Department of Legislative Services

Maryland General Assembly
2022 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

Senate Bill 207 (Chair, Finance Committee)(By Request - Departmental - Maryland Insurance Administration) and Senator Hester

Finance — Health and Government Operations and Economic Matters

Insurance Carriers and Managed Care Organizations - Cybersecurity Standards

This departmental bill adopts the National Association of Insurance Commissioners (NAIC) Model 668 – Data Security Model Law, which establishes data security standards for insurance regulators, insurers, and other specified carriers. Provisions of the bill are severable. The purpose of the bill is to establish standards applicable to carriers for data security, prompt investigation, and notification to the Insurance Commissioner of a cybersecurity event. Compliance with the bill does not relieve a carrier from a duty to comply with any other requirements of federal law or applicable State law relating to the protection and privacy of personal information. Each carrier has until (1) October 1, 2023, to implement most cybersecurity requirements, processes, and procedures and (2) October 1, 2024, to implement cybersecurity requirements for third-party service providers used by carriers. However, a carrier that has fewer than 25 employees and has revenues, assets, and written premiums below specified thresholds may defer the implementation dates required by the bill by one year.

Fiscal Summary

State Effect: The bill's requirements can be handled using existing budgeted resources, as discussed below. The bill's penalty provisions are not expected to materially affect State finances or operations.

Local Effect: The bill does not directly affect local government operations or finances.

Small Business Effect: The Maryland Insurance Administration (MIA) has determined that this bill has minimal or no impact on small business (attached). The Department of Legislative Services concurs with this assessment. (The attached assessment does not reflect amendments to the bill.)

Analysis

Bill Summary: The bill's requirements apply to "carriers" regulated by MIA. "Carrier" means an authorized insurer, a nonprofit health service plan, a health maintenance organization, a dental organization, a managed general agent, and a third-party administrator. "Carrier" does not include a purchasing group or a risk retention group chartered and licensed in a state other than this State or a person that is acting as an assuming insurer that is domiciled in another state or jurisdiction. A "cybersecurity event" covered by the bill is defined as an event resulting in unauthorized access to, or disruption or misuse of, an information system or nonpublic information stored on an information system. Broadly, the bill:

- establishes definitions, including what constitutes an information system that must be secured by the carrier;
- repeals existing requirements related to a carrier's protection of consumer personal data and information;
- establishes new cybersecurity and data protection requirements, processes, and procedures that must be followed by each carrier, including (1) completion of a risk assessment to assess and address potential vulnerabilities; (2) development and implementation of a written security program based on the risk assessment; (3) a requirement that third-party service providers implement specified cybersecurity measures; and (4) development and implementation of a written incident response plan to respond to and recover from cybersecurity events;
- requires a carrier to certify in writing to the Insurance Commissioner by April 15 of each year that it is in compliance with the bill's requirements, but exempts specified carriers not domiciled in the State from this requirement;
- requires a carrier to conduct a prompt investigation that includes specified processes and inquiries when the carrier learns that a cybersecurity event has or may have occurred;
- requires a carrier to notify the Insurance Commissioner and provide specified information as promptly as possible (and within three business days) when a cybersecurity event has occurred and other criteria have been met;
- establishes privacy and data sharing rules and processes for information that is provided to the Commissioner by a carrier when a cybersecurity event occurs;
- establishes that a carrier that is subject to, governed by, and compliant with the privacy, security, and breach notification rules from specified health-related federal agencies and laws must be deemed to be in compliance with the bill's requirements and the related requirements of existing State law, but must still notify the Commissioner when a cybersecurity event has occurred, as specified;
- requires a carrier to maintain specified records related to its cybersecurity plans, processes, and events for at least five years;

- establishes a penalty of no less than $100 but no more than $125,000 for each violation of the bill's requirements; and
- authorizes the Commissioner to adopt regulations to implement the bill.

The bill may not be construed to create or imply a private cause of action for a violation of its provisions or curtail a private cause of action that would otherwise exist in absence of the bill.

In addition, if a managed care organization (MCO) conducts an investigation as required by the Maryland Department of Health (MDH) in accordance with the MCO's contract with MDH and determines that a cybersecurity event has occurred, the MCO must provide to the Commissioner copies of all notices and reports provided to MDH at the same time and in the same manner that the MCO provides the notices and reports to MDH.

The bill expresses legislative intent that the Maryland Insurance Commissioner be added as a member to any Executive Branch council related to cybersecurity.

Current Law/Background: The Maryland Personal Information Protection Act generally requires businesses (including carriers affected by the bill) to protect their customers' and employees' personal information by implementing and maintaining reasonable security procedures and practices that are appropriate to the nature of the personal information. A business must investigate any breach of its security systems and report specified information to the Attorney General and to individuals whose personal information may have been accessed. A carrier that experiences a breach must also notify the Insurance Commissioner of the breach if an investigation is conducted and determines that breach of security creates a likelihood that personal information has been or will be misused.

MIA advises that the NAIC Model 668 – Data Security Model Law being adopted by the bill establishes data security standards for regulators and carriers in order to mitigate the potential damage of a data breach and that the model establishes a coherent and comprehensive approach for state uniformity. To date, 11 states have adopted the model, including Delaware and Virginia. As such, carriers in this region are likely to have already begun implementing the requirements of the model legislation.

Moreover, MIA advises that NAIC and the U.S. Treasury Department have been strongly recommending that states promptly adopt the model and plan to recommend that the U.S. Congress pass legislation to establish uniform requirements for insurer data security. MIA seeks to avoid potential federal preemptive action if such a law is passed by Congress.

For more information on cybersecurity issues in the State and across the nation, please see the **Appendix – Cybersecurity.**

Additional Information

Prior Introductions: None.

Designated Cross File: None.

Information Source(s): Department of Information Technology; Office of the Attorney General; Maryland Department of Health; Maryland Health Benefit Exchange; Maryland Insurance Administration; Department of Legislative Services

Fiscal Note History: First Reader - January 18, 2022
fnu2/mcr Third Reader - March 31, 2022
Revised - Amendment(s) - March 31, 2022

Analysis by: Richard L. Duncan

Direct Inquiries to:
(410) 946-5510
(301) 970-5510

Appendix – Cybersecurity

Cybersecurity Issues in the Nation and State

In recent years, cybersecurity and privacy issues have received significant attention from the general public and policymakers as a result of the many ransomware attacks, data breaches, and other cyberattacks that have taken place in the nation and the State. Globally, from 2019 through 2021, the Center for Strategic and International Studies identified over 300 cyberattacks and data breaches (many of which involved the United States) involving (1) government agencies; (2) defense and high-tech companies; or (3) economic crimes with losses of more than $1 million.

Maryland governmental entities have often been the victim of significant cyberattacks in recent years. For example:

- in 2019, (1) Baltimore City government's computer systems were infected with ransomware that made the systems inaccessible and unavailable for weeks and (2) the Maryland Department of Labor's licensing database was breached; the personal identifiable information (PII) of as many as 78,000 licensees may have been accessed by the hackers;
- in November 2020, Baltimore County Public Schools' information technology (IT) systems were made unusable by a ransomware attack; and
- in 2021, (1) multiple southern Maryland towns lost computer access after a third-party vendor was the victim of a ransomware attack and (2) the Maryland Department of Health was the victim of a cyberattack, resulting in the delay of pandemic data and other information.

Additionally, in November 2021, the Virginia Legislature was the victim of a ransomware attack.

Cybersecurity Governance – Generally

In June 2019, the Governor signed Executive Order 01.01.2019.07, which creates the Maryland Cyber Defense Initiative to strengthen the State's ability to manage the effects of a cybersecurity incident. The initiative creates the Office for Security Management within the Department of Information Technology (DoIT) and charges the office with responsibility for the direction, coordination, and implementation of an overall cybersecurity strategy for all Executive Branch IT systems. The office is led by the State chief information security officer (SCISO), who is appointed by the Governor. The order

also established the Maryland Cybersecurity Coordinating Council to assist SCISO and the office in their duties.

In that same month, DoIT released the State of Maryland Information Technology Security Manual. The manual currently serves as the primary policy for establishing and defining the State's IT security practices and requirements; all State agencies are required to adhere to the manual.

Recent State Action

During the 2021 legislative session, multiple pieces of legislation were enacted to enhance State cybersecurity and resilience.

- Chapter 218 of 2021 requires the Secretary of Information Technology to consult with the Attorney General to oversee a consistent cybersecurity strategy specifically for the Executive Branch.
- Chapter 683 of 2021 establishes the Center for Cybersecurity at the University of Maryland Baltimore County in order to provide research and support for cybersecurity-related activities.
- Chapter 425 of 2021 expands the list of network-related prohibited acts on a broad array of computer networks in the State. Chapter 425 also prohibits a person from performing acts to impair network functioning, including exceeding authorized network access and distributing valid access codes to unauthorized persons, on public school or health care facility networks.

In July 2021, the Governor announced several new cybersecurity measures that his office will be undertaking, including (1) a new partnership with the National Security Agency; (2) a memorandum of understanding with the University of Maryland Baltimore County to establish the Maryland Institute of Innovative Computing; and (3) an executive order creating a statewide privacy framework to govern the manner in which the State secures the PII of its citizens.

Maryland Cybersecurity Council Study

The Maryland Cybersecurity Council is required to work with the National Institute of Standards and Technology, as well as other federal agencies, private-sector businesses, and private cybersecurity experts to address State cybersecurity issues. Over the 2021 interim, a council workgroup conducted a review and study of the State's cybersecurity governance and resilience. Through the study, the workgroup developed numerous recommendations for the State to improve and enhance its system. The recommendations include codifying the aforementioned executive order that established the Maryland Cyber Defense Initiative

and centralizing State cybersecurity and IT governance within DoIT. The workgroup's final report is expected to be released during the 2022 legislative session.

Cybersecurity Legislation in Other States

The National Conference of State Legislatures advises that 45 states, the District of Columbia, and Puerto Rico introduced or considered over 250 bills or resolutions that dealt significantly with cybersecurity in 2021. Some of the key cybersecurity issues considered included:

- requiring government agencies to implement training or specific types of security policies and practices and improving incident response and preparedness;
- increasing penalties for computer crime or addressing specific crimes, *e.g.*, ransomware;
- regulating cybersecurity within the insurance industry or addressing cybersecurity insurance;
- creating task forces, councils, or commissions to study or advise on cybersecurity issues; and
- supporting programs or incentives for cybersecurity training and education.

Federal Action

On October 8, 2021, President Joseph R. Biden, Jr., signed the K-12 Cybersecurity Act into law in response to cybersecurity attacks directed at schools. Narrow in scope, the law directs the federal Cybersecurity and Infrastructure Security Agency (CISA) to examine cybersecurity-related risks exclusive to K-12 educational settings. The Director of Cybersecurity and Infrastructure Security must conduct a study and make recommendations specific to K-12 related cybersecurity risks.

Additionally, the Infrastructure Investment and Jobs Act was signed into law on November 15, 2021. Related to cybersecurity, the act established a cyber grant program within the Federal Emergency Management Agency that must be managed in consultation with CISA. Through the program, $1 billion will be distributed to state and local governments over four years; however, to receive a grant, states must submit a cybersecurity plan to the Department of Homeland Security, establish a planning committee before grants are received, and match a portion of the funding provided over the grant program. Grant funding may not be used for ransomware attack payments, to supplant other funding, or for any noncyber purpose.

ANALYSIS OF ECONOMIC IMPACT ON SMALL BUSINESSES

TITLE OF BILL: Insurance Carriers and Managed Care Organizations - Cybersecurity Standards

BILL NUMBER: SB 207

PREPARED BY: Maryland Insurance Administration

PART A. ECONOMIC IMPACT RATING

This agency estimates that the proposed bill:

_X_ WILL HAVE MINIMAL OR NO ECONOMIC IMPACT ON MARYLAND SMALL BUSINESS

OR

___ WILL HAVE MEANINGFUL ECONOMIC IMPACT ON MARYLAND SMALL BUSINESSES

PART B. ECONOMIC IMPACT ANALYSIS

There is no economic impact on small businesses associated with this proposal.