Burns Ind. Code Ann. § 27-2-27-21

Current through P.L. 4-2024 of the Second Regular Session of the 123rd General Assembly.

Burns' Indiana Statutes Annotated > Title 27 Insurance (Arts. 1 — 19) > Article 2 Powers and Duties of Insurers (Chs. 1 — 29) > Chapter 27 Insurance Data Security (§§ 27-2-27-1 — 27-2-27-32)

27-2-27-21. Investigation of cybersecurity event — Records — Notice to commissioner.

(a) If a licensee learns that a cybersecurity event has or may have occurred, the licensee, or an outside vendor or service provider designated to act on the licensee's behalf, shall conduct a prompt investigation. During the investigation, the licensee or outside vendor or service provider designated to act on the licensee's behalf shall:

(1) determine:

(A) whether a cybersecurity event has occurred;

(B) if so, the nature and scope of the cybersecurity event; and

(C) whether any nonpublic information may have been involved in the cybersecurity event; and

(2) perform or oversee reasonable measures to restore the security of the information systems compromised in the cybersecurity event in order to prevent further unauthorized acquisition, release, or use of nonpublic information in the licensee's possession, custody, or control.

(b) A licensee shall maintain records concerning all cybersecurity events for at least five (5) years after the date of the cybersecurity event. A licensee shall produce these records upon demand of the commissioner.

(c) A licensee shall notify the commissioner as promptly as possible but not later than three (3) business days after a determination that a cybersecurity event involving nonpublic information that is in the possession of the licensee has occurred if either of the following applies:

(1) Indiana is the licensee's state of domicile, if the licensee is an insurer, or the licensee's home state, if the licensee is a producer, and the cybersecurity event has a reasonable likelihood of materially harming a consumer residing in Indiana or materially harming any material part of the normal operations of the licensee.

(2) The licensee reasonably believes that the nonpublic information of at least two hundred fifty (250) consumers residing in Indiana was affected by the cybersecurity event and that the cybersecurity event is either of the following:

(A) A cybersecurity event impacting the licensee of which notice is required to be provided by any other state, federal, or local law.

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

(i) a consumer residing in Indiana; or

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

(d) After learning that a cybersecurity event has or may have occurred, a licensee shall provide as much of the following information as possible in electronic form, as directed by the commissioner:

(1) The date of the cybersecurity event.

(2) A description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of any third party service providers.

(3) How the cybersecurity event was discovered.

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

(5) The identity of the source of the cybersecurity event.

(6) 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.

(7) A 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.

(8) The period during which the information system was compromised by the cybersecurity event.

(9) The total number of consumers in Indiana 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 under this section.

(10) The results of any internal review:

(A) identifying a lapse in either automated controls or internal procedures; or

(B) confirming that all automated controls or internal procedures were followed.

(11) A description of efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur.

(12) 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.

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

(e) The licensee has 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.

(f) A licensee shall comply with IC 24-4.9, as applicable, and provide a copy of the notice sent to consumers under IC 24-4.9 to the commissioner if the licensee is required to notify the commissioner under subsection (c).

(g) Nothing in this chapter abrogates or prevents an agreement between a licensee and:

(1) another licensee;

(2) a third party service provider; or

(3) any other party;

to fulfill any investigation requirements imposed under subsection (a) or notice requirements imposed under subsections (c) through (f).

History

P.L.130-2020, § 10, effective July 1, 2020.

End of Document