May 2019

GOVERNMENT RELATIONS
ISSUE BRIEF

700 HALL OF STATES
444 NORTH CAPITOL STREET N.W.
WASHINGTON, D.C. 20001
202-471-3990
www.naic.org

NAIC
National Association of Insurance Commissioners
& The Center for Insurance Policy and Research

Cybersecurity: Protecting Insurance Consumers in a Digital Age

- *Federal cybersecurity legislation should not disregard the existing state insurance regulatory framework nor inhibit ongoing efforts in the states to adopt data security laws and regulations in the best interests of insurance consumers.*

- *In response to the ever-evolving nature of cybersecurity risks, state insurance regulators continue to take proactive steps to upgrade safeguards to protect the security, confidentiality, and integrity of insurance customer information through standards, the examination processes, and model laws.*

- *The NAIC adopted the Insurance Data Security Model Law in 2017 to update state insurance regulatory requirements relating to data security, the investigation of a cyber event, and the notification to state insurance commissioners of cybersecurity events at regulated entities.*

Background

State insurance regulators have long been committed to addressing cybersecurity risks and to ensuring the insurers, agents, and brokers they regulate are adequately protecting the many kinds of highly sensitive consumer financial and health information they retain. All states have standards that comply with those set forth in the Gramm-Leach-Bliley Act and in recognition that the standards governing the protection of insurance consumer information must evolve to keep pace with cyber risks, the NAIC adopted the Insurance Data Security Model Law in 2017. The U.S. Treasury Department has endorsed the model and urged its prompt adoption. Further, state insurance regulators have updated and strengthened existing guidance for examiners regarding information technology systems and protocols to draw more focus to the consideration of cybersecurity during a financial exam.

Legislative proposals that preempt state laws and regulations undermine state insurance regulators' ability to establish data security requirements for their regulated insurance entities and to seek redress for policyholders following a breach. While state insurance regulators remain committed to working with federal and state regulatory counterparts as well as Congress to promote effective cyber risk management and to protect consumers' personal information, these approaches would limit individual state regulators from protecting consumers in their home state, undermine existing consumer protections, and inhibit future enhancements and innovation that are necessary for regulators and companies to adapt to evolving threats.

Key Points

- ✓ The NAIC opposes any legislative efforts that would prohibit state insurance regulators from protecting policyholders in their state. Such an approach would be fundamentally at odds with the strong existing state-based insurance regulatory regime and would erode insurance regulators' authorities to investigate or mitigate any potential harm to insurance consumers resulting from a data breach.

- ✓ Insurance commissioners have the expertise and experience with local insurance markets and are best positioned to protect a state's insurance consumers. Consumers harmed by an insurer's cyber breach should be able to rely on their own state insurance commissioner, not someone from Washington DC or another state.

Ethan Sonnichsen, Managing Director, Government Relations esonnichsen@naic.org
Mark Sagat, Assistant Director, Financial Policy and Legislation msagat@naic.org
Brooke Stringer, Senior Financial Policy and Legislative Advisor bstringer@naic.org