Tenn. Code Ann. § 56-2-1006

56-2-1006. Notification of a cybersecurity event.

(a) A licensee shall notify the commissioner as soon as practicable, and in no event more than three (3) business days, following a determination that a cybersecurity event has occurred if:

(1)

(A) The licensee is domiciled in this state, in the case of an insurer, as defined in § 56-6-102, or this state is the licensee's home state, in the case of an insurance producer, as defined in § 56-6-102; and

(B) The cybersecurity event has a reasonable likelihood of materially harming a consumer residing in this state or a material part of the licensee's normal operations; or

(2) The licensee reasonably believes that the nonpublic information of two hundred fifty (250) or more consumers residing in this state is involved in the cybersecurity event and that the cybersecurity event is:

(A) A cybersecurity event of which notice must be provided to a government body, self-regulatory agency, or other supervisory body pursuant to state or federal law; or

(B) A cybersecurity event with a reasonable likelihood of materially harming a consumer residing in this state or a material part of the licensee's normal operations.

(b)

(1) A licensee that must notify the commissioner under subsection (a) shall provide to the commissioner, in a format directed by the commissioner, as much of the following information as is available:

(A) The date of the cybersecurity event;

(B) A description of how the nonpublic information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers with respect to the nonpublic information, if any;

(C) How the cybersecurity event was discovered;

(D) Whether lost, stolen, or breached nonpublic information has been recovered and, if so, how recovery was accomplished;

(E) The identity of the source of the cybersecurity event;

(F) Whether the licensee has filed a police report or notified regulatory, governmental, or law enforcement agencies and, if so, when the notification was provided;

(G) A description of the specific types of nonpublic information or particular data elements acquired without authorization, which may include types of medical information, types of financial information, or types of information allowing for consumer identification;

(H) The period during which the licensee's 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 its best estimate of this number of consumers in its initial report to the commissioner and update this estimate with each subsequent report to the commissioner pursuant to this subsection (b);

(J) The results of an internal review and whether the review identified whether automated controls or internal procedures were followed or adhered to;

(K) A description of the efforts 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 that the licensee will take to investigate which consumers were affected by the cybersecurity event and to notify affected consumers;

(M) The name of a person who is both knowledgeable regarding the cybersecurity event and authorized to act on behalf of the licensee to serve as a representative of the licensee for contact from the commissioner; and

(N) A copy of the notice sent to affected consumers, if the notice is required under subsection (c).

(2) Licensees shall continually provide material updates or supplements to the information provided under subdivision (b)(1).

(c) Following a determination that a cybersecurity event has occurred and that the cybersecurity event has a reasonable likelihood of materially harming a consumer, a licensee shall notify consumers residing in this state whose nonpublic information has been acquired, or reasonably believed to have been acquired, by the cybersecurity event. The disclosure must be made no later than forty-five (45) days after the determination of the cybersecurity event, unless a longer period of time is required due to the legitimate needs of law enforcement. For purposes of this section, notice may be provided by:

(1) Written notice;

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001, or if the licensee's primary method of communication with the consumer has been by electronic means. Electronic means may include email notification; or

(3) Substitute notice, if the licensee demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), the affected class of subject persons to be notified exceeds five hundred thousand (500,000) persons, or the licensee does not have sufficient contact information and the notice consists of the following:

(A) Email notice, when the licensee has an email address for the consumer;

(B) Conspicuous posting of the notice on the licensee's website, if the licensee maintains a website page; and

(C) Notification to major statewide media.

(d)

(1) If a licensee becomes aware of a cybersecurity event in the licensee's information system maintained by a third-party service provider, then the licensee must treat the event as if it occurred in an information system maintained by the licensee for purposes of subsection (a).

(2) The licensee's time limitations for purposes of providing notification under subsection (a) begin running when the third-party service provider notifies the licensee of the cybersecurity event or the licensee otherwise gains actual knowledge of the cybersecurity event, whichever is sooner.

(3) This part does not limit or abrogate an agreement between a licensee and another party to fulfill the investigation requirements imposed under § 56-2-1005 or the notice requirements imposed under this section.

(e)

(1)

(A) In the case of a cybersecurity event involving nonpublic information that is used by, or in the possession, custody, or control of, a licensee acting as an assuming insurer that does not have a direct contractual relationship with the affected consumers, the assuming insurer shall notify the affected ceding insurers and the commissioner of the licensee's state of domicile within three (3) business days of determining that a cybersecurity event has occurred.

(B) The ceding insurers that have a direct contractual relationship with affected consumers must fulfill the consumer notification requirements required under this section.

(2)

(A) In the case of a cybersecurity event involving nonpublic information 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 the affected ceding insurers and the commissioner of the licensee's state of domicile within three (3) business days of the third-party service

provider notifying the licensee of the cybersecurity event or the licensee otherwise gaining actual knowledge of the cybersecurity event, whichever is sooner.

(B) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements required under this section.

(3) Except as provided in this subsection (e), a licensee acting as assuming insurer has no other notice obligations relating to a cybersecurity event under this section.

(f) In the case of a cybersecurity event involving nonpublic information in the possession, custody, or control of a licensee that is an insurer, or the 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 part, the insurer shall notify the producers of record of all affected consumers, if known, as soon as practicable, but not later than when such notice is provided to the affected consumers. The insurer is 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

Acts 2021, ch. 345, § 1.