OFFICE of the INSURANCE COMMISSIONER
WASHINGTON STATE

Providing Digital Consumer Protection: Concerning Insurance Data Security in the Era of Technology

Issue: Establishing data protection for insurance consumers from cybersecurity events or breaches through nationally recognized best practices including information security programs, investigation standards, and notification requirements.

Legislative proposal seeking consumer data protection from cybersecurity events involving insurers or insurance information

Insurance Commissioner Mike Kreidler is proposing legislation to increase consumer protection as it relates to insurance data and cybersecurity events. The topics of cybersecurity and consumer data protection have been top priorities for the National Association of Insurance Commissioners (NAIC) during the last five years, due in part to several major data breaches involving large insurers. These events have exposed and compromised the sensitive personal information of millions of insurance consumers.

To address consumer protection in this field, the NAIC developed the Insurance Data Security Model Law (#668). The legislation offered by the Office of the Insurance Commissioner (OIC) is substantially similar to the NAIC Model Law (#668), with provisions for proactive information technology security programs, cybersecurity investigations standards, and notification requirements.

This legislation has not only been developed with assistance from the NAIC, but has also been recommended by the U.S. Treasury Department, with a suggestion for prompt adoption by the states prior to October 2022. The U.S. Treasury Department urged prompt state adoption, explaining that if adoption and implementation of this type of legislation does not result in uniform data security regulations nationwide, then Congress must act by passing legislation setting forth uniform requirements for insurer data security.

The OIC proposes adding a new chapter to Title 48 RCW, which will be known and cited as an Act Concerning Insurance Data Security.

This Act establishes data security standards for regulators and insurers to prevent, mitigate, and respond to cybersecurity events and data breaches.

This Act will apply to insurers, insurance agents, and other insurance entities regulated by the OIC.

Sufficient security standards to prevent, mitigate, and triage cybersecurity events

The Commissioner's proposal will require insurers and other entities regulated by the OIC to develop, implement, and maintain an information security program that is based according to an appropriate risk assessment, and to designate individuals with the duty to administer the information security program. The legislation will also require insurers to follow proper protocol in investigating cybersecurity events, and when appropriate, notify the Commissioner within three business days of experiencing a cybersecurity event or data breach.

Recently data breaches have been exhibited on the state and national levels. Washington employees experienced exposure of their employment insurance information in 2020, due to a cybersecurity event at the Washington State Auditor's Office. American citizens also observed

major systems being disrupted due to IT breaches, such as the East Coast oil pipeline shutdown and ransomware attacks on government agencies. These events show the need for this type of legislation to provide consumers with data protection from similar cybersecurity events or risks.

The OIC's Legislation:

- Aligns state insurance data security standards with national best practices, established by the NAIC through coordination among state insurance regulators across the country. The coordination included two years of extensive deliberations, and thorough input from state insurance regulators, consumer representatives, and the insurance industry.
- Requires insurers and other entities regulated by the OIC to implement an information security program that is based off an appropriate risk assessment, and where appropriate, notify the Commissioner within three business days of experiencing a cybersecurity event.
- Provides that each information security program employed must establish a written incident response plan designed to promptly triage any cybersecurity event experienced by an insurer. Annually each insurer domiciled in Washington state must submit to the Commissioner, a written statement by Feb. 15 of each year, certifying the insurer is in compliance with this program.
- This Act also provides the Commissioner with power to examine and investigate the affairs of any licensee to determine whether the licensee is in compliance with this program.

Proactive consumer data protection that considers all affected parties

The legislative proposal being offered provides confidentiality and protections for any documents, materials, or other information in the control or possession of the Commissioner and processed under this Act. This will provide confidentiality and protections not only to the insurer, but also to the insurance consumer. However, the Commissioner can use these items in furtherance of any regulatory or legal action brought as a part of regular duties.

This Act allows entities regulated by the OIC sufficient time to implement adequate risk assessments, information security programs, investigation protocols, and notification procedures. The bill is anticipated to take effect on July 1, 2022, and includes a one-year buffer for licensee compliance with Section 4 requirements (information security programs).

Protecting consumer data insurance information in an increasingly technological world

Commissioner Kreidler's legislative proposal ensures consumer insurance data is protected from future cybersecurity events or data breaches through thorough information security programs, based on proper risk assessments, and with annual certification requirements, while allowing adequate time for compliance. Legislation of this nature, and substantially similar to the NAIC Insurance Data Security Model Law (# 668), has been adopted by 18 states, as of August 2021. If the Act is not passed, then Washington state risks pre-emption by federal law.