N.D. Cent. Code, § 26.1-02.2-05

Current through all legislation from the 68th Legislative Assembly - Special Session (2023).

North Dakota Century Code Annotated > TITLE 26.1 Insurance (Chs. 26.1-01 — 26.1-59) > CHAPTER 26.1-02.2 Insurance Data Security (§§ 26.1-02.2-01 — 26.1-02.2-11)

26.1-02.2-05. Notification of a cybersecurity event.

1. A licensee shall notify the commissioner as promptly as possible, but no later than three business days from a determination that a cybersecurity event involving nonpublic information that is in the possession of a licensee has occurred if:

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 a producer as defined in chapter 26.1-26, and the cybersecurity event has a reasonable likelihood of materially harming a consumer residing in this state or reasonable likelihood of materially harming any material part of the normal operations of the licensee; or

b. The licensee reasonably believes the nonpublic information involved is of two hundred fifty or more consumers residing in this state and is:

(1) A cybersecurity event impacting the licensee for 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; or

(2) A cybersecurity event that has a reasonable likelihood of materially harming any consumer residing in this state or materially harming any part of the normal operations of the licensee.

2. The licensee shall provide the notice required under this section in electronic form as directed by the commissioner. The licensee shall update and supplement the initial and any subsequent notifications to the commissioner regarding material changes to previously provided information relating to the cybersecurity event. The licensee's notice required under this section must include:

a. The date of the cybersecurity event;

b. Description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any;

c. How the cybersecurity event was discovered;

d. Whether any lost, stolen, or breached information has been recovered and if so, how;

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 the notification was provided;

g. Description of the specific types of information acquired without authorization. Specific types of information means particular data elements, including medical information, financial information, or any other information allowing identification of the consumer;

h. The period during which the information system was compromised by the cybersecurity event;

i. The total number of consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the commissioner and update the estimate with a subsequent report to the commissioner 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. 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; and

m. Name of a contact person that is both familiar with the cybersecurity event and authorized to act for the licensee.

3. The licensee shall comply with chapter 51-30, as applicable, and provide a copy of the notice sent to consumers to the commissioner, when a licensee is required to notify the commissioner under subsection 1.

4. 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 in accordance with subsection 1 unless the third-party service provider provides the notice required under chapter 26.1-02.2 to the commissioner.

a. The computation of licensee's deadlines under this subsection 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.

b. Nothing in this chapter prevents or abrogates 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 26.1-02.2-04 or notice requirements imposed under subsection 1.

5. If a cybersecurity event involving nonpublic information that is used by a licensee that is acting as an assuming insurer or in the possession, custody, or control of a licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected consumers, the assuming insurer shall notify the insurer's affected ceding insurers and the commissioner of the insurer's state of domicile within three business days of making the determination that a cybersecurity event has occurred. The ceding insurer that has a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under chapter 51-30 and any other notification requirements relating to a cybersecurity event imposed under subsection 1.

6. If 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 the insurer's affected ceding insurers and the commissioner of the insurer's 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 affected consumers shall fulfill the consumer notification requirements imposed under chapter 51-30 and any other notification requirements relating to a cybersecurity event imposed under subsection 1.

7. Any licensee acting as assuming insurer does not have any other notice obligations relating to a cybersecurity event or other data breach under this section or any other law of this state.

8. If a cybersecurity event involving nonpublic information that is in the possession, custody, or control of a licensee that is an insurer or the insurer's 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 by chapter 51-30, 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 is excused from the obligation imposed under this subsection for any producers that are not authorized by law or contract to sell, solicit, or negotiate on behalf of the insurer, and those instances in which the insurer does not have the current producer of record information for an individual consumer.

History

S.L. 2021, ch. 229, § 1, effective August 1, 2021.

End of Document