

215 ILCS 215/20

Statutes current with legislation through P.A. 103-585 of the 2024 Regular Session of the 103rd General Assembly.

Illinois Compiled Statutes Annotated > *Chapter 215 INSURANCE (§§ 5/1 — 215/999)* > *Insurance Data Security Law (§§ 215/1 — 215/999)*

215 ILCS 215/20 Notification of a cybersecurity event.

(a) A licensee shall notify the Director as promptly as possible but no later than 3 business days after 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 an insurance producer, as those terms are defined in Article XXXI of the Illinois Insurance Code [215 ILCS 5/500-5 et seq.], and the cybersecurity event has a reasonable likelihood of materially harming any consumer residing in this State or any material 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:

(A) 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

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

(i) any consumer residing in this State; or

(ii) any material part of the normal operations of the licensee.

(b) A licensee shall provide as much of the following information as possible:

(1) the date of the cybersecurity event;

(2) a 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 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 such notification was provided;

- (7) a description of the specific types of information acquired without authorization, including 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 Director and update this estimate with each subsequent report to the Director 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 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) the name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.

The licensee shall provide the information in electronic form as directed by the Director. The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the Director regarding material changes to previously provided information relating to the cybersecurity event.

(c) Licensees shall comply with the Personal Information Protection Act, as applicable, and provide a copy of the notice sent to consumers under that statute to the Director when a licensee is required to notify the Director under subsection (a).

(d) If a licensee becomes aware of a cybersecurity event in a system maintained by a third-party service provider, the licensee shall treat the event as it would under subsection (a) unless the third-party service provider provides the notice required under subsection (a) to the Director. 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.

(e) Nothing in this Act 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 15 or notice requirements imposed under this Section.

(f) 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 Director of its state of domicile within 3 business days after making the determination that a cybersecurity event has occurred.

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 Director of its state of domicile within 3 business days after receiving notice from its third-party service provider that a cybersecurity event has occurred.

The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under the Personal Information Protection Act and any other notification requirements relating to a cybersecurity event imposed under this Section.

(g) 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 Director. 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

2023 P.A. 103-142, § 20, effective January 1, 2024.

Illinois Compiled Statutes Annotated
Copyright © 2024 All rights reserved.