# KRS § 304.3-760

This document is current through Chapter 5 of the 2024 session.

*Michie's™ Kentucky Revised Statutes > TITLE XXV Business and Financial Institutions (Chs. 286 — 307) > CHAPTER 304 Insurance Code (§§ 304.001 — 304.99-154) > SUBTITLE 3. Authorization of Insurers and General Requirements (§§ 304.3-010 — 304.3-768) > Data Security (§§ 304.3-750 — 304.3-768)*

## 304.3-760. Notification to commissioner of cybersecurity event — Procedures.

**(1)** Each licensee shall notify the commissioner of a cybersecurity event involving nonpublic information that is in the possession of the licensee as promptly as possible, but in no event later than three (3) business days from a determination that a cybersecurity event has occurred, if:

**(a)** In the case of an insurer, this state is the licensee's state of domicile and the cybersecurity event has a reasonable likelihood of harming any material part of normal operations of the licensee;

**(b)** In the case of an insurance producer, this state is the licensee's home state, as those terms are defined in KRS 304.9-020; or

**(c)** The licensee reasonably believes that:

**1.** The nonpublic information involved in the cybersecurity event is related to two hundred fifty (250) or more consumers residing in this state; and

**2.** The cybersecurity event is either of the following:

**a.** A cybersecurity event requiring the licensee to provide notice to any governmental 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 any:

**i.** Consumer residing in this state; or

**ii.** Material part of the normal operations of the licensee.

**(2)**

**(a)** In its notification to the commissioner under subsection (1) of this section, the licensee shall provide, in an electronic form prescribed by the commissioner, the following information:

**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 the information 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, including but not limited to types of medical information, financial information, or information allowing identification of the consumer;

**8.** The period during which the information system was compromised by the cybersecurity event;

**9.** The licensee's best estimate of the number of total consumers in this state affected by the cybersecurity event, which shall be updated with each subsequent report to the commissioner pursuant to this section;

**10.** The results of any internal review:

**a.** Identifying a lapse in automated controls or internal procedures; or

**b.** Confirming that all automated controls or internal procedures were followed;

**11.** A description of the 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;

**13.** A copy of the notice sent to consumers under KRS 365.732, if applicable; and

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

**(b)** The licensee shall have a continuing obligation under subsection (1) of this section to update and supplement initial and subsequent notifications to the commissioner concerning the cybersecurity event.

**(3)** Each licensee shall comply with KRS 365.732, as applicable.

**(4)** In the case of a cybersecurity event in a system maintained by a third-party service provider of which the licensee has become aware:

**(a)** Except as provided under subsection (5) of this section, the licensee shall treat the cybersecurity event as it would under subsection (1) of this section; and

**(b)** The computation of the licensee's deadlines under this subsection shall begin on the earlier of the day after:

**1.** The third-party service provider notifies the licensee of the cybersecurity event; or

**2.** The licensee otherwise has actual knowledge of the cybersecurity event.

**(5)** Nothing in KRS 304.3-750 to 304.3-768 shall prevent or abrogate an agreement between a licensee and another licensee, a third-party service provider, or any other party to fulfill the obligations of or obligations similar to:

**(a)** Investigation requirements under KRS 304.3-758; or

**(b)** Notice requirements under this section.

**(6)**

**(a)** In the case of a cybersecurity event involving nonpublic information that is used by a licensee acting as an assuming insurer, or that is in the possession, custody, or control of a licensee that is acting as an assuming insurer, and the assuming insurer 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 three (3) business days of making the determination that a cybersecurity event has occurred.

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

**(c)** A ceding insurer under paragraph (a) or (b) of this subsection that has a direct contractual relationship with affected consumers shall fulfill:

**1.** The consumer notification requirements imposed under KRS 365.732; and

**2.** Any other notification requirements relating to a cybersecurity event under this section.

**(d)** Except as provided in paragraph (a) or (b) of this subsection, a licensee acting as an assuming insurer shall not be subject to any notice obligations relating to a cybersecurity event or other data breach under this section.

**(7)**

**(a)** Except as provided in paragraph (b) of this subsection, 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 at the same time as all affected consumers when a licensee is required to notify consumers under KRS 365.732.

**(b)** An insurer shall not be required to comply with paragraph (a) of this subsection when the insurer does not have the current producer of record information for any individual consumer.

## History

2022 ch. 149, § 6, effective January 1, 2023.



End of Document