amended law went into effect on April 4, 2017, the day on which it was signed by the governor.

TIP: Companies with nationwide incident response plans should keep in mind Tennessee's new definition of encryption, the need to notify data owners (if the company is a vendor) within 45 days, and the added flexibility for providing email notification.

1 Min Read

Author

Eric Shinabarger

Related Locations

Chicago

Related Topics

Data Breach

Related Capabilities

Privacy & Data Security

Related Regions

North America

Related Professionals

Eric Shinabarger

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.