Published on *The National Law Review* https://natlawreview.com

Michigan-Based Insurance Licensees Now Subject to New Data Security Requirements

Article By:

John J. Rolecki

Under new rules put forth by the National Association of Insurance Commissioners' (NAIC) Insurance Data Security Model Law and adopted by the Michigan legislature in 2018, Michigan-based insurance licensees are now subject to additional requirements relating to data security as of Jan. 20, 2021. The new rules are codified as chapter 5A of the Insurance Code (the "Act") and focus on regulating "licensees," which are defined as "any licensed insurer or producer required by DIFS to hold a certificate of authority, such as life & health, property & casualty, surplus lines, fraternal, and title insurers."

The portions of the Act that became effective on January 20 include terms requiring licensees:

- with 25 or more employees to develop, implement, and maintain a comprehensive written information security program (WISP) that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system, in addition a written incident response plan; and
- to contractually bind their third-party service providers to implement appropriate measures to protect and secure the information systems and nonpublic information they can access or hold.

Notably, many of these requirements are similar to those of the federal Gramm-Leach-Bliley Act (GLBA)'s Safeguards Rule, which also imposes data privacy-related obligations on "financial institutions," including insurance agencies.

Unlike the GLBA, however, the Act also contains specific data breach notification requirements. Although Michigan's general data breach notification law expressly exempts entities subject to or regulated by the Michigan Insurance Code, under the Act's recently effective terms licensees of any size – even those having fewer than 25 employees – must notify the director of the Department of Insurance and Financial Services (DIFS) within 10 days after a determination of a cybersecurity event is made. In its notification to DIFS, the licensee must include a copy of its privacy policy, a summary of the event, and a statement regarding whether the event resulted from a lapse in its controls and procedures.

If the event is likely to cause substantial loss or injury, or result in identity theft, to one or more Michigan residents, the licensee must provide notice to each resident whose personal information was accessed without authorization. Non-Michigan licensees are only required to notify DIFS of a security breach if 250 Michigan residents are impacted; for Michigan licensees, there is no such threshold.

What this means for you:

- If you are a licensee with 25 or more employees, you are required to have a WISP in place.
- If you are a licensee with 25 or more employees, you are required to have contractual terms in place that require third-party service providers to implement security measures to protect the data that you share with them.
- If you are a licensee of any size and you experience a data breach of any size, you must provide DIFS with a detailed notification, including whether your controls and procedures contributed to the security event.

National Law Review, Volume XI, Number 49