Legislative Analysis

Phone: (517) 373-8080
http://www.house.mi.gov/hfa

INSURANCE DATA SECURITY MODEL LAW

Analysis available at
http://www.legislature.mi.gov

House Bill 6491 as introduced
Sponsor: Rep. Lana Theis
Committee: Insurance
Complete to 11-29-18

SUMMARY:

House Bill 6491 would amend the Insurance Code by adding Chapter 5A (Data Security). The chapter would enact new data security requirements for licensees that handle sensitive information, including creating and maintaining an adequate information security program, and outline the licensee's responsibilities to law enforcement and its customers in the case of a cybersecurity event. The chapter is based on the Insurance Data Security Model Law of the National Association of Insurance Commissioners (NAIC).[1] A detailed description of the bill follows.

Information security program

House Bill 6491 would require ***licensees*** to build and maintain an information security program capable of protecting the nonpublic information of its customers from a ***cybersecurity event***. The licensee would have to create and maintain the program based on its risk assessment.

> ***Licensee*** would mean a licensed insurer or producer and other persons required to gain a certificate of authority under the bill.
>
> ***Cybersecurity event*** would mean an event that resulted in unauthorized access to, acquisition of, disruption of, or misuse of the information system or the nonpublic information that it stores.

A licensee that employed fewer than 50 employees, made less than $10.0 million in gross annual revenue, or had less than $25.0 million in year-end total assets would be exempt from the requirement to implement and maintain an information security program. However, if the licensee ceased to fall under this exception, it would have 180 days to comply with the bill's requirements.

The information security program would have to be designed to do all of the following:

- Protect the security and confidentiality of nonpublic information and the security of the information system.
- Protect against any threats or hazards to the security or integrity of nonpublic information and the system.

[1] Insurance Data Security Model Law: https://www.naic.org/store/free/MDL-668.pdf
NAIC background: https://www.naic.org/documents/cmte_legislative_liaison_brief_data_security_model_law.pdf

- Protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to any consumer.
- Maintain policies and procedures for the secure and periodic disposal of unnecessary nonpublic information.

Under the bill, the licensee would have to assign one or more of its employees, or contract an affiliate or outside vendor, to monitor and maintain the program. Additionally, the licensee would have to conduct a risk assessment that identified reasonably foreseeable internal or external threats that could result in unauthorized access to and use of nonpublic information—including any accessible to, or held by, third-party service providers. The licensee would have to assess the likelihood and potential damage of these threats, then assess the sufficiency of the licensee's safeguards in stopping these threats and implementing additional security measures where necessary. Those measures could include implementation of access controls, restricting access to nonpublic information, encryption, or regular monitoring for cyberattacks, among other measures. The licensee would have to conduct a risk assessment at least once a year.

If the licensee had a board of directors, the board or a committee of the board would have to require the licensee's executive management to develop, implement, and maintain the information security program while also providing the board with an annual report detailing the overall status of the program as well as material matters relating to it, such as information on cybersecurity events, risk assessments, and recommendations for changes.

The licensee would also have to exercise due diligence in selecting a third-party service provider and require it to uphold the security of the licensee's nonpublic information. A licensee would need to keep up-to-date with any changes that would affect the security of its information security system, such as changes in technology or the licensee's own changing business arrangements.

Incident response plan

A licensee would have to develop a written incident response plan that would take effect in case of a cybersecurity event that compromised its information security system or its nonpublic information. Among other things, the plan would lay out the licensee's mechanisms for responding to and recovering from such a security breach, as well as specifying the roles, responsibilities, and levels of decision-making authority.

Required certification of compliance

Under the bill, by February 15 of each year, each Michigan insurer would be required to submit a written statement certifying its compliance with the requirements of Chapter 5A to the Director of the Department of Insurance and Financial Services (DIFS). The insurer would have to maintain all records, schedules, and data supporting this certification for examination by DIFS for five years. If the insurer found that any part of its security was in need of improvement, then the insurer would have to report on it and outline its plans for making these improvements to the director.

Required actions in the case of a cybersecurity event

If the licensee learned that a cybersecurity event had or may have occurred, then either the licensee or those to whom the licensee delegated responsibility for the information security program would be required to conduct a prompt investigation. The investigation would have to determine whether a cybersecurity event had occurred, assess its nature, identify any nonpublic information that may have been compromised, and perform any reasonable measures necessary to restore the security of its information systems and the nonpublic information they hold. The licensee would have to maintain records concerning all cybersecurity events for at least five years for review by the DIFS director.

If a Michigan licensee determined that a cybersecurity event had happened, the licensee would have to notify the director within 10 business days after the determination if the event were reasonably likely to materially harm either a customer residing in Michigan or the normal operation of the licensee itself. A licensee would have that notification requirement if the licensee reasonably believed that 250 or more Michigan consumers were affected and that the event was a qualifying cybersecurity event.

This report would have to include as much information about the cybersecurity event as possible, including what information was compromised, the identity of the source of the event, and measures being taken to restore security to the information security program.

If the cybersecurity event occurred in a system maintained by a third-party service provider, then the licensee would still be required to submit a report to the director if the third-party service provider did not do so.

If the event involving nonpublic information occurred where a licensee was acting as an assuming insurer, then the assuming insurer would have to inform both the DIFS director and the ceding insurer of the cybersecurity event. In such a case, the ceding insurer would then be responsible for informing its customers. If the licensee were an insurer or third-party service provider through whom an independent insurance producer accessed nonpublic information for a customer, then the licensee would need to notify the producer of all affected customers no later than when the notice is provided for the affected customer. This obligation would not exist in cases where the producer is not known or does not have requisite legal standing.

Unless the licensee determined that the security breach did not or was not likely to cause substantial harm to, or cause the identity theft of, one or more Michigan residents, a licensee that owns or licenses data that suffered from a security breach would have to give notice of the breach to the affected residents. If the licensee did not own or hold license to the data in a security breach, but maintained the database, the licensee would have to inform the owner or licensor of the data (unless the licensee determined that the breach was harmless). A licensee would be required to act with the care an "ordinarily prudent person" would exercise under similar circumstances. The licensee would have to provide these notices without unreasonable delay unless a delay was either necessary to assess the scope of the breach and restore its integrity or if the licensee was informed not to provide a notice by law enforcement.

Requirements for notice of a breach

The notice would have to be provided by mail, email, or telephone, with specified requirements for each. If the licensee showed that providing notice would exceed $250,000 or that notice to 500,000 or more Michigan residents was required, the licensee could use substitute notice of a mass email to the licensee's customers, conspicuous posting on the licensee's website, and notification of statewide media. The notice would have to provide recipients with certain specified information about the breach.

After filing the notices listed in the bill, the licensee would have to notify required national consumer reporting agencies of the security breach without unreasonable delay. The licensee would not be required to notify agencies if the licensee were providing notice to 1,000 or fewer Michigan residents or if the licensee fell under federal reporting requirements.

Certain notification requirements would be waived if the licensee were subject to and compliant with the Health Insurance Portability and Accountability Act (HIPAA) and related regulations.

The notice requirements would be applicable in the case of a security breach occurring after December 31, 2019. These requirements would preempt any local rule or ordinance intended to regulate these matters.

Violations and penalties

If a person provided notice of a security breach when one had not occurred with the intent to defraud, the person would be guilty of a misdemeanor punishable by up to 93 days' imprisonment or a fine of up to $250 for the first violation, or both, with the possible imprisonment and fine increasing for subsequent violations. If a person knowingly failed to provide notice of a security breach required under the bill, the person could be ordered to pay a civil fine of up to $250 for each failure to provide notice, up to a possible total of $750,000 for a single security breach.

Confidentiality of materials

Materials acquired by DIFS in compliance with the bill would not be subject to the Freedom of Information Act (FOIA), subpoena, or discovery or admissible in evidence in any private civil action. In addition, the director would be authorized to use this information to fulfill the duties of DIFS, but otherwise could not make any of the information public without the consent of the licensee. The director would be allowed to share and receive documents, while complying with applicable rules concerning confidentiality and privilege.

Effective date

The bill would take effect January 20, 2020. Licensees would have to implement the information security program requirements by January 20, 2021, but would have until January 20, 2022 to fulfill certain requirements related to third-party service providers.

Proposed MCL 500.550 et al.

FISCAL IMPACT:

House Bill 6491 would create numerous responsibilities for the Department of Insurance and Financial Services (DIFS) related to the oversight of licensees' information security programs and relevant notifications. Costs related to DIFS' responsibilities would likely be supported by existing departmental appropriations. The bill would establish a civil fine not to exceed $250 for each failure by a person to provide a notice of a security breach, as required under the bill. The bill stipulates that aggregate liability for failing to provide notice of a security breach for multiple violations related to the same security breach is not to exceed $750,000. Revenues resulting from collection of the civil fine would be deposited to the state's general fund.

Under the bill, persons that provide notice of a security breach, when a security breach has not occurred, with the intent to defraud, would be guilty of a misdemeanor. New misdemeanor convictions would increase costs related to county jails and/or local misdemeanor probation supervision. The costs of local incarceration in a county jail and local misdemeanor probation supervision, and how the costs are financed, vary by jurisdiction. Any fiscal impact on the judiciary and local court systems would depend on how provisions of the bill affect caseloads and related administrative costs. Any increase in penal fine revenues would increase funding for local libraries, which are the constitutionally designated recipients of those revenues.

Legislative Analyst: Nick Kelly
Fiscal Analysts: Marcus Coffin
Robin Risko