# The NAIC Insurance Data Security Model Law: Key Provisions and Adoption to Date

In the wake of numerous data breaches involving insurers, the National Association of Insurance Commissioners ("NAIC") undertook a nearly two-year evaluation of cybersecurity and consumer data protection issues, and in October 2017, adopted its Insurance Data Security Model Law (the "NAIC Model").[1] The NAIC Model generally requires insurers, agents, and other entities licensed by a state department of insurance to develop, implement, and maintain an information security program, investigate any cybersecurity events, and notify the state insurance commissioner of such events.

While all 50 states and the District of Columbia have adopted data breach notification laws,[2] prior to the NAIC Model, very few states had implemented cybersecurity standards applicable to the insurance industry, with the notable exception of New York's regulation, *Cybersecurity Requirements for Financial Services Companies*.[3] To date, eleven states have adopted the NAIC Model, as modified, including three in 2020. The adopting states are: Alabama, Connecticut, Delaware, Indiana, Louisiana, Michigan, Mississippi, New Hampshire, Ohio, South Carolina, and Virginia.[4]

In late 2017, the U.S. Treasury recommended "prompt adoption" of the NAIC Model by the states and further recommended that if adoption and implementation have not occurred within five years, Congress pass a law setting forth requirements for insurer data security, subject to state supervision.[5]

The key elements of the NAIC Model are as follows:

- Insurers and other entities licensed by a state department of insurance must develop, implement, and maintain an information security program based on its risk assessment, with a designated employee or third-party in charge of the information security program, and provide an annual certification of compliance.
- Compliance with the information security program can be phased in, especially for oversight of third-party service providers.
- Licensees must determine the appropriate security measures to implement based on careful, ongoing risk assessment for internal and external threats.
- Each cybersecurity event must be investigated, and the state insurance commissioner notified of a cybersecurity event.

*Read more on page 33*

**Salvatore Scanio**
*Ludwig & Robinson PLLC*

***Salvatore Scanio** is a Member with Ludwig & Robinson PLLC in Washington, DC. He is a graduate of Tulane University, earning B.A., J.D., and M.B.A. degrees. His practice focuses on domestic and international litigation involving banking, insurance, and other commercial disputes. He advises clients on liability, defenses, and loss recovery in cybercrime and other fraud schemes as well as on regulatory compliance, cybersecurity, privacy, data protection, and payments. Previously he was in-house counsel with a large commercial bank. Salvatore can be reached at sscanio@ludwigrobinson.com*

*NAIC... Continued from page 10*

- Insurance commissioners have the power to examine and investigate licensees to determine compliance with the law and to require resolution of data security deficiencies.
- Smaller licensees (*i.e.*, less than 10 employees), those compliant with Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and other agents are exempted.
- No private cause of action is created by the NAIC Model, nor does it limit any existing private right of action.

In adopting the NAIC Model, states have taken varying approaches with certain provisions. For example, the NAIC Model requires an insurer to notify an insurance commissioner "within 72 hours from a determination that a cybersecurity event has occurred." Alabama, however, requires notice to the commissioner no later than three business days after the determination of a cybersecurity event. In Michigan, an insurer need only notify a commissioner within 10 days of determination of a cybersecurity event. Michigan also exempts companies with less than 25 employees, exceeding the NAIC Model's exemption for 10 employees.

Finally, the NAIC Model gives licensees one year to implement their own information security program and two years to ensure oversight of third-party service providers.

Even apart from state adoption, like many other emerging norms in the cybersecurity and data privacy space, insurers and other licensees would be well advised to proactively adopt policies and procedures in conformity with the NAIC Model.

**Endnotes**

1 NAIC, Insurance Data Security Model Law (4th Quarter 2017), available at https://content.naic.org/sites/default/files/inline-files/MDL-668.pdf (last visited Dec. 14, 2020).

2 National Conference of State Legislators, Security Breach Notification Laws (July 17, 2017), available at https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Dec. 14, 2020).

3 23 NYCRR pt. 500.

4 NAIC, State Legislative Brief, The NAIC Insurance Data Security Model Law (June 2020), available at https://content.naic.org/sites/default/files/inline-files/cmte_legislative_liaison_brief_data_security_model_law_1.pdf (last visited Dec. 14, 2020).

5 U.S. Department of the Treasury, A Financial System That Creates Economic Opportunities – Asset Management and Insurance, Oct. 2017, at 117, available at https://www.treasury.gov/press-center/press-releases/Documents/A-Financial-System-That-Creates-Economic-Opportunities-Asset_Management-Insurance.pdf (last visited Dec, 14, 2020).