Akin Gump
STRAUSS HAUER & FELD LLP

Cybersecurity Alert

October 31, 2017

Key Points

- NAIC recently adopted an Insurance Data Security Model Law that follows the risk assessment-based approach of the New York DFS Cybersecurity Regulation. This signals the growing influence of the New York Regulation, including its 72-hour disclosure deadline. Compliance with the New York Regulation ensures compliance with the Model Law.
- Reinsurers face new notification requirements under the Model Law, which require that they provide notice of any cybersecurity event to insurers and state departments of insurance.
- Adoption of the Model Law could provide welcome encouragement for uniformity between states with regard to data security regulations in the insurance sphere.

National Association of Insurance Commissioners (NAIC) Issues Insurance Data Security Model Law

On October 24, 2017, the National Association of Insurance Commissioners (NAIC) adopted the "Insurance Data Security Model Law" ("Model Law"), which signals the continued trend toward greater regulatory interest in data security issues within the insurance context and adopts the risk assessment-based approach first promulgated by New York regulators.

Origins and Purpose

NAIC promulgates model laws in an effort to, among other things, encourage uniformity in the regulation of insurance products. This issue is particularly important in the cyber context, given the expanding number of states adopting data security regulations. The recent wave of data security breaches has also heightened regulatory interest in data held by insurance-related entities, given the typically sensitive nature of that data and the volume of data at issue.

The Model Law creates model rules and standards for insurers, agents and other licensed entities related to data security, investigation, and notification of a breach of data security. Adoption of the Model Law is voluntary; some member states may choose to adopt only portions of it, some none of it, and others all of it. The authors solicited input from regulators as well as industry and consumer representatives during the drafting process.

The Model Law follows the pattern of the New York State Department of Financial Services (DFS) Cybersecurity Regulation, which went into effect on March 1, 2017. Details of the DFS statute can be found in earlier client alerts.

The DFS Superintendent recently "applaud[ed] the NAIC for recognizing the need for a national uniform cybersecurity standard for the insurance industry modeled on New York's trailblazing risk assessment-based approach."

Key Components

The Model Law takes as its starting place DFS's proactive approach that requires entities to undertake a risk assessment to use in creating their information security programs. Indeed, the drafters of the Model Law make clear that compliance with the DFS Cybersecurity Regulation (*see* 23 NYCRR 500) ensures compliance with the Model Law. Key components of the information security program required under the Model Law include:

- maintaining an information security program based on a cybersecurity risk assessment, including, among other things, the proactive identification of threats, protection against unauthorized access and periodic destruction of data no longer necessary
- requiring oversight by an entity's board of directors, including receipt of an annual written report from executive management concerning the status of the entity's program
- evaluating and addressing cybersecurity risks posed by third-party service providers, including requiring implementation of appropriate security measures
- establishing a written incident response plan that, among other things, identifies requirements for the remediation of any identified weakness in the system
- providing an annual certification of compliance to departments of insurance.

Exceptions to the information security program requirements outlined above vary from the exemptions included in the DFS Cybersecurity Regulation. Unlike the DFS Regulation, the Model Law does not exempt companies that have under $5 million in gross annual revenue for each of the prior three years from in-state operations, or less than $10 million in year-end total assets. (See 23 NYCRR 500.19 (2) & (3).) Exceptions under the Model Law include:

- a general exception for licensees with fewer than 10 employees
- an exception for entities that have and maintain information security programs that comply with the Health Insurance Portability and Accountability Act ("HIPAA") and all related statutes, rules, guidelines, etc.
- an exception for employees or agents of a licensee, which are also themselves licensees.

The Model Law also outlines standards for the notification of departments of insurance, as well as consumers, regarding cybersecurity incidents. Highlights of those requirements include:

- 72-hour deadline in which to provide electronic notice to departments of insurance regarding cybersecurity events if certain requirements are met
- list of standard criteria to include in department notices and requirement that consumer notice letter be attached, standard criteria include whether police report filed, identity of source of event, copy of licensee's privacy policy, name of contact person, etc.
- continuing obligation on licensee to update and supplement notifications
- obligation on reinsurers to provide notice of cybersecurity events to insurers and departments, which marks a departure from the DFS statute that did not address this issue

Looking Forward

Although the Model Law is not mandatory, it will likely lead to increased adoption of the risk assessment-based approach to cybersecurity. The proactive, preparation-focused approach espoused by both the DFS Cybersecurity Regulation and the Model Law is fast becoming industry best practice.

Similarly, the Model Law adopts and lends added importance to DFS's expansive definition of "non-public information" (NPI). That definition encompasses three types of data: (1) business related information of the licensee, (2) personally identifiable information of consumers, and (3) certain health data. NAIC's use of DFS's NPI definition suggests that companies may be best served by adopting this expansive definition within internal policies and programs to ensure full compliance with developing industry standards and best practices.

Contact Information

If you have any questions concerning this alert, please contact:

Michelle Reed
mreed@akingump.com
214.969.2713
Dallas

Shawn Hanson
shanson@akingump.com
415.765.9528
San Francisco

Natasha Kohne
nkohne@akingump.com
415.765.9505
San Francisco

Jo-Ellyn Sakowitz Klein
jsklein@akingump.com
202.887.4220
Washington, D.C.

Diana Schaffner
dschaffner@akingump.com
415.765.9507
San Francisco

Adam Axler
aaxler@akingump.com
202.887.4256
Washington, D.C.