LARRY HOGAN
Governor

BOYD K. RUTHERFORD
Lt. Governor

KATHLEEN A. BIRRANE
Commissioner

GREGORY M. DERWART
Deputy Commissioner

Maryland
INSURANCE ADMINISTRATION

200 St. Paul Place, Suite 2700, Baltimore, Maryland 21202
Direct Dial: 410-468-2471 Fax: 410-468-2020
Email: kathleen.birrane@maryland.gov
www.insurance.maryland.gov

TESTIMONY OF
THE
MARYLAND INSURANCE ADMINISTRATION
BEFORE THE
SENATE FINANCE COMMITTEE

JANUARY 19, 2022

SENATE BILL 207 – INSURANCE CARRIERS - CYBERSECURITY STANDARDS

POSITION: SUPPORT

Thank you for the opportunity to provide written comments regarding Senate Bill (SB) 207.

SB 207 is a departmental bill that establishes data security and incident response requirements for segments of the insurance industry, including insurance companies. While the Insurance Article, Annotated Code of Maryland, currently addresses data privacy, there are no specific regulatory requirements related to data security or the establishment of a data security program within an insurer. Likewise, legislation passed in 2019 requires certain licensees of the Maryland Insurance Administration (MIA) Commissioner to notify the Commissioner of a data security breach at the same time and in the same manner the licensee is required to provide a breach notice to the Office of the Attorney General (OAG), there are no comprehensive regulatory requirements specific to the insurance industry related to incident response plans or notice to the Commissioner. The MIA believes that these are significant gaps in regulatory oversight and in protection for Maryland residents, as well as for the industry itself. SB 207 will fill these gaps by establishing reasonable, proportionate requirements for data security and incident response programs and for regulatory notice.

SB 207 adopts key provisions of the National Association of Insurance Commissioners' (NAIC) Model Act #668 - Insurance Data Security Law (the Model), which was adopted by the NAIC in 2017. The Model was developed in response to several major data breaches involving large insurers that exposed and compromised the sensitive personal information of millions of insurance consumers. The Model requires carriers licensed by a department of insurance to

develop, implement, and maintain an information security program, investigate any cybersecurity events, and notify the state insurance commissioner of such events. As of this writing, 18 jurisdictions, including the neighboring states of Delaware and Virginia, have adopted the Model. Facilitating adoption of the Model is a strategic priority for the NAIC to ensure and formalize insurance data security protections in a reasonably uniform manner across U.S. insuring jurisdictions and to avoid risking federal preemption of state laws in this area if states fail to act.

SB 207 requires insurers and certain other licensees of the Commissioner to develop, implement, and maintain an information security program based on its risk assessment, with a designated employee in charge of the information security program. Requirements for compliance with the information security program and oversight of third-party service providers are phased in over time. Covered licensees determine the appropriate security measures to implement based on their own ongoing risk assessment for internal and external threats. If a cybersecurity event occurs, a covered licensee is required to investigate the cybersecurity event and notify the Commissioner of a cybersecurity event. SB 207 also grants the Commissioner the power to examine and investigate covered licensees to determine compliance with the law and to require that deficiencies be remedied.

For context, insurance is a 1.28 trillion dollar industry in the U.S. and a 41 billion dollar industry in Maryland, with approximately 1,600 licensed insurers conducting business in the state. Nearly every resident provides some level of personally identifiable information to an insurer, including protected health and financial information, either directly or through claims. Hackers are aware of this and the profitable opportunity for disruption it engenders. Consequently, insurers are frequent targets of hacking, phishing schemes, and ransomware.

As noted above, under legislation passed in 2019, carriers are required to notify the MIA of a security system breach at the same time that the carrier is required to notify the OAG under the Commercial Law Act. The circumstances in which a business must provide notice to the OAG are narrowly defined and not tailored to the insurance industry. However, even under those very narrow circumstances, since the law went into effect on October 1, 2019, there has been a significant increase in the frequency and severity of confidential data breaches as to which notice has been given.

Date Range	Number of Breaches	Total Impacted MD Residents	Number of Residents Impacted in a **single** breach
10/1/2019 - 12/31/2019 (3 months)	7	783	517
1/1/2020 - 12/31/2020 (12 months)	31	18,454	9,753
1/1/2021 - 8/8/2021 (8 months)	52	38,535	15,556

This limited data demonstrates the need to ensure that carriers have data security systems in place, are actively assessing and acting to mitigate their data security risk, have incident response plans in place, and keep the Commissioner informed of cyber incidents.

The standards and reporting requirements reflected in the Model and incorporated into SB 207 are consistent with current business standards and practices for the industry and its vendors. The Model was developed iteratively over the course of 2 years with extensive input from the insurance industry, other state insurance regulators and consumer representatives. Given that, it reflects a reasoned effort to assure reasonable and coherent regulatory uniformity of standards across states and reporting platforms. In addition, the existence and depth of carriers' cybersecurity protection programs are already evaluated by credit rating agencies and cybersecurity risk analysis and are part of each carrier's triennial financial examination and other risk reporting requirements.

Requiring an insurer to have a written data security and incident response reporting program is also consistent with other types of operational risk program standards imposed by the Insurance Article. For example, carriers are required to maintain disaster recovery and business interruption plans that meet certain standards.

While based on the Model, SB 207 takes an incremental approach to addressing data security in the Maryland insurance market. While the Model imposes requirements on essentially all licensees, including producers, SB 207 is limited to risk-bearing entities and the health claim administrators for those entities. In addition, while most large national and regional insurers have programs in place that meet and far exceed the standards in the Model, this legislation considers the needs of smaller, regional insurers in that it phases in requirements for compliance with the information security program and oversight of third-party service provider obligations set forth in the Model.

Adopting SB 207 is necessary to protect the integrity of consumer and insurer data against security breaches and to assure that the Commissioner has the tools needed to enforce protection standards and to mitigate the potential damage of a carrier's data breach. Therefore, the MIA respectfully requests a favorable report on SB 207.