24-A M.R.S. § 2266

Current through Chapter 559 of the 2024 Second Regular Session and Chapter 1 of the Revisor's Report of the 131st Maine Legislature

Maine Revised Statutes Annotated by LexisNexis® > TITLE 24-A. Maine Insurance Code (Chs. 1 — 99) > CHAPTER 24-B. Maine Insurance Data Security Act (§§ 2261 — 2272)

§ 2266. Notification of cybersecurity event

(WHOLE SECTION TEXT EFFECTIVE 1/1/22 by T. 24-A, 2272)

1. Notification to superintendent. Notwithstanding Title 10, chapter 210-B, a licensee shall notify the superintendent as promptly as possible but in no event later than 3 business days from a determination that a cybersecurity event has occurred if:

A. This State is the licensee's state of domicile, in the case of an insurance carrier, or this State is the licensee's home state, as that term is defined in section 1420-A, subsection 2, in the case of an insurance producer; or

B. The licensee reasonably believes that the nonpublic information involved concerns 250 or more consumers residing in this State and that the cybersecurity event is either of the following:

(1) A cybersecurity event affecting the licensee of which notice is required to be provided to any government body, self-regulatory organization or other supervisory body pursuant to any state or federal law; or

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

(a) Any consumer residing in this State; or

(b) Any material part of the normal operation of the licensee.

2. Provision of information by licensee. A licensee shall provide in electronic form as directed by the superintendent as much of the following information regarding a cybersecurity event as possible:

A. The date of the cybersecurity event;

B. A description of how the information was exposed, lost, stolen or breached, including the specific roles and responsibilities of 3rd-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 this was done;

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 report was filed or the notification was provided;

G. A description of the specific types of information acquired without authorization. For purposes of this subsection, "specific types of information" includes, but is not limited to, medical information, financial information and information allowing identification of a consumer;

H. The period of time 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 its best estimate in the notification provided pursuant to subsection 1 to the superintendent and update this estimate with each subsequent report to the superintendent pursuant to this section;

J. The results of any review conducted by or for the licensee identifying a lapse in either automated controls or internal procedures or confirming that all automated controls or internal procedures were followed;

K. A 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. The name and contact information of a person who is familiar with the cybersecurity event and authorized to act for the licensee.

The licensee has a continuing obligation to update and supplement initial and subsequent notifications to the superintendent concerning the cybersecurity event.

3. Notification to consumers. A licensee shall comply with Title 10, chapter 210-B, as applicable, and, when required to notify the superintendent under subsection 1, provide to the superintendent a copy of the notice sent to consumers pursuant to Title 10, chapter 210-B.

4. Notice regarding cybersecurity events of 3rd-party service providers. In the case of a cybersecurity event in an information system maintained by a 3rd-party service provider of which the licensee has become aware:

A. The licensee shall respond to the cybersecurity event as described under subsection 1; and

B. The computation of the licensee's deadlines for notification under this section begins on the day after the 3rd-party service provider notifies the licensee of the cybersecurity event or the day after the licensee otherwise has actual knowledge of the cybersecurity event, whichever is sooner.

Nothing in this chapter may be construed to prevent or abrogate an agreement between a licensee and another licensee, a 3rd-party service provider or any other party to fulfill any

of the investigation requirements imposed under section 2265 or notice requirements imposed under this subsection.

5. Notice regarding cybersecurity events of reinsurers to insurers. This subsection governs notice regarding cybersecurity events of reinsurers to insurers.

A. In the case of a cybersecurity event involving nonpublic information that is used by a licensee that is acting as an assuming insurer or is 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:

(1) The assuming insurer shall notify its affected ceding insurers and the superintendent of its state of domicile within 3 business days of making the determination that a cybersecurity event has occurred; and

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

B. In the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of a 3rd-party service provider of a licensee that is acting as an assuming insurer:

(1) The assuming insurer shall notify its affected ceding insurers and the superintendent of its state of domicile within 3 business days of receiving notice from its 3rd-party service provider that a cybersecurity event has occurred; and

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

6. Notice regarding cybersecurity events of insurance carriers to producers of record. In the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of a licensee that is an insurance carrier or its 3rd-party service provider, and for which information a consumer accessed the insurance carrier's services through an independent insurance producer, the insurance carrier shall notify the producers of record of all affected consumers no later than the time consumers must be notified under subsection 3 or as directed by the superintendent, except that the insurance carrier is excused from this obligation for those instances in which it does not have the current producer of record information for any individual consumer.

History

Section History

PL 2021, c. 24, §1 (NEW)..

End of Document