40 Pa.C.S. § 4518

Pa.C.S. documents are current through 2024 Regular Session Act 13; P.S. documents are current through 2024 Regular Session Act 13

§ 4518. Notification of cybersecurity event.

(a) Notification to commissioner. A licensee shall notify the commissioner as promptly as possible, but in no event later than five 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 have been met:

(1) The cybersecurity event has a reasonable likelihood of materially harming a consumer residing in this Commonwealth or any material part of the normal operations of the licensee and either:

(i) in the case of an insurer, this Commonwealth is the insurer's state of domicile; or

(ii) in the case of an insurance producer, as defined in section 601-A of the act of May 17, 1921 (P.L.789, No.285), known as The Insurance Department Act of 1921, this Commonwealth is the insurance producer's home state.

(2) The licensee reasonably believes that the nonpublic information involves 250 or more consumers residing in this Commonwealth and the cybersecurity event:

(i) impacts the licensee of which notice is required to be provided to a governmental body, self-regulatory agency or another supervisory body under any Federal or State law; or

(ii) has a reasonable likelihood of materially harming a consumer residing in this Commonwealth or any material part of the normal operations of the licensee.

(b) Content of notification. As part of the notification under this section, a licensee shall provide as much of the following information as possible in electronic form:

(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 third-party service providers, if any.

(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, governmental or law enforcement agency and, if so, when the notification was provided.

(7) A description of the specific types of information acquired without authorization, including particular data elements such as the types of medical information, financial information or other types of information allowing identification of the consumer.

(8) The period during which the information systems were compromised by the cybersecurity event.

(9) The number of total consumers in this Commonwealth 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 identifying a lapse in either automated controls or internal procedures or 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 that the licensee will take to investigate and notify consumers affected by the cybersecurity event.

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

(c) Continuing obligation. A 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 a cybersecurity event.

(d) Other notices required. A licensee shall comply with section 3 of the act of December 22, 2005 (P.L.474, No.94), known as the Breach of Personal Information Notification Act, as applicable, and provide a copy of the notice sent to consumers under the Breach of Personal Information Notification Act to the commissioner, whenever the licensee is required to notify the commissioner under subsection (a).

(e) Notice regarding cybersecurity events of third-party service providers.

(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, the licensee shall treat the event as it would under subsection (a) unless the third-party service provider provides the notice required under subsection (a) directly to the commissioner.

(2) The computation of a licensee's deadlines under this section 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.

(f) Notice regarding cybersecurity events of reinsurers to insurers.

(1) In the case of a cybersecurity event involving nonpublic information that is used by a licensee, which is acting as an assuming insurer, or that is in the possession, custody or control of a licensee, which is acting as an assuming insurer and which 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. The ceding insurers that have a direct contractual relationship with the affected consumers shall fulfill the consumer notification requirements imposed under section 3 of the Breach of Personal Information Notification Act and any other notification requirements relating to a cybersecurity event imposed under this section.

(2) 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. The ceding insurers that have a direct contractual relationship with the affected consumers shall fulfill the consumer notification requirements imposed under section 3 of the Breach of Personal Information Notification Act and any other notification requirements relating to a cybersecurity event imposed under this section.

(3) A licensee acting as an 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 Commonwealth.

(g) Notice regarding cybersecurity events of insurers to producers of record. In the case of a cybersecurity event involving nonpublic information 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 insurance producer, and for which consumer notice is required under section 3 of the Breach of Personal Information Notification Act, 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 in those instances in which the insurer does not have the current producer of record information for an individual consumer.

History

Act 2023-2 (H.B. 739), § 1, approved June 14, 2023, effective December 11, 2023.