Legislative Analysis

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

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

INSURANCE DATA SECURITY MODEL LAW

House Bill 6406 as enacted
Public Act 649 of 2018
Sponsor: Rep. Joseph Graves
House Committee: Financial Services
Senate Committee: Finance

House Bill 6491 as enacted
Public Act 690 of 2018
Sponsor: Rep. Lana Theis
House Committee: Insurance
Senate Committee: Finance

Complete to 6-24-19

BRIEF SUMMARY: House Bill 6491 adds Chapter 5A (Data Security) to the Insurance Code to enact new data security requirements for insurers that handle sensitive information, including creating and maintaining an adequate information security program, and outlines the insurer's responsibilities to law enforcement and its customers in a cybersecurity event. House Bill 6406 exempts insurers from the Identity Theft Protection Act.

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, all of which would generate new costs. (See **Fiscal Information**, below, for further discussion.)

THE APPARENT PROBLEM:

In recent years, cyber-attacks on institutions holding sensitive information for large numbers of individuals—such as the hack of credit reporting company Equifax in 2017[1]—have raised concerns over the amount of security that companies provide for the information with which they are entrusted. This concern has grown especially prevalent for insurance providers, who handle a wide range of sensitive information, including medical records and credit information, that, among other things, may be used to steal an individual's identity.

THE CONTENT OF THE BILLS:

House Bill 6491 adds Chapter 5A to the Insurance Code. The chapter contains new data security requirements for licensees that handle sensitive information, including creating and maintaining an adequate information security program, and outlines 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).[2] A detailed description follows.

[1] https://www.pbs.org/newshour/nation/2-5-million-americans-may-affected-equifax-hack-company-says
[2] Insurance Data Security Model Law: https://www.naic.org/store/free/MDL-668.pdf

Information security program

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

> ***Licensee*** means a licensed insurer or producer and other persons required to gain a certificate of authority under the Insurance Code.
>
> ***Cybersecurity event*** means an event that results in unauthorized access to and acquisition of, or disruption or misuse of, an information system or the nonpublic information that it stores.
>
> ***Nonpublic information*** means electronic information that is not publicly available and is any of the following:
>
> - Business-related information of a licensee that, if tampered with or disclosed, accessed, or used in an unauthorized way, would cause a material adverse impact to the licensee's business, operations, or security.
> - Information about a consumer, by which the consumer can be identified, in combination with any of the following:
>   - Social Security number.
>   - Driver license or ID card number.
>   - Financial account, credit card, or debit card number.
>   - Any code or password that would allow access to a financial account.
>   - Biometric records.
> - Information about a consumer, by which the consumer can be identified, that relates to any of the following:
>   - The physical, mental, or behavioral health or condition of any consumer or a member of the consumer's family.
>   - The provision of health care to any consumer.
>   - Payment for the provision of health care to any consumer.

A licensee that employs fewer than 25 employees is exempt from the requirement to implement and maintain an information security program. However, if the licensee ceases to fall under this exception, it has 180 days to comply with the bill's requirements.

The information security program must 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.
- 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.

NAIC background: https://www.naic.org/documents/cmte_legislative_liaison_brief_data_security_model_law.pdf

Under the bill, the licensee must assign one or more of its employees, or contract an affiliate or outside vendor, to monitor and maintain the program. Additionally, the licensee must conduct a risk assessment that identifies 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 must assess the likelihood and potential damage of these threats, then assess the sufficiency of the licensee's safeguards in stopping these threats and implement additional security measures where necessary. Those measures may include implementation of access controls, restricting access to nonpublic information, encryption, or regular monitoring for cyberattacks, among other measures. The licensee must conduct a risk assessment at least once a year.

If the licensee has a board of directors, the board or a committee of the board must 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 also must 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 must 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 must develop a written incident response plan that will take effect if a cybersecurity event compromises its information security system or its nonpublic information. Among other things, the plan must lay out the licensee's mechanisms for responding to and recovering from such a security breach, as well as specifying roles, responsibilities, and levels of decision-making authority.

Required certification of compliance

By February 15 of each year, each Michigan insurer must 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 must maintain all records, schedules, and data supporting this certification for examination by DIFS for five years. If the insurer finds that any part of its security is in need of improvement, the insurer must report on it and outline its plans for making these improvements to the director.

Required actions in the case of a cybersecurity event

If a licensee learns that a cybersecurity event has or may have occurred, then either the licensee or those to whom it delegated responsibility for the information security program must conduct a prompt investigation to determine whether a cybersecurity event has 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 must maintain records concerning all cybersecurity events for at least five years for review by the DIFS director.

If a Michigan licensee determines that a cybersecurity event has happened, the licensee must notify the director within 10 business days after the determination if the event is reasonably likely to materially harm either a customer residing in Michigan or the normal operation of the

licensee itself. A licensee has that notification requirement if the licensee reasonably believes that 250 or more Michigan consumers are affected and that the event is a qualifying cybersecurity event.

This report must 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, the licensee must still submit a report to the director.

If the event involving nonpublic information occurred where a licensee was acting as an assuming insurer, the assuming insurer must inform both the DIFS director and the ceding insurer of the cybersecurity event. In such a case, the ceding insurer is then responsible for informing its customers. If the licensee is an insurer or third-party service provider through whom an independent insurance producer accesses nonpublic information for a customer, the licensee must notify the producer of all affected customers no later than when the notice is provided for the affected customer. This obligation does not exist if the producer is not known or does not have requisite legal standing. Unless the licensee determines that the security breach did not or is not likely to cause substantial harm to, or the identity theft of, one or more Michigan residents, a licensee that owns or licenses data that suffered from a security breach must give notice of the breach to the affected residents. If the licensee does not own or hold license to the data in a security breach, but maintains the database, the licensee must inform the owner or licensor of the data (unless the licensee determines that the breach is harmless). A licensee must act with the care an "ordinarily prudent person" would exercise under similar circumstances. The licensee must provide these notices without unreasonable delay unless a delay is necessary to assess the scope of the breach and restore its integrity or if the licensee is instructed by law enforcement not to provide a notice.

Requirements for notice of a cybersecurity event

The notice must be provided by mail, email, or telephone, with specified requirements for each. If the licensee shows that the cost of providing notice would exceed $250,000 or that notice to 500,000 or more Michigan residents is required, the licensee may 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 must provide recipients with certain specified information about the breach. After filing the notices listed in the bill, the licensee must notify required national consumer reporting agencies of the security breach without unreasonable delay. The licensee is not required to notify agencies if the licensee is providing notice to 1,000 or fewer Michigan residents or if the licensee falls under federal reporting requirements. Certain notification requirements are waived if the licensee is subject to and compliant with the Health Insurance Portability and Accountability Act (HIPAA) and related regulations. The notice requirements are applicable in the case of a security breach occurring after December 31, 2019. These requirements preempt any local rule or ordinance intended to regulate these matters.

Violations and penalties

If a person provides notice of a security breach when one had not occurred, with the intent to defraud, the person is 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 fails to provide required notice of

a security breach, the person may 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 are not subject to the Freedom of Information Act (FOIA), subpoena, or discovery or admissible in evidence in any private civil action. In addition, the director may use this information to fulfill the duties of DIFS, but otherwise may not make any of the information public without the consent of the licensee. The director may share and receive documents, while complying with applicable rules concerning confidentiality and privilege.

Effective date

The bill takes effect January 20, 2021. Licensees must implement the information security program requirements by January 20, 2022, but have until January 20, 2023, to fulfill certain requirements related to third-party service providers.

MCL 500.550 et seq.

House Bill 6406 amends the Identity Theft Protection Act to exempt from that act an entity subject to or regulated under the Insurance Code (namely, an insurer) as well as an entity that owns, is owned by, or is under common ownership with an insurer and maintains the same cybersecurity procedures as the insurer.

The bill takes effect January 20, 2020.

[Note: There is a one-year gap between the effective dates of the bills. It is unclear whether insurance company data security would be subject to any specific state law during that time.]

FISCAL INFORMATION:

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.

House Bill 6406 would have no direct fiscal impact on the state or local units of government.

ARGUMENTS:

For:

Supporters of HB 6491 argued that, by adapting the standards of the national security model put forth by the NAIC, the bill would potentially exempt Michigan insurers from certain requirements of the Identity Theft Prevention Act. Supporters believe that the bill would create a better model for data security than that act, and thus may set a new standard for other states to follow. In contrast to the Identity Theft Prevention Act, the bill requires insurers to report a cybersecurity event only if it results in a "material breach," meaning one reasonably likely to cause harm to consumers or an insurer. Supporters argue that this standard of materiality will prevent insurers from being overburdened by the new data security requirements, while still holding them to a standard that protects their customers from harm.

Against:

Opponents argued that the bills create a special exemption from the Identity Theft Prevention Act specifically for insurers and that this will lead to other industries asking for the same treatment.

Legislative Analysts: Nick Kelly
E. Best
Fiscal Analysts: Marcus Coffin
Robin Risko
Michael Cnossen

■ This analysis was prepared by nonpartisan House Fiscal Agency staff for use by House members in their deliberations and does not constitute an official statement of legislative intent.