LARRY HOGAN
Governor

BOYD K. RUTHERFORD
Lt. Governor

KATHLEEN A. BIRRANE
Commissioner

GREGORY M. DERWART
Deputy Commissioner

Maryland
INSURANCE ADMINISTRATION

200 Saint Paul Place, Suite 2700, Baltimore, Maryland 21202
Direct Dial: 410-468-2471 Fax: 410-468-2020
1-800-492-6116 TTY: 1-800-735-2258
www.insurance.maryland.gov

Bulletin 22-13

Date: September 30, 2022

To: All Insurers, Health Maintenance Organizations, Dental Plan Organizations, Nonprofit Health Service Plans, Managed Care Organizations, and Third Party Administrators

Re: Chapter 231 of the Laws of 2022 (SB207) (Effective 10/1/2022)
Reporting Cybersecurity Events to the Maryland Insurance Administration

---

Chapter 231 of the Laws of 2022, (SB 207) adds Title 33 to the Insurance Article, Maryland Code Annotated.[1] Title 33 requires Carriers (as that term is defined below) to, among other things, establish and maintain an information security program that meets certain standards and to notify the Maryland Insurance Administration ("MIA") of certain Cybersecurity Events, as defined and described below.[2]

SB 207 becomes effective on October 1, 2022. The date by which Carriers must implement specific requirements of Title 33 differs by requirement and, in some instances, by category of Carrier. **However, the Cybersecurity Event notification requirements set forth in § 33-105 are effective on October 1, 2022.** The purpose of this Bulletin is to remind Carriers of this obligation and to provide Carriers with instructions as to how to provide the required notice.[3]

Definition of Carrier

SB 207 applies to a ""Carrier," which is broadly defined by § 33-101(c) as follows:

(c)(1) "Carrier" means:

---

[1] Unless otherwise stated, all citations in this Bulletin are to the Insurance Article.
[2] Prior to the enactment of Title 33, §4-406 of the Insurance Article required a carrier to notify the Commissioner of a security breach. Effective October 1, 2022, this section is repealed and replace with the notice requirements set forth in newly enacted §33-105.
[3] It is important to note that SB 207 does not change the requirements of Title 14 of the Commercial Law Article regarding notifications required thereunder in the event of security breach subject to that section.

(i) an authorized insurer;
(ii) a nonprofit health service plan;
(iii) a health maintenance organization;
(iv) a dental organization;
(v) a managed general agent; or
(vi) a third–party administrator.

(2) "Carrier" does not include:

(i) a purchasing group or a risk retention group chartered and licensed in a state other than this State; or
(ii) a person that is acting as an assuming insurer that is domiciled in another state or jurisdiction.

Initial Notice Requirements

Section 33-105 of the Insurance Article requires Carriers to notify the Commissioner of a ""Cybersecurity Event," which is defined by § 33-101(e) as follows:

(e) (1) "Cybersecurity Event" means an event resulting in unauthorized access to, or disruption or misuse of, an information system or nonpublic information stored on an information system.

(2) "Cybersecurity Event" does not include:

(i) the unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization; or

(ii) an event with regard to which the carrier has reasonably determined that the nonpublic information accessed by an unauthorized person has not been and will not be used or released and has been returned or destroyed.

Carriers are not required to notify the MIA of every Cybersecurity Event. Notice is required if:

(1) (i) the State is the carrier's state of domicile; and
(ii) the cybersecurity event has a reasonable likelihood of harming a consumer residing in the state or any material part of the normal operations of the carrier; or

(2) the carrier reasonably believes that the nonpublic information involved is of 250 or more consumers residing in the state and either of the following circumstances is present:

(i) a cybersecurity event impacting the carrier has occurred for which notice must be provided to a government body, self–regulatory agency, or any other supervisory body under state or federal law; or
(ii) a cybersecurity event has occurred that has a reasonable likelihood of materially harming:
(1) a consumer residing in the state; or
(2) a material part of the normal operation of the carrier

Md. Code Ann. Ins. Art.§ 33-105(a)(1) and (2).

When required, notice must be given as promptly as possible, but in no event more than **three business days** from the date on which there has been a determination by the Carrier that a Cybersecurity Event has occurred. The content of the initial notice is set forth in § 33-105(b).

Form and Method of Initial Notice

In accordance with § 33-105(c), the Commissioner requires that the initial notice of a qualifying Cybersecurity Event required by § 33-105(a) be given electronically using the Cybersecurity Event Initial Reporting Form that may be accessed here: https://marylandinsurance.jotform.com/222405158165048. A direct link to the Initial Notice Form is also available on the MIA's website.

The Initial Notice Form includes a mandatory section for identification of the Carrier, the Carrier's contact for this Event, and the information relied on by the Carrier in determining that the Cybersecurity Event triggered the notice requirement. The remainder of the Initial Notice Form addresses each item of information described in § 33-105(b). Carriers are required to provide as much information as is reasonably possible as to each item of information.

Carriers will receive immediate confirmation of the MIA's receipt of the submission. That confirmation will be followed by an e-mail from the MIA providing an MIA Reference Number and a link to the Cybersecurity Event Supplemental Reporting Form to be used by the Carrier to provide the updates required by § 33-105(d), including submission to the Commissioner of any notice required by § 14-3504 of the Commercial Law Article.

Form and Method of Supplemental Notice

Providing initial notification is not sufficient to comply with § 33-105 of the Insurance Article. Pursuant to § 33-105(c), a Carrier has a **continuing obligation to update and supplement the initial notification to the Commissioner** concerning the Cybersecurity Event. This is an affirmative and proactive obligation of the Carrier and is not dependent on requests by the MIA for additional information. Updated and supplemental information must be submitted in real time, as soon as reasonably possible after it becomes available, with respect to each of the categories of information and each area of inquiry set forth in the Cybersecurity Event Initial Notice Form.

All updates and supplemental information must use the MIA's reference number for that Cybersecurity Event and must be submitted on the Cybersecurity Event Supplemental Reporting Form.

Managed Care Organizations

Effective October 1, 2022, managed care organizations (MCO) are subject to § 33-105(f). This section provides that **if** a MCO conducts an investigation as required by the Maryland Department of Health pursuant to its contract with the MCO and determines that a Cybersecurity Event has occurred, the MCO must provide the Commissioner with copies of all notices and reports provided to the Maryland Department of Health at the same time and in the same manner that the MCO provides the notices and reports to the Maryland Department of Health. MCO's are not otherwise subject to the provisions of § 33-105.

Any questions about this Bulletin may be directed to Dawna Kokosinski in the Market Regulation and Professional Licensing Division at 410-468-2322 or dawna.kokosinski@maryland.gov.

KATHLEEN A. BIRRANE
Commissioner

By: SIGNATURE ON ORIGINAL

Mary M. Kwei
Associate Commissioner
Market Regulation and Professional Licensing