RSA 420-P:6

Statutes current through Chapter 8 of the 2024 Regular Session.

LEXIS™ New Hampshire Revised Statutes Annotated > Title XXXVII Insurance (Chs. 400 — 420-Q) > Chapter 420-P Insurance Data Security Law (§§ 420-P:1 — 420-P:14)

420-P:6. Notification of a Cybersecurity Event.

I. Each licensee shall notify the commissioner within 3 business days of a determination that a cybersecurity event has occurred when either of the following criteria has been met:

(a) New Hampshire 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 RSA 402-J, 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 that the nonpublic information involves 250 or more consumers residing in New Hampshire and that the cybersecurity event:

(1) Impacts the licensee, in which case notice shall be provided to any government body, self-regulatory agency, or any other supervisory body pursuant to any state or federal law; or

(2) Has a reasonable likelihood of materially harming:

(A) Any consumer residing in this state; or

(B) Any material part of the normal operations of the licensee.

II. The licensee shall provide as much of the following information as possible. The licensee 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 regarding material changes to previously provided information relating to the cybersecurity event.

(a) 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 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 such notification was provided.

(g) 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.

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

(i) 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.

(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 which 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.

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

III. A licensee shall notify consumers by complying with RSA 359-C:20, I(a) and (c), II-IV, and VI, and providing a copy of the notice sent to consumers under that statute to the commissioner, when a licensee is required to notify the commissioner under paragraph I.

IV.

(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 paragraph I, unless the third-party service provider provides the notice required under paragraph I to the commissioner.

(b) The computation of 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 this chapter 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 RSA 420-P:5 or notice requirements imposed under RSA 420-P:6.

V.

(a)

(1) As to notice of cybersecurity events of reinsurers to insurers, 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 3 business days of making the determination that a cybersecurity event has occurred.

(2) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under RSA 359-C:20, I(a) and (c), II-IV, and VI, and any other notification requirements relating to a cybersecurity event imposed under this section.

(b)

(1) 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 3 business days of receiving notice from its third-party service provider that a cybersecurity event has occurred.

(2) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under RSA 359-C:20, I(a) and (c), II-IV, and VI, and any other notification requirements relating to a cybersecurity event imposed under this section.

(c) Any licensee acting as assuming insurer shall have no other notice obligations relating to a cybersecurity event or other data breach under this section or any other law of this state.

VI. As to notice of cybersecurity events from insurers 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 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.

History

2019, 309:1, effective January 1, 2020.