PUBLIC PROTECTION CABINET
Kentucky Department of Insurance
500 Mero Street, 2SE11
Frankfort, KY 40601
Phone: (502) 564-3630

Andy Beshear
GOVERNOR
Jacqueline Coleman
LIEUTENANT GOVERNOR

Toll Free: (800) 595-6053

Ray A. Perry
SECRETARY
Sharon P. Clark
COMMISSIONER

ADVISORY OPINION
2023-01

The following Advisory Opinion is to advise the reader of the current position of the Kentucky Department of Insurance ("Department"), on the specified issue. The Advisory Opinion is not legally binding on either the Department or the reader.

TO: ALL LICENSEES AND PERSONS AUTHORIZED TO TRANSACT BUSINESS IN KENTUCKY

FROM: SHARON P. CLARK, COMMISSIONER
KENTUCKY DEPARTMENT OF INSURANCE

RE: INSURANCE DATA SECURITY & CYBERSECURITY REQUIREMENTS

DATE: January 3, 2023

Effective Date
This advisory opinion is effective January 3, 2023.

Purpose
This advisory opinion is intended to clarify the Commonwealth of Kentucky Department of Insurance ("Department") requirements for reporting and handling cybersecurity events, pursuant to KRS 304.3-750 to KRS 304.3-768, as enacted by the Kentucky General Assembly during the 2022 Regular Session through House Bill 474. The effective date of the new data security provisions is January 3, 2023.

Interpretation
The new data security provisions require all licensees, as defined by KRS 304.3-750(6), including all persons licensed or authorized to conduct insurance business in the Commonwealth of Kentucky who are not exempt under KRS 304.3-752, to Notify the Commissioner of the Department ("Commissioner") of cybersecurity events in accordance with KRS 304.3-760.

The Department's initial notification process will be in place beginning on January 3, 2023, until further details and guidance can be created through the promulgation of a new regulation.

All non-exempt licensees (for example, those who are not required to comply with the Health Insurance Portability and Accountability Act [HIPAA] of 1996, Pub.L. 104-191, or the Gramm-Leach-Bliley Act [GLB], Pub.L. 106-102) will also be required to:

- Establish written information security programs pursuant to KRS 304.3-756; and
- Conduct cybersecurity event investigations pursuant to KRS 304.3-758.

Beginning on January 3, 2023, no later than three (3) business days from a determination that a cybersecurity event has occurred, all licensees who are not exempt under KRS 304.3-752 shall provide written notice to the Commissioner via the following e-mail address: DOI.CommissionerOffice@ky.gov. The notice shall include all the following required information, pursuant to KRS 304.3-760:

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 (if known);
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 KRS 304.3-760;
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.

In addition, the notice should state:

- The licensee's name and DOI or NAIC number;
- The licensee's best estimate of the total consumers affected globally and nationally, in addition to those reported within Kentucky;
- The anticipated materiality of the harm to affected consumers;
- Any expected harm to a material part of the licensee's operations; and
- Whether the licensee is also required to report the event to any governmental body, self-regulatory agency, or other supervisory body outside of the Department, pursuant to state or federal law.

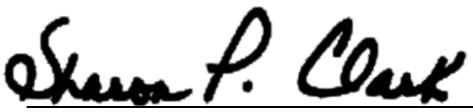
Licensees are under a continuing obligation to update and supplement the initial and any subsequent notices to the Commissioner on an ongoing basis throughout the investigation of a cybersecurity event. KRS 304.3-760(2)(b).

Licensees who are exempt under HIPPA and GLB are required to notify the Commissioner via the following e-mail address: DOI.CommissionerOffice@ky.gov, no later than three (3) business days from a determination that a cybersecurity event has occurred, in accordance with the reporting procedures set forth in the relevant federal law exempting them from the information security program requirement in KRS 304.3-756, beginning on January 1, 2023.

All licensees should prepare for annual compliance certifications, which shall be submitted to the Commissioner next year, as required by KRS 304.3-756 and KRS 304.3-766, by February 15, 2024, via the following e-mail address: DOI.CommissionerOffice@ky.gov.

Licensees and registered entities are charged with notifying their agents and employees of the Department's notification process and all programs established in accordance with the new data security provisions in KRS 304.3-750 to KRS 304.3-768. The Department does not provide legal advice to insurers or entities. The information provided herein has been offered for the sole purpose of clarifying the Department's regulatory authority pursuant to KRS 304.2-100 and KRS 304.3-762.

Questions regarding this advisory opinion should be directed to the Commissioner's Office, Phone: (502) 564-6026; TTY: (800) 648-6056; Fax: (502) 564-1453; or Email: DOI.CommissionerOffice@ky.gov.



Sharon P. Clark, Commissioner
Kentucky Department of Insurance
On this 3rd day of January 2023