BRIAN E. FROSH
Attorney General

ELIZABETH F. HARRIS
Chief Deputy Attorney General

CAROLYN QUATTROCKI
Deputy Attorney General

WILLIAM D. GRUHN
Chief
Consumer Protection Division

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

January 17, 2022

TO: The Honorable Delores G. Kelley, Chair
Finance Committee

FROM: Hanna Abrams, Assistant Attorney General

RE: Senate Bill 207 – Insurance Carriers – Cybersecurity Standards – SUPPORT WITH AMENDMENTS

The Consumer Protection Division of the Office of the Attorney General supports Senate Bill 207 ("SB 207") with the amendments discussed below. SB 207 establishes cybersecurity standards for insurance carriers, which the Division agrees is critical. However, based on the Division's experience investigating cybersecurity breaches, we believe the two amendments discussed below are essential.

First, for the purpose of clarity, SB 207 should reinstate the requirement that insurers comply with federal law and the Maryland Personal Information Protection Act (Md. Com. Law §14-3501 *et seq*.) currently set forth in § 4-406:

> **Compliance with this section does not relieve a carrier from a duty to comply with any other requirements of federal law or Title 14 of the Commercial Law Article relating to the protection and privacy of personal information.**

The compliance requirement is implicit in the cross references contained in § 33-105, but the Division strongly believes the requirement should be incorporated explicitly in SB 207.

Second, the definition of a "cybersecurity event" includes exclusions in § 33-101(E)(2). This exclusion must contemplate potential misuse in the future. In addition, in recent ransomware attacks, companies pay the attacker in exchange for access to their systems and the promise that the information will be destroyed after payment is received. This promise is nothing more than the word of a thief that has already breached their system and held information hostage. The Consumer Protection Division urges the committee to add language providing an objective standard for a determination that the information has been destroyed or returned. To that end, we propose the following additional language to § 33-101(E)(2)(II) (bolded language added):

"CYBERSECURITY EVENT" DOES NOT INCLUDE: . . .

(II) AN EVENT WITH REGARD TO WHICH THE CARRIER HAS DETERMINED **with reasonably high degree of certainty** 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.

The Consumer Protection Division urges a favorable report with amendments discussed.

Cc: Members, Finance Committee
Kathleen Birrane, Insurance Commissioner