507F.7 Cybersecurity event — notification and report to the commissioner.

1. A licensee shall notify the commissioner no later than three business days from the date of the licensee's confirmation of a cybersecurity event if any of the following conditions apply:

a. The licensee is an insurer who is domiciled in this state, or is a producer whose home state is this state, and any of the following apply:

(1) The laws of this state or federal law requires that notice of the cybersecurity event be given by the licensee to a government body, self-regulatory agency, or other supervisory body.

(2) The cybersecurity event has a reasonable likelihood of causing material harm to a material part of the normal business, operations, or security of the licensee.

b. The licensee reasonably believes that nonpublic information compromised by the cybersecurity event involves two hundred fifty or more consumers and either of the following apply:

(1) State or federal law requires that notice of the cybersecurity event be given by the licensee to a government body, self-regulatory agency, or other supervisory body.

(2) The cybersecurity event has a reasonable likelihood of causing material harm to a consumer, or to a material part of the normal business, operations, or security of the licensee.

2. A licensee's notification to the commissioner pursuant to subsection 1 shall provide, in the form and manner prescribed by the commissioner by rule, as much of the following information as is available to the licensee at the time of the notification:

a. The date and time of the cybersecurity event.

b. A description of how nonpublic information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of the licensee's third-party service providers, if any.

c. How the licensee discovered or became aware of the cybersecurity event.

d. If any lost, stolen, or breached nonpublic information has been recovered and if so, how the recovery occurred.

e. The identity of the source of the cybersecurity event.

f. The identity of any regulatory, governmental, or law enforcement agencies the licensee has notified, and the date and time of each notification.

g. A description of the specific types of nonpublic information that were lost, stolen, or breached.

h. The total number of consumers affected by the cybersecurity event. The licensee shall provide the best estimate of affected consumers in the licensee's initial report to the commissioner and shall update the estimate in each subsequent report to the commissioner under subsection 3.

i. The results of any internal review conducted by the licensee that identified a lapse in the licensee's automated controls or internal procedures, or that confirmed the licensee's compliance with all automated controls or internal procedures.

j. A description of the licensee's efforts to remediate the circumstances that allowed the cybersecurity event.

k. A copy of the licensee's privacy policy.

l. A statement outlining the steps the licensee is taking to identify and notify consumers affected by the cybersecurity event.

m. The contact information for the individual authorized to act on behalf of the licensee and who is also knowledgeable regarding the cybersecurity event.

3. A licensee shall have a continuing obligation to update and supplement the licensee's initial notification to the commissioner as material changes to information previously provided to the commissioner occur.

2021 Acts, ch 79, §7, 17

Referred to in §507F.8, 507F.9, 507F.11