CARLTON FIELDS

Ohio Moves on Insurance Cybersecurity

December 31, 2018

Ohio has joined South Carolina in becoming the next state to adopt a variation of the NAIC Insurance Data Security Model Law ("MDL-668"). This legislation makes a number of changes to Ohio's insurance law, including the addition of a new Chapter 3965, which establishes "standards for data security and for the investigation of and notification to the Superintendent of Insurance of a cybersecurity event" (containing new Sections 3965.01 through 3965.11). Licensees will have one year to come into compliance with the new requirements, with the exception of the third party service provider provisions (Section 3965.02(F)), which have been granted a two-year implementation date.

Like MDL-668, Ohio's law applies to all individuals or non-governmental entities required to be authorized, registered, or licensed pursuant to the state's insurance laws ("licensees"). Among other things, the law provides specific requirements for an information security program, risk assessment and management, board of directors' oversight, third-party service provider due diligence and monitoring, notice and investigation of cybersecurity events, and annual certification to the Superintendent of Insurance.

Ohio has largely followed MDL-668, but contains several notable modifications:

- New Chapter 3965 and rules promulgated thereunder are the "exclusive state standards and requirements applicable to licensees regarding cybersecurity events, the security of nonpublic information, data security, investigation of cybersecurity events, and notification to the superintendent of cybersecurity events." [See Section 3965.09]. Ohio's law further states that the Superintendent of Insurance considers the nature, scale, and complexity of licensees in adopting rules and administering the new law. Section 3965.11

- The law provides an affirmative defense to any tort cause of action that "alleges that the failure to implement reasonable information security controls resulted in a data breach concerning nonpublic information." [See Section 3965.08]. Section 3965.02(J) also states that "a licensee that meets the requirements of this chapter shall be deemed to have implemented a cybersecurity program that reasonably conforms to an industry-recognized cybersecurity framework for purposes of Chapter 1354 of the Revised Code.
- Two Sections, 3965.01 and 3965.04, address materiality of a cybersecurity event, both indicating that there must be a "reasonable likelihood" of material harm to a consumer or the licensee's normal operations in order to qualify as a cybersecurity event or to trigger a notice to the Superintendent of a cybersecurity event.
- The Superintendent of Insurance must be notified of an event no later than "three business days" after a determination that a cybersecurity event has occurred. MDL-668 requires notification no later than 72 hours after breach determination.
- When a licensee determines there has been a cybersecurity event that triggers a notice to the Superintendent, the notice contents required by Section 3965.04(B)(1) mirror that of MDL-668. However, under the new Ohio law, updates to the Superintendent are only required for "material developments relating to the cybersecurity event."
- Clearer confidentiality and privilege protection for information shared with regulators. "Documents, materials or other information" in the possession of the NAIC, a vendor, NAIC third-party consultant, or a third-party service provider are: privileged and confidential by law; are not public records, and shall not be released; not subject to subpoena; not subject to discovery or admissible as evidence in a private civil action. [Section 3965.06(F)]
- In addition to the exemptions found in MDL-668, Ohio exempts a licensee from complying with the Information Security Program requirement, provided the licensee meets any of the following requirements [see Section 3965.07(A)]: less than 20 employees; gross annual revenue under $5,000,000; and under $10,000,000 in assets as measured at the end of the licensee's fiscal year.
- Ohio-domiciled insurers that do not conduct business in any other states are permitted to include the annual certification of compliance required by February 15 of each year in their corporate governance annual disclosure required by Section 3901.073 of the Revised Code.

The above is a general overview and discussion and interested parties should review the complete text of the legislation for additional information. It is expected that other states will take active measures to enact MDL-668 during 2019 legislative sessions.

Click here to view the NAIC Insurance Data Security Model Law (MDL-668).

Click here to view the Ohio Law.

Related Practices

Cyber Insurance Coverage Disputes
Cybersecurity and Privacy