

TECHNOLOGY

WEB WORRIES

» Data breach notification law now in effect but legislation open to interpretation

By **WALLY NORTHWAY** | STAFF WRITER
wally.northway@msbusiness.com

A new state law requiring all persons or entities, both in the private and public sectors, that conduct business in Mississippi to notify customers in the event of a data breach is now in effect.

However, some important provisions in the legislation are vague, particularly in determining if a breach must be reported and the required minimum response time.

That may have to be hammered out in court, according to Mississippi Attorney General Jim Hood.

Hood said the bill originally was meant to combat breaches whether the cause was negligence on the company's part or malicious intent. The final bill was restricted to only malicious intent, Hood said, and was amended so as not to overburden businesses, especially small ones.

While the final bill was not entirely what he was hoping for, still Hood said it was a step in the right direction in curbing ever-growing cyber crime.

"The Internet is the crime scene of the 21st century," Hood said.

With its passage, Mississippi became the 46th state to enact a data breach notification law, which became effective July 1.

"These laws were enacted in response to an escalating number of breaches of consumer databases containing personal information that could be used to perpetuate crimes such as financial or medical identity theft," said Tony Brooks, CISA, principal and director of information technology assurance and risk services at Ridgeland-based HORNE LLP.

Last April, Gov. Haley Barbour signed House Bill 583 into law. The bill cleared both houses of the Mississippi Legislature during the Regular Session without a single dissenting vote.

"These laws were enacted in response to an escalating number of breaches of consumer databases containing personal information that could be used to perpetuate crimes such as financial or medical identity theft."

BREACH OF SECURITY

» **WHO:** The law "applies to any person who conducts business in this state and who, in the ordinary course of the person's business functions, owns, licenses or maintains personal information of any resident of this state."

» **WHAT:** "Breach of security" means unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of this state when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements: social security number; driver's license number or state identification card number; or, an account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account; "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media."

» **HOW:** "Any notice...may be provided by one of the following methods: Written notice; telephone notice; electronic notice, if the person's primary means of communication with the affected individuals is by electronic means or if the notice is consistent with the provisions regarding electronic records and signatures set forth in 15 USCS 7001; or substitute notice, provided the person demonstrates that the cost of providing notice...would exceed \$5,000, that the affected class of subject persons to be notified exceeds 5,000 individuals

or the person does not have sufficient contact information. Substitute notice shall consist of the following: Electronic mail notice when the person has an electronic mail address for the affected individuals; conspicuous posting of the notice on the Web site of the person if the person maintains one; and, notification to major statewide media, including newspapers, radio and television.

"Notification shall not be required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals."

» **WHEN:** "Any person who conducts business in this state that maintains computerized data which includes personal information that the person does not own or license shall notify the owner or licensee of the information of any breach of the security of the data as soon as practicable following its discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person for fraudulent purposes.

"Any notification...shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation or national security and the law enforcement agency has made a request that the notification be delayed.

"Failure to comply...shall constitute an unfair trade practice and shall be enforced by the Attorney General."

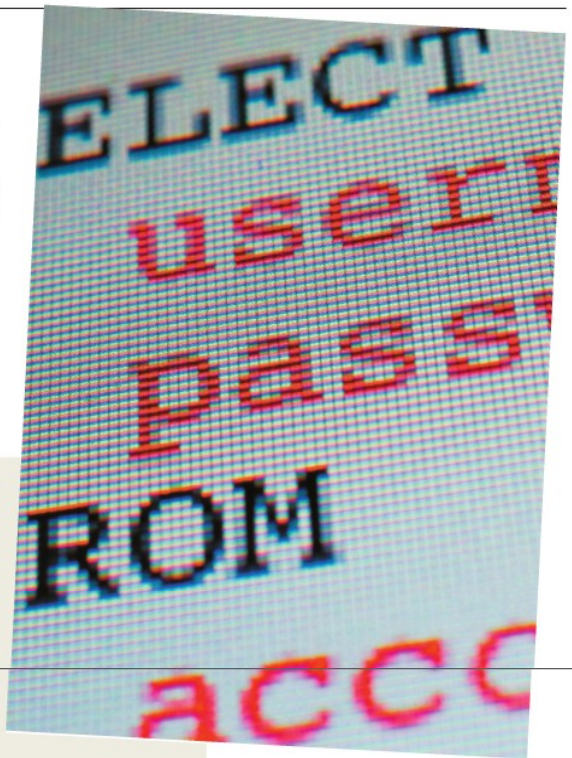
— Wally Northway

"I was pleased with the vote. You never know how these things are going to go during an election year," said Rep. George Flaggs Jr. (D-Warren), who co-wrote the bill with principal author Rep. Brandon Jones (D-Jackson).

When asked about some of the law's provisions, especially those governing response

time and notification requirements, Flaggs said that the new law's aim is "not to run companies out of business; its aim is to protect consumers."

Hood said some companies may use leeway in the provisions to skirt it. For example, the law allows affected companies to determine —



"after reasonable investigation" — if a breach caused any harm to its customers. If they see no potential harm, they do not have to report it.

Another provision Hood said might be contested is the mandated response time, which is simply "as soon as possible."

"That is just another potential defense companies are going to throw up in court," Hood said.

Brooks, who has 26 years in the business, the last eight of those with HORNE, has other questions.

"How is a company to know if its data has been breached, and how are consumers to know?" he asked.

Chad Curtis, vice president of engineering at BCI, which offers network security solutions, agreed.

"Companies need more than just intrusion protection," Curtis said. "Companies have to have a way to monitor and correlate events and watch for malicious intent. What scares me the most is small businesses. They might not have such a system in place. If they are breached, they might not even know it."

Curtis said when it comes to securing data, costs can vary. It depends on the size of the company, scale, number of transactions, etc.

Brooks said he has known of companies spending as much as \$100,000 to secure their system and monitor any potential breaches.

Hood said he is worried more about the cost to consumers.

"My social security number is mine," he said. "I don't care if it's due to negligence or not. I just want to know (if there is a breach)."

Noncompliance will be treated as an unfair trade act under the Consumer Protection Act. The penalties will depend on the violation. Civil violations carry a fine not to exceed \$10,000 per violation.

Criminal offenses are a misdemeanor, and carry a maximum penalty of one to five years in prison and/or a fine of \$1,000 to \$5,000.



Hood



Brooks

Tony Brooks
HORNE LLP, Ridgeland