SENATE APPROPRIATIONS COMMITTEE
FISCAL NOTE

BILL NO. House Bill 739

PRINTER NO. 688

AMOUNT

No Fiscal Impact

FUND

Insurance Regulation and Oversight Fund

DATE INTRODUCED

March 28, 2023

PRIME SPONSOR

Representative Boyle

DESCRIPTION

House Bill 739 amends Title 40 (Insurance) by adding a new Chapter 45 (Insurance Data Security) to require licensees to submit an annual written statement to the Insurance Department (department) certifying compliance with the risk assessment, information security program and oversight provisions of the act as well as to promptly notify the commissioner of a cybersecurity event.

Section 4512. Risk Assessment
The bill requires insurers and other entities licensed by the department to develop, implement and maintain an information security program based on its risk assessment, with a designated employee or two in charge of the program.

Section 4513. Information Security Program
The bill phases in requirements for compliance with the information security program and oversight of third-party service providers. Insurers determine the appropriate security measures to implement based on careful, ongoing risk assessment for internal and external threats.

Section 4514. Corporate Oversight
For licensees with a board of directors, the board shall require executive management to develop and implement the information security program and require annual compliance updates and a report of material matters such as risk management decisions and cybersecurity events.

Section 4515. Oversight of Third-party service provider arrangements
A licensee shall require third-party service providers to implement measures to protect and secure information systems and nonpublic information.

Section 4516. Certification
No later than the April 15 that is at least one year after the effective date of this section and each April 15 thereafter, each insurer domiciled in this Commonwealth shall submit to the commissioner a written statement certifying that the insurer is in compliance with the risk assessment, information security program, corporate oversight provisions and oversight of third-party service provider arrangements.

Each insurer shall maintain all records supporting the certification for a period of five years and make such records available for department examination. If an insurer has identified systems or processes that require material improvement or updating, the insurer shall document the remedial efforts.

Section 4517. Investigation of Cybersecurity Event

If a licensee discovers a cybersecurity event has or may have occurred, it shall conduct a prompt investigation to assess the nature and scope of the event and oversee reasonable measures to restore the security of the information systems compromised to prevent further unauthorized use. A licensee shall confirm the same steps are completed for a cybersecurity event involving a system maintained by a third-party service provider. A licensee shall maintain records of all cybersecurity events for at least five years and produce them to the commissioner upon demand.

Section 4518. Notification of Cybersecurity Event

A licensee shall notify the commissioner as promptly as possible, but no later than five business days, from a determination that a cybersecurity event involving nonpublic information has occurred for a Pennsylvania-domiciled licensee if the event has a reasonable likelihood of materially harming a consumer residing in the Commonwealth. For non-domestic licensees, notification shall be required if the event involves nonpublic information of 250 or more consumers residing in this Commonwealth.

Notification to the commissioner shall include as much information as possible about the cybersecurity event and efforts being undertaken to remediate the situation and impose a continuing obligation on a licensee to update and supplement notifications to the commissioner. A licensee shall also submit a copy of the notice sent to consumers under the Breach of Personal Information Notification Act.

Section 4521. Power to Examine Licensees

The commissioner shall have the powers provided under the Insurance Department Act of 1921 to examine and investigate licensees to determine whether the licensee has been or is engaged in conduct in violation of this chapter. This includes timely, convenient and free access at all reasonable hours at the licensee's offices to all records.

Section 4522. Penalties

For violations of this chapter, the commissioner may impose licensee suspensions, revocations or refusals to issue or renew and or fines.

Section 4531. Confidentiality

All documents disclosed to the department during an examination or investigation under this chapter shall be privileged and given confidential treatment not subject to private civil action, subpoena or the Right-to-Know Law. The department may share documents with other regulatory agencies, the NAIC and law enforcement agencies and likewise may receive documents from these sources while maintaining confidentiality.

SENATE APPROPRIATIONS COMMITTEE
FISCAL NOTE

Section 4532. Exemptions
Licensees with fewer than 10 employees, less than $5 million in gross revenue or less than $10 million in year-end total assets shall be exempt from sections 4512 (relating to risk assessment), 4513 (relating to information security program), 4514 (relating to corporate oversight), 4515 (relating to oversight of third-party service provider arrangements) and 4516 (relating to certification).

A licensee subject to the privacy, security and breach notification rules issued by the U.S. Department of Health and Human Services and the Health Insurance Portability and Accountability Act shall be deemed to comply with this chapter except for the notification to the commissioner.

Section 4536. Initial Compliance
Licensees shall have one year from the effective date to implement sections 4512 (relating to risk assessment), 4513 (relating to information security program), 4514 (relating to corporate oversight) and 4515 (relating to oversight of third-party service provider arrangements).

House Bill 739 repeals Section 7142 (relating to small company exemption) of Chapter 71 (Reserve Liabilities) and adds a new section 7143 (adoption of exemption standards of NAIC valuation manual) so that the commissioner shall annually determine whether to adopt the standards for company exemption specified in the most recent version of the NAIC valuation manual by submitting a statement of policy in the Pennsylvania Bulletin.

The addition of 40 Pa.C.S. Chapter 45 shall take effect in 180 days, and the remainder of this act shall take effect immediately.

FISCAL IMPACT:

According to the Pennsylvania Insurance Department, enactment of this legislation will have no fiscal impact on Commonwealth funds.