Va. Code Ann. § 38.2-625

Current through 2024 Acts effective April 1, 2024

Code of Virginia 1950 > Title 38.2. Insurance. (Chs. 1 — 66) > Chapter 6. Insurance Information and Privacy Protection. (Arts. 1 — 2) > Article 2. Insurance Data Security Act. (§§ 38.2-621 — 38.2-629)

§ 38.2-625. Notice to Commissioner.

A. If a licensee has determined that a cybersecurity event has actually occurred, such licensee shall notify the Commissioner, in accordance with requirements prescribed by the Commission, as promptly as possible but in no event later than three business days from such determination if:

1. The licensee is a domestic insurance company, or in the case of a producer, the Commonwealth is the licensee's home state and the cybersecurity event meets threshold and other requirements prescribed by the Commission; or

2. The licensee reasonably believes that the nonpublic information involved is of 250 or more consumers residing in the Commonwealth or the licensee is required under federal law or the laws of another state to provide notice of the cybersecurity event to any government body, self-regulatory agency, or other supervisory body.

B. Notice provided pursuant to this section shall be in electronic form and shall include as much of the following information as possible:

1. The date of the cybersecurity event;

2. A description of how the nonpublic 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. A description of the specific types of information acquired without authorization. Specific types of information include particular data elements such as medical information, financial information, or other information allowing identification of the consumer;

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

9. The number of consumers in the Commonwealth 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. A description of efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur;

12. A copy of the licensee's consumer 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 for the licensee.

C. A licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the Commissioner concerning the cybersecurity event.

D. Each licensee shall notify consumers in compliance with § 38.2-626, and provide a copy of the notice sent to consumers under such section to the Commissioner, when a licensee is required to notify the Commissioner under this section.

E. If there is a cybersecurity event in a system maintained by a third-party service provider, the licensee, once it has become aware of such cybersecurity event, shall treat such event as it would under this section, unless the third-party service provider provides notice in accordance with this section. The computation of a licensee's deadlines shall begin on the day after the third-party service provider notifies a licensee of the cybersecurity event or the licensee otherwise has actual knowledge of the cybersecurity event, whichever is sooner.

F. If a cybersecurity event involves nonpublic information that is used by a licensee that is acting as an assuming insurer or is in the possession, control, or custody of a licensee that is acting as an assuming insurer or its third-party service provider and the licensee does not have a direct contractual relationship with the affected consumers, the licensee shall notify its affected ceding insurers and the head of its supervisory state agency of its state of domicile within three business days of making the determination or receiving notice from its third-party service provider that a cybersecurity event has occurred. Ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under § 38.2-626 and any other notification requirements relating to a cybersecurity event imposed under this section.

G. If there is 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 Commissioner. 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.

H. Nothing in this article 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 § 38.2-624 or notice requirements imposed under this section.

History

2020, c. 264.

End of Document