La. R.S. § 22:2506

Current through the 2024 First Extraordinary Session and Act 22 of the Second Extraordinary Session. Revisions of the Louisiana State Law Institute now current through all titles received as of February 1, 2024.

§ 22:2506. Notification of a cybersecurity event

A. A licensee shall notify the commissioner without unreasonable delay but in no event later than three business days from a determination that a cybersecurity event involving nonpublic information that is in the possession of the licensee has occurred when either of the following criteria has been met:

(1) 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, an adjuster, or public adjuster as those terms are defined in R.S. 22:1542, 1661, or 1692, and the cybersecurity event has reasonable likelihood of materially harming either of the following:

(a) Any consumer residing in this state.

(b) Any material part of the normal operations of the licensee.

(2) A licensee reasonably believes that the nonpublic information involved is for two hundred fifty or more consumers residing in this state and that either of the following has occurred:

(a) A cybersecurity event affecting 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.

(b) A cybersecurity event that has a reasonable likelihood of materially harming any of the following:

(i) Any consumer residing in this state.

(ii) Any material part of the normal operations of the licensee.

B.

(1) 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 relative to the cybersecurity event.

(2) The licensee making the notification required in Subsection A of this Section shall provide as much of the following information as possible in electronic form as directed by the commissioner:

(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 any third-party service providers.

(c) How the cybersecurity event was discovered.

(d) Whether any lost, stolen, or breached information has been recovered and, if so, how reocvery was accomplished.

(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 when the notification was provided.

(g)

(i) Description of the specific types of information acquired without authorization.

(ii) For the purposes of this Subparagraph, "specific types of information" means particular data elements including but not limited to types of medical information, types of financial information, or types of information allowing identification of the consumer.

(h) The period during which the cybersecurity event compromised the information system.

(i)

(i) The total number of consumers in this state affected by the cybersecurity event.

(ii) 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.

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

C. A licensee shall comply with the Database Security Breach Notification Law, R.S. 51:3071 et seq., as applicable, and shall provide to the commissioner a copy of the notice sent to consumers if the licensee is required to notify the commissioner pursuant to Subsection A of this Section.

D.

(1) In the case of a cybersecurity event in a system maintained by a third-party service provider of which the licensee has become aware, all of the following shall apply:

(a) The licensee shall treat the cybersecurity event as it would pursuant to Subsection A of this Section, unless the third-party service provider gives the notice required in Subsection A of this Section.

(b) The computation of the 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 occurs first.

(2) Nothing in this Chapter shall be construed to 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 pursuant to R.S. 22:2505 or notice requirements pursuant to this Section.

E.

(1)

(a) In the case of a cybersecurity event involving nonpublic information used by a licensee acting as an assuming insurer or in the possession, custody, or control of a licensee 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 business days of making the determination that a cybersecurity event has occurred.

(b) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements pursuant to the Database Security Breach Notification Law and any other notification requirements relating to a cybersecurity event pursuant to this Section.

(2)

(a) 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 that is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the commissioner of its state of domicile within three business days of receiving notice from its third-party service provider that a cybersecurity event has occurred.

(b) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements pursuant to the Database Security Breach Notification Law and any other notification requirements relating to a cybersecurity event pursuant to this Section.

F. In the case of a cybersecurity event involving nonpublic information that is in the possession, custody, or control of a licensee that 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 by the Database Security Breach Notification Law, 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 shall be 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 an individual consumer.

History

Acts 2020, No. 283, § 1, effective August 1, 2020.

End of Document