THE INSURANCE CODE OF 1956 (EXCERPT)
Act 218 of 1956

500.559 Notification of cybersecurity event involving nonpublic information; duty to update and supplement notifications to director; contents; application to third-party service provider; duties of ceding insurers with direct contractual relationship.

Sec. 559. (1) Each licensee shall notify the director as promptly as possible but not later than 10 business days after 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, for an insurer, or this state is the licensee's home state, for an insurance producer as that term is defined in section 1201, and the cybersecurity event has a reasonable likelihood of materially harming either of the following:

(*i*) A consumer residing in this state.

(*ii*) Any material part of a normal operation of the licensee.

(b) The licensee reasonably believes that the nonpublic information involved is of 250 or more consumers residing in this state and 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 other supervisory body under any state or federal law.

(*ii*) A cybersecurity event that has a reasonable likelihood of materially harming either of the following:

(A) Any consumer residing in this state.

(B) Any material part of the normal operation of the licensee.

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

(a) The date of the cybersecurity event.

(b) A 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 the notification was provided.

(g) A description of the specific types of information acquired without authorization. As used in this subdivision, "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 director and update this estimate with each subsequent report to the director under 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) A description of efforts being undertaken to remediate the situation that 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) The name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.

(3) A licensee shall comply with this chapter, as applicable, and provide a copy of the notice sent to consumers under this chapter, if a licensee is required to notify the director under section 559.

(4) For a cybersecurity event in a system maintained by a third-party service provider, of which the licensee has become aware, the licensee shall treat the event as it would under this section. The computation of the licensee's deadlines begins 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 earlier. This chapter does not 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 557 or notice requirements imposed under this section.

(5) For a cybersecurity event involving nonpublic information that is used by the licensee that is acting as an assuming insurer or in the possession, custody, or control of a licensee that 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 director of its state of domicile within 10 business days after making the determination that a cybersecurity event has occurred. The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under this section. For 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 director of its state of domicile within 10 business days after receiving notice from its third-party service provider that a cybersecurity event has occurred. The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under this chapter.

(6) A licensee acting as an assuming insurer does not have other notice obligations relating to a cybersecurity event or other data breach under this section or any other law of this state.

(7) For 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 under this chapter, the insurer shall notify the producers of record of all affected consumers of the cybersecurity event not later than the time at which notice is provided to the affected consumers. The insurer is excused from this obligation for any producer who is 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: Add. 2018, Act 690, Eff. Jan. 20, 2021.

Popular name: Act 218