Miss. Code Ann. § 83-5-811

Current with 2024 1st and 2nd Extraordinary Sessions and Regular Session legislation signed by the Governor and effective upon passage through April 15, 2024, not including changes and corrections made by the Joint Legislative Committee on Compilation, Revision and Publication of Legislation.

§ 83-5-811. Notification of cybersecurity event involving nonpublic information; information to be provided; investigation of cybersecurity event in system maintained by third-party service provider.

(1) Each licensee shall notify the commissioner as promptly as possible but in no event later than three (3) business days from a determination that a cybersecurity event involving nonpublic information that is in the possession of a licensee has occurred when either of the following criteria has been met:

(a) This state is the licensee's state of domicile, in the case of an insurer, or this state is the licensee's home state, in the case of a producer, as those terms are defined in Section 83-17-53, and the cybersecurity event has a reasonable likelihood of materially harming a consumer residing in this state or reasonable likelihood of materially harming any material part of the normal operation(s) of the licensee; or

(b) The licensee reasonably believes that the nonpublic information involved is of two hundred fifty (250) or more consumers residing in this state and that is either of the following:

(i) A cybersecurity event impacting the licensee of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body pursuant to any state or federal law; or

(ii) A cybersecurity event that has a reasonable likelihood of materially harming:

1. Any consumer residing in this state; or

2. Any material part of the normal operation(s) of the licensee.

(2) The licensee shall provide as much of the following information as possible. The licensee shall provide the information in electronic form as directed by the commissioner. The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner regarding material changes to previously provided information relating to the cybersecurity event.

(a) Date of the cybersecurity event;

(b) Description of how the information was exposed, lost, stolen or breached, including the specific roles and responsibilities of third-party service providers, if any;

(c) How the cybersecurity event was discovered;

(d) Whether any lost, stolen, or breached information has been recovered and if so, how this was done;

(e) The identity of the source of the cybersecurity event;

(f) Whether the licensee has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;

(g) Description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information or types of information allowing identification of the consumer;

(h) The period during which the information system was compromised by the cybersecurity event;

(i) The number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner pursuant to this section;

(j) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;

(k) Description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur;

(l) A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event; and

(m) Name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.

(3) Licensee shall comply with Section 75-24-29, as applicable, and provide a copy of the notice sent to consumers under that statute to the commissioner, when a licensee is required to notify the commissioner under subsection (1) of this section.

(4)

(a) In the case of a cybersecurity event in a system maintained by a third-party service provider, of which the licensee has become aware, the licensee shall treat such event as it would under subsection (1) of this section unless the third-party service provider provides the notice required under subsection (1) of this section to the commissioner.

(b) The computation of licensee's deadlines shall begin on the day after the third-party service provider notifies the licensee of the cybersecurity event or the licensee otherwise has actual knowledge of the cybersecurity event, whichever is sooner.

(c) Nothing in this article shall prevent or abrogate an agreement between a licensee and another licensee, a third-party service provider or any other party to fulfill any of the

investigation requirements imposed under Section 83-5-809 or notice requirements imposed under this section.

(5)

(a)

(i) In the case of a cybersecurity event involving nonpublic information that is used by the licensee who is acting as an assuming insurer or in the possession, custody or control of a licensee who is acting as an assuming insurer and that does not have a direct contractual relationship with the affected consumers, the assuming insurer shall notify its affected ceding insurers and the commissioner of its state of domicile within three (3) business days of making the determination that a cybersecurity event has occurred.

(ii) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under Section 75-24-29 and any other notification requirements relating to a cybersecurity event imposed under this section.

(b)

(i) In the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of a third-party service provider of a licensee who is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the commissioner of its state of domicile within three (3) business days of receiving notice from its third-party service provider that a cybersecurity event has occurred.

(ii) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under Section 75-24-29 and any other notification requirements relating to a cybersecurity event imposed under this section.

(c) Any licensee acting as assuming insurer shall have no other notice obligations relating to a cybersecurity event or other data breach under this section or any other law of this state.

(6) In the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of a licensee who is an insurer or its third-party service provider for which a consumer accessed the insurer's services through an independent insurance producer, and for which consumer notice is required under Section 75-24-29, the insurer shall notify the producers of record of all affected consumers of the cybersecurity event no later than the time at which notice is provided to the affected consumers. The insurer is excused from this obligation for any producers who are not authorized by law or contract to sell, solicit or negotiate on behalf of the insurer, and in those instances in which the insurer does not have the current producer of record information for any individual consumer.

History

Laws, 2019, ch. 448, § 6, eff from and after July 1, 2019.

End of Document