

And then there were four

Mississippi becomes the 46th state to enact a data breach notification law: Only four states remain without similar laws

Mississippi has joined the majority of other states and now has a law that governs an organization's obligations should it suffer a data breach relative to Personal Information (PI) of a Mississippi resident. Only four states in the United States have not passed similar legislation – Alabama, Kentucky, New Mexico and South Dakota.

Similar to many other state data breach notification laws, the obligation falls on any organization which owns, licenses or maintains PI of any resident of Mississippi. Like others, Mississippi defines PI as an individual's first name or first initial and last name along with Social Security number, driver's license number or financial account number or credit card number (along with the required security or access code).

Should an organization be required to notify impacted individuals relative to a breach of their PI, such notice should be made without unreasonable delay. Notice can be made in writing, by telephone, through electronic means (if the person's primary means of communication with the affected individuals is by electronic means), or through substitute notice (provided that the cost of providing notice will exceed \$5,000 or the affected class of persons is more than 5,000 individuals).

A safe harbor exists if, after an appropriate investigation, the entity reasonably determines that the breach will not likely result in harm to the affected individuals. If the PI was encrypted, there is a presumption that harm will not result. In either case, notification would not be required.

The new Mississippi law will be enforced by the Mississippi Attorney General, but the law expressly excludes a private right of action.

If you have any questions, contact:

James J. Giszczak
248.220.1354
jgiszczak@mcdonaldhopkins.com

Dominic A. Paluzzi
248.220.1356
dpaluzzi@mcdonaldhopkins.com

or any of our Data Privacy and Network Security attorneys by clicking on the link below:

[Data Privacy and Network Security](#)

McDonald Hopkins counsels businesses and organizations regarding all aspects of data privacy and network security, including proactive compliance with the numerous state, federal and private data security regulations (including PCI DSS and HITECH) relative to personal information and protected health information, training of employees and preventative measures to decrease the risk of data theft. We also counsel businesses and organizations through the data breach response process and coordinate notifications to affected individuals and state attorneys general, as well as advising on media related issues. Our attorneys can help you properly assess your risks to ensure compliance. After you complete the brief McDonald Hopkins Data Privacy and Network Security Review, your company will be provided with an assessment of the required areas of compliance which have the greatest need of attention and improvement.