

HRS § 431:3B-302

This document is current through Act 2 of the 2024 Legislative Session. Subject to changes by Revisor pursuant to HRS 23G-15.

Michie's™ Hawaii Revised Statutes Annotated > Division 2. Business (Titles 22 — 27) > Title 24 Insurance (Chs. 431 — 435H) > Chapter 431 Insurance Code (Arts. 1 — 31) > Article 3B Insurance Data Security Law (Pts. I — III) > Part III. Cybersecurity Events (§§ 431:3B-301 — 431:3B-306)

[§ 431:3B-302.] Notification of a cybersecurity event.

(a) Each licensee shall notify the commissioner as promptly as possible, but in no event later than three business days from a determination that a cybersecurity event impacting two hundred fifty or more consumers has occurred. If law enforcement officials instruct a licensee not to distribute information regarding a cybersecurity event, the licensee shall not be required to provide notification until instructed to do so by law enforcement officials. Notification shall be provided when either of the following criteria has been met:

- (1) The licensee is domiciled in the State, in the case of an insurer, or the licensee's home state is Hawaii, in the case of an independent insurance producer; or
- (2) The licensee reasonably believes that the nonpublic information involved is of two hundred fifty or more consumers residing in the State and is a cybersecurity event that has a reasonable likelihood of materially harming:
 - (A) Any consumer residing in the State; or
 - (B) Any material part of the normal operation of the licensee.

(b) The licensee shall provide as much of the following information as possible and practicable and as promptly as possible:

- (1) The date of the cybersecurity event;
- (2) The 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 it was recovered;
- (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 the notification was provided;

- (7) A description of the specific types of information acquired without authorization. For purposes of this paragraph, “specific types of information” means particular data elements, including but not limited to 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 the State affected by the cybersecurity event. The licensee shall provide the best estimate in the initial notification to the commissioner and update this estimate with each subsequent notification 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 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) The licensee shall provide the information in electronic form as directed by the commissioner.
 - (d) 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 concerning the cybersecurity event.
 - (e) This section shall not supersede any reporting requirements in chapter 487N.

History

L 2021, c 112, § 2, effective July 1, 2021.