S.C. Code Ann. § 38-99-40

This document is current through 2024 Regular Session Act No. 120, not including changes and corrections made by the Code Commissioner.

South Carolina Code of Laws Annotated by LexisNexis® > Title 38. Insurance (Chs. 1 — 101) > Chapter 99. South Carolina Insurance Data Security Act (§§ 38-99-10 — 38-99-100)

§ 38-99-40. Licensee to notify director of cybersecurity event occurence.

(A) A licensee shall notify the director no later than seventy-two hours after determining that a cybersecurity event has occurred when either of the following criteria are met:

(1) South Carolina is the licensee's state of domicile in the case of an insurer, or the licensee's home state in the case of a producer; or

(2) the licensee reasonably believes that the nonpublic information involved is of no less than two hundred and fifty consumers residing in this State, and the cybersecurity event:

(a) impacts the licensee of which notice is required to be provided to any governmental body, self-regulatory agency, or any other supervisory body pursuant to state or federal law; or

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

(B) The licensee shall provide as much of the following information as possible. The licensee shall provide the information in electronic form as directed by the director. The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the director concerning the cybersecurity event. The information sent to the director must include:

(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 agencies and, if so, when such notification was provided;

(7) a description of the specific types of information acquired without authorization, which 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 number of total consumers in this State affected by the cybersecurity event, in which case 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 pursuant to 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 which 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; and

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

(C) A licensee shall comply with the notice requirements of Section 39-1-90, and other applicable law and provide a copy of the notice sent to consumers to the director when a licensee is required to notify the director.

(D)

(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 such event as it would under subsection (A).

(2) The computation of the licensee's deadlines 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 or notice requirements imposed under this chapter.

(E)

(1)

(a) In the case of a cybersecurity event involving nonpublic information used by the licensee who is acting as an assuming insurer or in the possession, custody, or control of a licensee who 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 seventy-two hours of making the determination that a cybersecurity event has occurred.

(b) A ceding insurer that has a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under Section 39-1-90, and

other notification requirements relating to a cybersecurity event imposed under this chapter.

(2)

(a) 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 who is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the director of its state of domicile within seventy-two hours after receiving notice from its third-party service provider that a cybersecurity event has occurred.

(b) A ceding insurer that has a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements of Section 39-1-90, and other notification requirements relating to a cybersecurity event imposed under this chapter.

(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 and for which a consumer accessed the insurer's services through an independent insurance producer, the insurer shall notify the producers of record of all affected consumers as soon as practicable as directed by the director. The insurer is excused from this obligation for those instances in which it does not have the current producer of record information for an individual consumer.

History

2018 Act No. 171, § 3, effective January 1, 2019.

End of Document