MINTZ

Insurance Commissioners Approve Data Security Model Law

December 12, 2017 | Blog |

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

The National Association of Insurance Commissioners (NAIC) has approved its draft of the Insurance Data Security Model Law (Model Law) via a meeting of its Executive and Plenary Committees. This important development follows New York Department of Financial Services ("DFS") Cybersecurity Requirements for Financial Services Companies regulation that took effect on March 1, 2017 (DFS Cybersecurity Regulation) that we have covered **previously**.

NAIC likely recognizes that the numerous data breaches that have occurred over the past year have created an opportunity to build upon the momentum created by the DFS Cybersecurity Regulation, and provide an environment of comprehensive compliance requirements to protect Licensees and Consumers. Indeed, the Model Law even contains Drafting Note stating that:

The drafters of this Act intend that if a Licensee, as defined in Section 3, is in compliance with N.Y. Comp. Codes R. & Regs. tit.23, § 500, *Cybersecurity Requirements for Financial Services Companies*, effective March 1, 2017, such Licensee is also in compliance with this Act.

In many cases, model laws approved by NAIC, a U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia and five U.S. territories, are approved within these jurisdictions as binding law. Below is a high level overview of particularly salient points of the Model Law.

1. **The Model Law Would Apply To All Licensees**

The Model Law is intended to apply to any "Licensee" which is defined as "any Person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State." The definition excludes "a purchasing group or a risk retention group chartered and licensed in a state other than this State or a Licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction."

2. **Licensee Must Identify And Assess Risks To Nonpublic Information**

All Licensees will be required to designate a responsible party, be it one or more employees, an affiliate or outside vendor. The risk assessment should be appropriate for the Licensee based on reasonably foreseeable internal or external threats that could result in unauthorized access, misuse or destruction of Nonpublic Information.

Nonpublic Information is quite broadly defined. It can consist of any information whose disclosure would create a material impact to business, operations or security of the Licensee, or any information that could be used to identify a consumer along with one or more of the following: (1) SSN, (2) Driver's license or identification card number, (3) Account number, credit or debit card number, (4) any security code, access code or password that would permit access to a Consumer's financial account, (5) Biometric records. Further, information besides age or gender, data derived from a healthcare provider or Consumer and involving the healthcare of the Consumer or the Consumer's family, within broad categories, would qualify as well.

Conducting this risk assessment will require a detailed understanding by the Licensee of the information flows and risk factors faced by the organization, including leveraging of Third-Party Service Providers that the Licensee contracts with.

3. **Licensees Must Implement And Maintain A Written Information Security Program To Mitigate Identified Risks**

Based on the findings of the risk assessment above, and "[c]ommensurate with the size and complexity of the Licensee, the nature and scope of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody or control" each Licensee must implement and maintain a written Information Security Program.

The Information Security Program must protect the security and confidentiality of Nonpublic Information and the Information System as a whole, including minimizing the likelihood of harm to any Consumer. The Information Security Program must define and periodically reevaluate a schedule for retention of Nonpublic Information and destruction of the same.

Numerous requirements, including appropriately restricting physical access, use of appropriate controls, and regular testing are also enumerated. Further, Licensees are required to "[p]rotect by encryption or other appropriate means, all Nonpublic Information while being transmitted over an external network and all Nonpublic Information stored on a laptop computer or other portable computing or storage device or media."

An appropriate incident response plan designed to allow the Licensee to "recover from, any Cybersecurity Event that compromises the confidentiality, integrity or availability of Nonpublic Information in its possession, the Licensee's Information Systems, or the continuing functionality of any aspect of the Licensee's business or operations" must also be established.

The definition of Cybersecurity Event is broad. Any "event resulting in unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System" will be deemed a Cybersecurity Event.

4. **Annual Compliance Certification And Five Year Period of Records Retention Required**

Each insurer domiciled in any state enacting the model law will be required to submit annually, by February 15th, a certification certifying compliance with the Model Law. Further, records supporting this certification must be maintained for no less than five years. If the insurer identifies areas that require material improvement, this must be documented and available for inspected by the Commissioner, who shall be the chief insurance regulatory official of the state.

5. **Cybersecurity Event Investigation Requirement**

Any Cybersecurity Event, defined as any "event resulting in unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System" must be investigated promptly. The investigation must determine to the extent possible: (1) if a Cybersecurity Event occurred, (2) if so, the nature and scope of the Cybersecurity Event, (3) identify any impacted Nonpublic Information, (4) and perform reasonable measures to restore security and prevent further unauthorized acquisition, release or of Nonpublic Information. If a Third-Party Service Provider has a Cybersecurity Event, the Licensee is responsible for conducting the same investigation of Third-Party Service Provider or ensuring that the Third-Party Service Provider completes the same.

Records concerning all Cybersecurity Events must be maintained for at least five years and produced to the Commissioner upon demand.

6. **Cybersecurity Event Reporting Requirement**

Cybersecurity Events must be reported to the Commissioner "as possible **but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred" where either of two conditions are satisfied.**

First, the reporting requirement applies when the state of occurrence is the Licensee's home state if the Licensee is a producer, as defined by the Producer Licensing Model Act. Second, the requirement applies if the Licensee reasonably believes that the Nonpublic Information of more than 250 Consumers within the state would be impacted and any state or federal law would require notice to a government body, or if the Cybersecurity Event has a "reasonable likelihood of materially harming any Consumer residing within the state or a material part of the normal operations of the Licensee.

7. **Third-Party Service Provider And Appropriate Measures Requirement**

Licensees must exercise due diligence in selecting any Third-Party Service Provider. Further, "Licensee[s] shall require a Third-Party Service Provider to implement appropriate administrative, technical, and physical measures to protect and secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider." Please note that this would also need to be accomplished at least through the required written Information Security Program as discussed above.

If you have any questions regarding the implications of the Model Law and likely compliance requirements, please do not hesitate to contact the team at **Mintz Levin**.

Authors