Ohio Revised Code

Section 3965.04 Notification to superintendent.

Effective: March 20, 2019
Legislation: Senate Bill 273 - 132nd General Assembly

(A) Each licensee shall notify the superintendent of insurance as promptly as possible after a determination that a cybersecurity event involving nonpublic information in the possession of the licensee has occurred, but in no event later than three business days after that determination, when either of the following criteria has been met:

(1) Both of the following apply:

(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 an independent insurance agent.

(b) The cybersecurity event has a reasonable likelihood of materially harming a consumer or a material part of the normal operations of the licensee.

(2) The licensee reasonably believes that the nonpublic information involved relates to two hundred fifty or more consumers residing in this state and the cybersecurity event is either of the following:

(a) 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;

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

(i) Any consumer residing in this state;

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

(B)(1) In providing the notification described in division (A) of this section, 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 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 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) A description of the specific types of information acquired without authorization. "Specific types of information" means particular data elements, including 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 superintendent and update this estimate with each subsequent report to the superintendent 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) 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.

(2) The licensee shall provide the information in electronic form as directed by the superintendent. The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the superintendent regarding material developments relating to the cybersecurity event.

(C) A licensee shall comply with section 1349.19 of the Revised Code as applicable and provide a copy of the notice sent to consumers under that section to the superintendent, when the licensee is required to notify the superintendent under division (A) of this section.

(D)(1) If a licensee becomes aware of a cybersecurity event in a system maintained by a third-party service provider, the licensee shall treat the event as it would under division (A) of this section.

(2) The computation of the licensee's deadlines specified in 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.

(3) Nothing in this chapter 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 3965.03 of the Revised Code or notice requirements imposed under this section.

(E)(1) In the case of a cybersecurity event involving nonpublic information that is used by or in the possession, custody, or control of a licensee that is acting as an assuming insurer, including an assuming insurer that is domiciled in another state or jurisdiction, and that does not have a direct contractual relationship with the affected consumers, both of the following apply:

(a) The assuming insurer shall notify its affected ceding insurers and the insurance commissioner of

its state or jurisdiction 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 imposed under section 1349.19 of the Revised Code 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 licensee's third-party service provider, when the licensee is acting as an assuming insurer, including an assuming insurer that is domiciled in another state or jurisdiction, both of the following apply:

(a) The assuming insurer shall notify its affected ceding insurers and the insurance commissioner of its state or jurisdiction 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 imposed under section 1349.19 of the Revised Code and any other notification requirements relating to a cybersecurity event imposed under this section.

(3) Any licensee acting as an assuming insurer shall have no other notice obligations relating to a cybersecurity event or other data breach under division (A) of 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, that was obtained by the insurer from a consumer accessing the insurer's services through an independent insurance agent, and for which disclosure or notice is required under section 1349.19 of the Revised Code, the insurer shall notify the independent insurance agents of record of all affected consumers.

The insurer is excused from this obligation for any independent insurance agents who are not authorized by law or contract to sell, solicit, or negotiate on behalf of the insurer, and for those instances in which the insurer does not have the current independent insurance agent of record information for an individual consumer.