60A.9853 NOTIFICATION OF A CYBERSECURITY EVENT.

Subdivision 1. **Notification to the commissioner.** Each licensee shall notify the commissioner of commerce or commissioner of health, whichever commissioner otherwise regulates the licensee, without unreasonable delay but in no event later than five business days from a determination that a cybersecurity event has occurred when either of the following criteria has been met:

(1) 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 those terms are defined in chapter 60K and the cybersecurity event has a reasonable likelihood of materially harming:

(i) any consumer residing in this state; or

(ii) any part of the normal operations of the licensee; or

(2) the licensee reasonably believes that the nonpublic information involved is of 250 or more consumers residing in this state and that is either of the following:

(i) 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; or

(ii) a cybersecurity event that has a reasonable likelihood of materially harming:

(A) any consumer residing in this state; or

(B) any part of the normal operations of the licensee.

Subd. 2. **Information; notification.** A licensee making the notification required under subdivision 1 shall provide the information in electronic form as directed by the commissioner. The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner concerning material changes to previously provided information relating to the cybersecurity event. The licensee shall provide as much of the following information as possible:

(1) date of the cybersecurity event;

(2) 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, government, or law enforcement agencies and, if so, when such notification was provided;

(7) description of the specific types of information acquired without authorization. Specific types of information 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. The licensee shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner 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) 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) name of a contact person who is familiar with the cybersecurity event and authorized to act for the licensee.

Subd. 3. **Notification to consumers.** (a) If a licensee is required to submit a report to the commissioner under subdivision 1, the licensee shall notify any consumer residing in Minnesota if, as a result of the cybersecurity event reported to the commissioner, the consumer's nonpublic information was or is reasonably believed to have been acquired by an unauthorized person, and there is a reasonable likelihood of material harm to the consumer as a result of the cybersecurity event. Consumer notification is not required for a cybersecurity event resulting from the good faith acquisition of nonpublic information by an employee or agent of the licensee for the purposes of the licensee's business, provided the nonpublic information is not used for a purpose other than the licensee's business or subject to further unauthorized disclosure. The notification must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system. The notification may be delayed to a date certain if the commissioner determines that providing the notice impedes a criminal investigation. The licensee shall provide a copy of the notice to the commissioner.

(b) For purposes of this subdivision, notice required under paragraph (a) must be provided by one of the following methods:

(1) written notice to the consumer's most recent address in the licensee's records;

(2) electronic notice, if the licensee's primary method of communication with the consumer is by electronic means or if the notice provided is consistent with the provisions regarding electronic records and signatures in United States Code, title 15, section 7001; or

(3) if the cost of providing notice exceeds $250,000, the affected class of consumers to be notified exceeds 500,000, or the licensee does not have sufficient contact information for the subject consumers, notice as follows:

(i) email notice when the licensee has an email address for the subject consumers;

(ii) conspicuous posting of the notice on the website page of the licensee; and

(iii) notification to major statewide media.

(c) Notwithstanding paragraph (b), a licensee that maintains its own notification procedure as part of its information security program that is consistent with the timing requirements of this subdivision is deemed to comply with the notification requirements if the licensee notifies subject consumers in accordance with its program.

(d) A waiver of the requirements under this subdivision is contrary to public policy, and is void and unenforceable.

Subd. 4. **Notice regarding cybersecurity events of third-party service providers.** (a) 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 subdivision 1 unless the third-party service provider provides the notice required under subdivision 1.

(b) The computation of a 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.

(c) Nothing in sections 60A.985 to 60A.9858 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 60A.9854 or notice requirements imposed under this section.

Subd. 5. **Notice regarding cybersecurity events of reinsurers to insurers.** (a) In the case of a cybersecurity event involving nonpublic information that is used by the 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 its affected ceding insurers and the commissioner of its state 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 subdivision 3 and any other notification requirements relating to a cybersecurity event imposed under this section.

(c) 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 that is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the commissioner of its state of domicile within three business days of receiving notice from its third-party service provider that a cybersecurity event has occurred.

(d) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under subdivision 3 and any other notification requirements relating to a cybersecurity event imposed under this section.

(e) Any licensee acting as an assuming insurer shall have no other notice obligations relating to a cybersecurity event or other data breach under this section.

Subd. 6. **Notice regarding cybersecurity events of insurers to producers of record.** (a) 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 no later than the time at which notice is provided to the affected consumers.

(b) The insurer is excused from this obligation for those instances in which it does not have the current producer of record information for any individual consumer or in those instances in which the producer of record is no longer appointed to sell, solicit, or negotiate on behalf of the insurer.

History: *1Sp2021 c 4 art 3 s 8*