March 9, 2016

NAIC Introduces New Insurance Data Security Model Law for Comment

Last week, the Cybersecurity Task Force of the National Association of Insurance Commissioners voted to subject the new "Insurance Data Security Model Law" for public comment during the brief period between now and Wednesday, March 23. The NAIC has also announced that the new model law will be discussed at the Cybersecurity Task Force's meeting during the NAIC's spring meeting in New Orleans, currently scheduled for 2:30 p.m. on Monday, April 4.

The new model act builds on four of the NAIC's previously released works, and then goes further to implement specific practices and penalties. First, the new model law incorporates elements of two prior model laws – the Insurance Information and Privacy Protection Model Act (the Privacy Protection Model Act), currently adopted in approximately one-third of the states, and the Privacy of Consumer Financial and Health Information Regulation, currently adopted in more than two-thirds of the states – both of which are currently under review for amendment. The new model law also builds on the NAIC's previously announced Principles for Effective Cybersecurity: Insurance Regulatory Guidance and the NAIC Roadmap for Cybersecurity Consumer Protections (fka the Cybersecurity Bill of Rights). The new model law is not circumscribed by these prior pronouncements; rather, it addresses specific practices and has a wider scope than earlier models.

Types of information: The scope of the new model law reaches many types of personal information, including "information that the consumer provides...to obtain an insurance product," "information about the consumer resulting from a transaction involving an insurance product or service," or information obtained "in connection with providing an insurance product or service" but all within products or services "used primarily for personal, family or household purposes."

Parties regulated: The new model law specifically applies to licensed insurers and producers, but it also talks about persons "required to be authorized or registered," perhaps signaling an intent to regulate more than just admitted primary insurers. The model law, however, does not stop there. It also requires licensees to contractually mandate that third-party service providers maintain safeguards, notify of breaches and indemnify the licensees against losses due to the breach. Finally, the model law invokes the McCarran-Ferguson Act to pre-empt enforcement of "federal law or regulation regarding data security or investigation or notification of a breach of data security" in regard to licensees. It remains to be seen whether this pre-emption could reach noninsurance members of an insurance holding company system.

What is required of the licensee:

1. **An information security program** to control risks and anticipate threats, using the Framework for Improving Critical Infrastructure Cybersecurity by the National Institute of Standards and Technology as a guide, but including (i) access controls on information systems; (ii) restrictions on access to physical locations; (iii) encryption of data, both in transit and at rest; (iv) design procedures to ensure security of system modifications; (v) multifactor authentication; (vi) system monitoring; (vii) actions to be taken in the event of a breach; (viii) measures to prevent data loss due to fire, water or other perils; and (ix) procedures for disposal of personal information. The program should be appropriate to the size and complexity of the licensee.
2. **Board of directors' oversight** of the development and maintenance of the information security program as well as approval of the written program. The new model law mandates that the board assign specific responsibility for the implementation of the program.

3. **Mandatory provisions in contracts with third-party service providers**, including contractual enforcement of appropriate safeguards, notice, indemnification, audit and representation/warranties of compliance. Note: if history is a guide, it is possible that vendors will resist some of these conditions.
4. **Ongoing monitoring and adjustment** of the information security program in light of changes in technology, threats, personal information and business arrangements (such as mergers, acquisitions and joint ventures).
5. **Investigation of any breach**, including assessment of the incident, identification of any personal information involved, and implementation of measures to restore the security and confidentiality of any compromised systems.
6. **Notification to** (i) the commissioner within five days that provides a highly detailed list of items, (ii) consumers and law enforcement "without unreasonable delay" if consumers face a risk of substantial harm or inconvenience, (iii) consumer reporting agencies within 60 days if the breach involves a specified number or more of consumers, and (iv) consumers – by mail unless the consumer has agreed to email – within 60 days of identifying the breach, including giving the commissioner a draft within 45 days of the breach and allowing him to edit the notice. Notification to the commissioner and consumers (along with identity theft protection services) is also required in the event of a breach by a third-party provider.
7. **Provision of an offer of credit identity theft protection services** to affected consumers for a minimum of 12 months.

Examination, hearing and penalties: The new model law also provides for examination and investigation of a licensee along with the regulator's power to hold hearings in the event of a violation. Any adversely affected person must be allowed to intervene upon showing good cause. If a violation is found, the commissioner will provide written findings and serve a cease and desist order on the licensee. If no violation is found, the report must be served on those whose rights were allegedly violated. The model law provides for suggested penalties of up to $500 per violation, up to a maximum of $10,000, plus $10,000 per violation of a cease and desist order, up to a maximum of $50,000. The model law provides for judicial review by a court.

Individual remedies: The new model law borrows some individual remedy provisions from the Privacy Protection Model Act, allowing consumers to bring private actions seeking equitable relief for violations of consumer rights. The new model law also permits consumers to recover costs and attorney fees if they should prevail. The new model law does not contain the Privacy Protection Model Act's prohibition on monetary awards exceeding actual damages but does say that there will be no remedy or recovery except as specifically provided.

Confidentiality: Information provided pursuant to the model law is to be protected from FOIA-type disclosure and subpoena of regulators receiving information; however, it is not entirely clear whether such protection would extend to all disclosures required under the model law.

This new model law provides for extensive regulation of insurers and producers, reinforced by examinations and penalties. The new model law is specifically oriented toward mandating security procedures and imposing penalties for breaches and resulting disclosures, whereas the Privacy Protection Model Act has been oriented toward identifying permitted disclosures, and the Privacy of Consumer Financial and Health Information Regulation is oriented toward privacy policies and violations of those policies. Neither of the prior models imposes substantial obligations in regard to the conduct of third parties as the new model law does. The two prior cybersecurity pronouncements of the NAIC, the Roadmap and the Principles, lack the high level of specificity found in the new model law. Given the bold statement about pre-emption of federal law, insurers and producers who believe this new model law would have an unwarranted adverse effect on them are encouraged to comment on or before March 23.

Authors



Stanley A. Twardy, Jr.

Of Counsel

Stamford, CT | (203) 977-7368

satwardy@daypitney.com