Mississippi Code of 1972
Title 75 – Regulation of Trade, Commerce and Investments
Chapter 24 – Regulation of Business for Consumer Protection

§ 75-24-29. Persons conducting business in Mississippi required to provide notice of a breach of security involving personal information to all affected individuals; enforcement [Effective July 1, 2011].

(1) This section 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.

(2) For purposes of this section, the following terms shall have the meanings ascribed unless the context clearly requires otherwise:

(a) "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;

(b) "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:

(i) Social security number;

(ii) Driver's license number or state identification card number; or

(iii) 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;

(iv) "Affected individual" means any individual who is a resident of this state whose personal information was, or is reasonably believed to have been, intentionally acquired by an unauthorized person through a breach of security.

(3) A person who conducts business in this state shall disclose any breach of security to all affected individuals. The disclosure shall be made without unreasonable delay, subject to the provisions of subsections (4) and (5) of this section and the completion of an investigation by the person to determine the nature and scope of the incident, to identify the affected individuals, or to restore the reasonable integrity of the data system. 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.

(4) 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.

(5) Any notification required by this section 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. Any such delayed notification shall be made after the law enforcement agency determines that notification will not compromise the criminal investigation or national security and so notifies the person of that determination.

(6) Any notice required by the provisions of this section may be provided by one (1) of the following methods: (a) written notice; (b) telephone notice; (c) 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 (d) substitute notice, provided the person demonstrates that the cost of providing notice in accordance with paragraph (a), (b) or (c) of this subsection would exceed Five Thousand Dollars ($5,000.00), that the affected class of subject persons to be notified exceeds five thousand (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.

(7) Any person who conducts business in this state that maintains its own security breach procedures as part of an information security policy for the treatment of personal information, and otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security breach notification requirements of this section if the person notifies affected individuals in accordance with the person's policies in the event of a breach of security. Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or federal functional regulator, as defined in 15 USCS 6809(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided the person notifies affected individuals in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or federal functional regulator in the event of a breach of security of the system.

(8) Failure to comply with the requirements of this section shall constitute an unfair trade practice and shall be enforced by the Attorney General; however, nothing in this section may be construed to create a private right of action.