HINSHAW

Alerts

Maine Enacts NAIC-Inspired Cybersecurity Law

April 7, 2021
Hinshaw Privacy & Cyber Bytes

Maine has become the latest state to adopt a version of the National Association of Insurance Commissioners (NAIC) model cybersecurity law. Signed into law on March 17, 2021, the Maine Insurance Data Security Act establishes investigation procedures, data security program standards, and notification requirements for persons authorized or registered to operate pursuant to the insurance laws of Maine (licensees), with the aim of protecting the security and confidentiality of non-public information and the security of the licensee's information systems. Licensees with fewer than ten employees are exempt.

Like the NAIC model law and the New York State Department of Financial Services Cybersecurity Regulation that inspired it, the Act requires licensees to develop, implement, and maintain a written information security program to protect the licensee's systems and non-public information. These programs must be proportionate to the licensee's size and complexity and the nature and scope of the licensee's activities regarding sensitive non-public information. The program must contain administrative, technical, and physical safeguards based on the licensee's risk assessment.

The risk assessment serves to identify any foreseeable internal or external threats that could compromise sensitive non-public information and determine potential damages that could arise from said threats. The assessment must also evaluate the sufficiency of current policies and procedures to detect, prevent, and respond to cybersecurity threats and events. Based on this information, the licensee must create and implement a program that mitigates the identified risks. The risk assessment must include an evaluation of the licensee's third-party service providers.

The Act mandates oversight by the board of directors or an appropriate board committee, as well as at least annual written reports to the board concerning the overall status of the licensee's information security program, compliance with the Act, cyber events and violations, and related issues.

Compliance with the law also requires yearly reporting by April 15th of each year, certifying that the licensee is in compliance with the Act. Licensees must also maintain records of the past five years in the event the state requests to review compliance with the Act.

Service Areas

Privacy, Security & Artificial Intelligence

In the event of a cybersecurity event, certain licensees—including insurance carriers domiciled in Maine—must notify the Insurance Superintendent **within three days** of the nature of the event or if the licensee reasonably believes that the incident affects more than 250 consumers and has a reasonable likelihood of materially harming any Maine consumer or a material part of the licensee's business operations. Consumers must be notified when required by Maine's breach notification law. The Act also addresses cyber event notice requirements for producers, third-party service providers, and reinsurers. Maine's Bureau of Insurance Superintendent is responsible for establishing the rules and procedures to enforce the Act. It may commence an investigation if it learns that a cybersecurity event has or may have occurred. If the Superintendent determines there has been a violation of the Act, a corporation, or any entity other than an individual, could be subject to a fine of up to $10,000. There is no private right of action under the Act. Information provided to the Bureau in connection with the Act is considered confidential and is not subject to discovery or admissible in any private civil action. Neither the Superintendent nor any other person who receives such information may be permitted or required to testify in a private civil action concerning the information.

Licensees are required to be in compliance when the law becomes effective on January 1, 2022.