18 Del. C. § 8606

This document is current through 84 Del. Laws, c. 254.

Delaware Code Annotated > Title 18 Insurance Code (Pts. I — II) > Part II Miscellaneous (Chs. 77 — 88) > Chapter 86 Insurance Data Security Act (§§ 8601 — 8611)

§ 8606. Notification of a cybersecurity event.

(a) Notification to the Commissioner. — A licensee shall notify the Commissioner as promptly as possible but in no event later than 3 business days from the licensee's determination that a cybersecurity event has occurred if either of the following criteria has been met:

(1) The licensee is an insurer who is domiciled in this State or a producer whose home state is this State, as "home state" is defined under Chapter 17 of this title, and the cybersecurity event results in any of the following:

a. A reasonable likelihood of materially harming a consumer.

b. A reasonable likelihood of materially harming any material part of the licensee's normal operation.

c. The licensee is required to provide notice of the cybersecurity event to a government body, self-regulatory agency, or other supervisory body under state or federal law.

(2) The licensee reasonably believes that the nonpublic information involved is regarding 250 or more consumers and either of the following apply:

a. The cybersecurity event impacts a licensee that is required to provide notice to a government body, self-regulatory agency, or other supervisory body under state or federal law.

b. The cybersecurity event has a reasonable likelihood of materially harming either of the following:

1. A consumer.

2. A material part of the licensee's normal operations.

(b) Notice requirements. —

(1)

a. If notice to the Commissioner is required under subsection (a) of this section, a licensee shall provide the information in a form as directed by the Commissioner.

b. A licensee has a continuing obligation to update and supplement initial and subsequent notifications to the Commissioner regarding material changes to previously-provided information relating to a cybersecurity event.

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

a. Date of the cybersecurity event.

b. Description of how the information was exposed, lost, stolen, or breached, including the specific role and responsibility of a third-party service provider, if any.

c. How the cybersecurity event was discovered.

d. Whether any lost, stolen, or breached information has been recovered and, if so, how it was lost, stolen, or breached.

e. The identity of the source of the cybersecurity event.

f. Whether the licensee has filed a police report or notified a regulatory, government, or law-enforcement agency and, if so, when the notification was provided.

g. Description of the specific types of information acquired without authorization. For the purposes of this paragraph (b)(2)g., "specific types of information" means particular data elements, including medical information, financial information, or information allowing identification of a consumer.

h. The period during which the cybersecurity event compromised the information system.

i. The number of total consumers in this State who are affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the Commissioner and update the estimate with each subsequent report to the Commissioner under this section.

j. The results of an internal review identifying a lapse in either automated controls or internal procedures, or confirming that the 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 a consumer affected by a cybersecurity event.

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

(c) Notification to consumers. — If a licensee determines that a cybersecurity event that has a reasonable likelihood of materially harming a consumer has occurred and the event is 1 for which the licensee is required under subsection (a) of this section to notify the Commissioner, the licensee shall provide notice of the event to each affected consumer and provide a copy of the notice to the Commissioner.

(1) A licensee must provide notice under this subsection (c) of this section without unreasonable delay but no later than 60 days after determining that a cybersecurity event occurred, unless any of the following apply:

a. Federal law requires a shorter time period.

b. A law-enforcement agency determines that the notice will impede a criminal investigation and the law-enforcement agency has requested that the licensee delay notice.

Delayed notice must be made after the law-enforcement agency determines, and notifies the licensee, that notice will not compromise the criminal investigation.

c. If a licensee that is otherwise required by this section to provide notice could not, through reasonable diligence, identify within 60 days of a cybersecurity event that a customer's nonpublic information was included in the event, the licensee must provide the notice required under this section to the consumer as soon as practicable after the identification, unless the licensee provides or has provided substitute notice under § 8603(m)(4) of this title.

(2) If a cybersecurity event includes a Social Security number, a licensee shall offer to each consumer whose nonpublic information, including Social Security number, was breached or is reasonably believed to have been breached, credit monitoring services at no cost to the consumer for a period of 1 year.

a. The licensee shall provide all information necessary for the consumer to enroll in credit monitoring services and include information on how the consumer can place a credit freeze on the consumer's credit file.

b. Credit monitoring services are not required if, after an appropriate investigation, the licensee reasonably determines that the cybersecurity event is unlikely to result in harm to the consumer whose nonpublic information has been breached.

(3) If a cybersecurity event consists of a breach of email account login credentials that the licensee furnished to the consumer, including a username or email address and in combination with a password or security question and answer that permit access to an online account, the licensee may not provide notice under this section via the involved email address. The licensee must instead provide notice under this section through another method under § 8603(m) of this title or by clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an internet protocol address or online location from which the licensee knows the consumer customarily accesses the account.

(d) Notice regarding cybersecurity events of third-party service providers. —

(1) If a cybersecurity event occurs in a system that a third-party service provider maintains and of which a licensee has become aware, the licensee shall treat the event as it would under subsection (a) of this section unless the third-party service provider provides the notice to the Commissioner under this section.

(2) The computation of a licensee's deadline under this section begins on the first business 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.

(3) Nothing in this chapter prevents or abrogates an agreement between a licensee and another licensee, a third-party service provider, or another party to fulfill the investigation requirements under § 8605 of this title or notice requirements under this section.

(e) Notice regarding cybersecurity events of reinsurers to insurers. —

(1) If a cybersecurity event involves nonpublic information that is used by a licensee who is acting as an assuming insurer, or the nonpublic information is in the possession, custody, or control of a licensee who is acting as an assuming insurer and does not have a direct

contractual relationship with the affected consumer, the licensee who is acting as an assuming insurer shall notify its affected ceding insurers and the Commissioner of the licensee who is acting as an assuming insurer's state of domicile within 3 business days of determining that a cybersecurity event has occurred. A ceding insurer who has a direct contractual relationship with an affected consumer shall fulfill the consumer notification requirements under subsection (c) of this section and any other notification requirement under this section relating to a cybersecurity event.

(2) If a cybersecurity event involves nonpublic information that is in the possession, custody, or control of a third-party service provider of a licensee who is acting as an assuming insurer, the licensee who is acting as an assuming insurer shall notify the affected ceding insurer and the Commissioner of the licensee who is acting as an assuming insurer's state of domicile within 3 business days of receiving notice from the licensee who is acting as an assuming insurer's third-party service provider that a cybersecurity event has occurred. A ceding insurer that has a direct contractual relationship with an affected consumer shall fulfill the consumer notification requirements under subsection (c) of this section and any other notification requirement under this section relating to a cybersecurity event.

(f) Notice regarding cybersecurity events of insurers to producers of record. — If a cybersecurity event for which consumer notice is required under this section involves nonpublic information that is in the possession, custody, or control of a licensee who is an insurer, or a licensee's third-party service provider and for which a consumer accessed the insurer's services through an independent insurance producer, the licensee shall notify the producers of record of the consumer who was affected by the cybersecurity event in a reasonable manner and at a time reasonably concurrent with the time at which notice is provided to the affected consumer. The insurer is excused from this obligation for a producer who is not authorized by law or contract to sell, solicit, or negotiate on behalf of the insurer, and in an instance in which the insurer does not have the current producer of record information for the consumer.

History

82 Del. Laws, c. 176, § 1.