Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

4 Key Battles To Watch Over NAIC's Cyber Model Law

By **Jeff Sistrunk**

Law360, Los Angeles (August 30, 2016, 9:45 PM ET) -- As the insurance industry's standard-setting body plows ahead on a model law outlining how insurers must safeguard consumers' information and respond in the event of a data breach, experts say it will encounter resistance from insurers challenging the proposal's breach notification requirements and consumer groups looking for stronger policyholder protections.

The National Association of Insurance Commissioners is collecting public comments through mid-September on a revised draft of the insurance data security model law, which is designed to set exclusive standards for information security and data breach notification practices for insurance companies, agents and brokers. Since the model law was first rolled out in March, it has drawn intense criticism, with some insurance sector representatives decrying what they say are overly stringent notice requirements and consumer advocates expressing concerns that the proposal offers narrower protections for breach victims than existing state privacy laws.

While the NAIC's revisions have assuaged some of that unease, experts say heated debate will continue on the model law, which regulators are aiming to finalize by year's end.

"I think the bottom line is that the current draft contains many favorable aspects, including requiring insurers to implement a security plan, oversight of third-party providers, and notification of data breaches to consumers and insurance commissioners, but there are important unanswered questions," saidK&L Gates LLP partner Roberta Anderson, who specializes in insurance coverage and cybersecurity.

Here, Law360 breaks down some of the most hotly contested aspects of the model law.

Data Security Standards

The second draft of the model law, which was released on Aug. 17, requires insurance licensees — including insurance carriers, agents and brokers — to develop and maintain a comprehensive written information security program to safeguard consumers' personal information.

The initial draft of the proposal appeared to set a single standard for data security programs for all licensees, regardless of their size or the extent of their operations, prompting a great deal of criticism by insurance industry groups. In response, the NAIC revised the model law to establish that each licensee's data protection protocols should correspond to its size, complexity and nature of its operations, as well as the sensitivity of the personal information that it collects.

"The new draft gave insurers some relief by doing away with a single information security standard and allowing size and complexity to be taken into account," said Day Pitney LLP partner Bill Goddard.

However, despite providing licensees a greater degree of flexibility to craft their data security programs, the revised draft still doesn't go into detail about the types of measures that are required, which could prompt calls for further guidance, experts say.

"There are likely to be significant questions about what constitutes a comprehensive written information security program," Anderson said. "The model law draft says the program should be developed commensurate with the sensitivity of the information at issue, as well as the complexity and scope of the insurer's activities, but that language does not offer concrete guidance."

Indeed, Goddard said that, even after the revisions, insurers have still been left wondering about the scope of the information that they must protect, how they must notify consumers about the type of data they collect and how the requirements of the model law will be harmonized with existing privacy laws in the states.

"A lot of progress has been made, but those three questions are still haunting," Goddard said.

Third-Party Vendor Oversight

Another aspect of the model law that has been the subject of fierce debate is the extent to which insurance licensees are responsible for data breaches suffered by third-party service providers that have been entrusted with their consumers' personal information.

The initial draft mandated that licensees require third-party vendors to agree by contract to indemnify them for any losses stemming from a cybersecurity incident. That provision was met with firm resistance, with service providers expressing fears that they would have little power in negotiating contracts with larger companies.

"The third-party service provider indemnification language had caused a great deal of anxiety," Goddard said. "For example, if I'm a tiny agent, what do I do when I'm dealing with a huge company? It would be difficult to negotiate specific terms within my third-party contract. The removal of the indemnification provision alleviated some of those concerns."

The current iteration of the model law states that insurance licensees shall only enter into contracts with third-party service providers "that are capable of maintaining appropriate safeguards" to shield consumer data. However, that language raises the question of what qualifies as appropriate safeguards, so the insurance industry will continue to pursue clarity on that front, experts say.

Regulatory Notice Requirements

The revised model law requires insurance companies, agents and brokers hit by cyberattacks to notify the insurance commissioners for the states in which consumer information was compromised within three business days after determining that a data breach occurred. Under the proposal, insurance licensees must provide regulators with a litany of information, including a description of the data breach, how the breach was discovered and the type of data that was lost or stolen.

According to some experts, those requirements are unnecessarily onerous, as it can take weeks or even months for hacked companies to determine the extent of a breach with any degree of certainty.

"Almost none of the questions posed by a data breach could be answered with certainty after only three business days," said Debevoise & Plimpton LLPpartner Jim Pastore, a member of the firm's cybersecurity and data privacy practice. "What that risks is inconsistent reporting by companies, which would report and then modify their initial statements to the commissioner. I would question the value of requiring such detailed information at such an early stage."

Goddard said that perhaps the biggest blow to the insurance industry with respect to breach notification was the elimination of language in the model law establishing that a licensee's notification obligations only kick in once it determines that a cyberattack is "reasonably likely to cause substantial harm or inconvenience" to the consumers whose information was compromised.

In lieu of that "harm trigger," the model law now states that licensees are obligated to provide notice if they discover that an "unauthorized acquisition of personal information" has transpired.

"For the industry, the one big loss was the removal of the harm trigger from the notice requirements," Goddard said. "Without a harm trigger, licensees are very worried that the model law will be problematic. Now, the requirement is much less clear-cut. If you can't determine whether or not you were breached, do you have to send a notice?"

Consumer Protection Measures

Insurance consumer groups have questioned whether the NAIC's model law provides sufficient protections for policyholders. Among other things, the revised draft calls for licensees to notify consumers affected by a data breach "as expediently as possible and without unreasonable delay," no more than 60 days after a breach is discovered.

According to experts, the 60-day time frame is significantly longer than the notification windows permitted in the 47 states that have passed their own data breach notification laws.

"There is a trend for the notification period to be significantly shorter — historically, not longer than 30 days, even in a state where laws don't specify a specific time frame," Anderson said. "A requirement of 60 days is longer than would be considered acceptable under typical circumstances under most current state laws."

From a policyholder's standpoint, a requirement pushing a data holder to disclose a breach sooner rather than later is always better, absent some justification to delay disclosure, such an ongoing law enforcement investigation, said Anderson Kill PC shareholder Joshua Gold.

"I would hope the insurance commissioners would agree to require disclosure earlier in the process, rather than waiting until every forensic investigation report is signed, sealed and delivered," Gold said.

In addition, in a move that was met with praise by the insurance industry, the NAIC added language to its revised draft stating that the model law doesn't allow for any private actions by consumers who suspect that an insurance company, agent or broker has violated the law's terms. Gold said that the lack of a private cause of action to enforce the model law may limit its protection of policyholders.

"One of the concerns that policyholders have had under consumer protection provisions of the insurance code is that, if there is no private right of action, are policyholders really protected?" Gold said. "Insurance regulators may not have the time, resources or incentive to go after their licensees as often as they should."

--Editing by Katherine Rautenberg and Jill Coffey.
