Senate Fiscal Agency
P. O. Box 30036
Lansing, Michigan 48909-7536

BILL ANALYSIS

Telephone: (517) 373-5383
Fax: (517) 373-1986

House Bill 6491 (Substitute H-1 as passed by the House)
Sponsor: Representative Lana Theis
House Committee: Insurance
Senate Committee: Finance

Date Completed: 12-13-18

CONTENT

The bill would create Chapter 5A (Data Security) under the Insurance Code, which would do the following:

-- Require a licensee to develop, implement, and maintain a comprehensive written information security program that contained administrative, technical, and physical safeguards for the protection of nonpublic information and its information system.
-- List criteria an information security program would have to meet.
-- Specify further requirements a licensee would have to adhere to regarding security and security protocols.
-- Require the board of directors or an appropriate committee of the board, if the licensee had a board, to require the licensee's executive management to develop, implement, and maintain its information security program; and require its executive management to report at least annually in writing certain information.
-- Require a licensee to monitor, evaluate, and adjust, as appropriate, the information security program consistent with certain changes listed in the bill.
-- Require each licensee to establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromised certain information or systems, and list what the plan would have to address.
-- Require each insurer domiciled in the State, by February 15 of each year, to submit to the Director of the Department of Insurance and Financial Services (DIFS) a written statement, certifying that the insurer was in compliance with Chapter 5A.
-- Require each insurer to maintain for examination by the DIFS all records, schedules, and data supporting the certificate for five years.
-- Require the licensee or an outside vendor or service provider, or both, designated to act on behalf of the licensee, to conduct a prompt investigation if the licensee learned that a cybersecurity event had or could have occurred.
-- Require the licensee to maintain records concerning all cybersecurity events for at least five years from the date of the cybersecurity event.
-- Require each licensee to notify the Director within 10 business days after a determination that a cybersecurity event had occurred involving nonpublic information that was in the possession of a licensee.
-- Specify other notification conditions pertaining to a cybersecurity event involving nonpublic information.

-- Require a licensee that owned or licensed data that were included in a database that discovered a security breach, or received notice of a security breach, to provide a notice of the security breach to each resident of the State if certain conditions were met.
-- List the methods by which a licensee could provide notice of a security breach to a resident of the State.
-- Require a licensee to notify each consumer reporting agency that compiled and maintained files on consumers on a nationwide basis of a security breach under certain circumstances.
-- Specify that a person who provided notice of a security breach when a security breach had not occurred, with the intent to defraud, would be guilty of a misdemeanor punishable as described in Chapter 5A.
-- Specify that a person who knowingly failed to provide a notice of a security breach would be ordered to pay a civil fine.
-- Specify that certain notification provisions would preempt any charter, ordinance, resolution, regulation, rule, or other action by a municipal corporation or other political subdivision of the State to regulate those matters.
-- Specify that any documents, materials, or other information in the control or possession of the DIFS or its Director relating to Chapter 5A would be confidential by law and privileged.
-- List actions the Director could take to assist in the performance of his or her duties under Chapter 5A.
-- List the entities that would be exempt from Chapter 5A or certain provisions specified in Chapter 5A.

Chapter 5A would take effect on January 20, 2020. A licensee would have to implement provisions regarding the information security program and other specified licensee requirements by January 20, 2021. However, a licensee would have until January 20, 2022, to 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 were accessible to, or held by, the third-party service provider.

Definitions

Under Chapter 5A, "authorized individual" would mean an individual known to and screened by the licensee and determined to be necessary and appropriate to have access to the nonpublic information held by the licensee and its information systems.

"Licensee" would mean a licensed insurer or producer, and other people licensed or required to be licensed, authorized, or registered, or holding or required to hold a certificate of authority under the Chapter. Licensee would not include a purchasing group or a risk retention group chartered and licensed in a state other than Michigan or a person that was acting as an assuming insurer that was domiciled in another state or jurisdiction.

"Consumer" would mean an individual, including an applicant, a policyholder, an insured, a beneficiary, a claimant, and a certificate holder, who is a resident of the State and whose nonpublic information is in a licensee's possession, custody, or control.

"Nonpublic information" would mean electronic information that is not publicly available information and is either of the following:

-- Any information concerning a consumer that because of name, number, personal mark, or other identifier can be used to identify the consumer, in combination with any one or more of the following data elements: Social Security number, driver license number or

nondriver identification card number, financial account number, or credit or debit card number, any security code, access code, or password that would permit access to a consumer's financial account, and biometric records.
-- Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a consumer, that can be used to identify a particular consumer, and that relates to any of the following: 1) the past, present, or future physical, mental, or behavioral health or condition of any consumer or a member of the consumer's family, 2) the provision of health care to any consumer, or 3) payment for the provision of health care to any consumer.

"Cybersecurity event" would mean an event that results in unauthorized access to and acquisition of, or disruption or misuse of, an information system or nonpublic information stored on an information system. Cybersecurity event would not include either of the following:

-- The unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key were not also acquired, released, or used without authorization.
-- The unauthorized access to data by a person if the access met all of the following criteria: 1) the person acted in good faith in accessing the data, 2) the access was related to activities of the person, and 3) the person did not misuse any personal information or disclose any personal information to an unauthorized person.

"Information system" would mean a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic nonpublic information, as well as any specialized system such as an industrial or process controls system, a telephone switching and private branch exchange system, or an environmental control system.

"Encrypted" would mean the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key.

"Information security program" would mean the administrative, technical, and physical safeguards that a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle nonpublic information.

"Multi-factor authentication" would mean authentication through verification of at least two of the following types of authentication factors:

-- Knowledge factors, such as a password.
-- Possession factors, such as a token or text message on a mobile phone.
-- Inherence factors, such as a biometric characteristic.

"Publicly available information" would mean any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from Federal, State, or local government records, by widely distributed media, or by disclosures to the general public that are required to be made by Federal, State, or local law. A licensee would have a reasonable basis to believe that information was lawfully made available to the general public if both of the following applied:

-- The licensee had taken steps to determine that the information was of the type that was available to the general public.
-- If an individual could direct that the information not be made available to the general public, that the licensee's consumer had not made that direction.

"Third-party service provider" would mean a person that is not a licensee and that contracts with a licensee to maintain, process, or store, or otherwise is permitted access to nonpublic information, through its provision of services to the licensee.

Licensee Requirements

Commensurate with the size and complexity of the licensee, the nature and scope of its activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in its possession, custody, or control, each licensee would have to develop, implement, and maintain a comprehensive written information security program, based on the licensee's risk assessment, that contained administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

A licensee's 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 information 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 disposal on a periodic basis of any nonpublic information that was no longer necessary for business operations or for other legitimate business purposes.

A licensee would have to do all of the following:

-- Designate one or more employees, an affiliate, or an outside vendor to act on its behalf who would be responsible for the information security program.
-- Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information.
-- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the nonpublic information.
-- Assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the licensee's operations.
-- Implement information safeguards to manage the threats identified in its ongoing assessment, and, no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.

Based on its risk assessment, a licensee would have to design its information security program to mitigate the identified risks, commensurate with its size and complexity, the nature and scope of the its 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.

Based on its risk assessment, the licensee would have to determine which of the following security measures were appropriate and implement those measures:

-- Placing access controls on information systems, including controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of information.

-- Identifying and managing the data, personnel, devices, systems, and facilities that enabled the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy.
-- Restricting physical access to nonpublic information to authorized individuals only.
-- Protecting 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.
-- Adopting secure development practices for in-house developed applications it used.
-- Modifying the information system in accordance with the licensee's information security program.
-- Using effective controls, which could include multi-factor authentication procedures for employees accessing nonpublic information.
-- Regularly testing and monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems.
-- Including audit trails within the information security program designed to detect and respond to cybersecurity events and to reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee.
-- Implementing measures to protect against destruction, loss, or damage of nonpublic information due to environmental hazards or other catastrophes or technological failures.
-- Developing, implementing, and maintaining procedures for the secure disposal of nonpublic information in any format.

The licensee also would have to do the following based on its risk assessment:

-- Include cybersecurity risks in the licensee's enterprise risk management process.
-- Stay informed regarding emerging threats or vulnerabilities and use reasonable security measures when sharing information relative to the character of the sharing and the type of information shared.
-- Provide its personnel with cybersecurity awareness training that was updated as necessary to reflect risks identified by the licensee in the risk assessment.

Licensee: Board of Directors & Executive Management Requirements

If a licensee had a board of directors, the board or an appropriate committee of the board, at a minimum, would have to require its executive management or its delegates to develop, implement, and maintain its information security program; and to require the licensee's executive management or its delegates to report in writing, at least annually, all of the following information:

-- The overall status of the information security program and the licensee's compliance with Chapter 5A.
-- Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, results of testing, cybersecurity events or violations, and management's responses to the material matters described in this provision, and recommendations for changes in the information security program.
-- If executive management delegated any of its responsibilities, it would have to oversee the development, implementation, and maintenance of the licensee's information security program prepared by a delegate and would have to receive a report from the delegate complying with the requirements of the report to the board of directors.

Third-Party Service Provider

A licensee would have to exercise due diligence in selecting its third-party service provider. A licensee would have to 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.

Information Security Program & Incident Response Plan

A licensee would have to monitor, evaluate, and adjust, as appropriate, the information security program consistent with any relevant changes in technology, the sensitivity of its nonpublic information, internal or external threats to information, and its own changing business arrangements.

As part of its program, each licensee would have to establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromised 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. An incident response plan would have to address all of the following areas:

-- The internal process for responding to a cybersecurity event.
-- The goals of the incident response plan.
-- The definition of clear roles, responsibilities, and levels of decision-making authority.
-- External and internal communications and information sharing.
-- Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls.
-- Documentation and reporting regarding cybersecurity events and related incident response activities.
-- The evaluation and revision as necessary of the incident response plan following a cybersecurity event.

Written Statement Ensuring Compliance

By February 15 of each year, each insurer domiciled in the State would have to submit to the Director a written statement, certifying that the insurer was in compliance with the requirements described above. Each insurer would have to maintain for examination by the DIFS all records, schedules, and data supporting this certificate for five years. To the extent an insurer had identified areas, systems, or processes that required material improvement, updating, or redesign, the insurer would have to document the identification and the remedial efforts planned and underway to address those areas, systems, or processes. The documentation would have to be available for inspection by the Director.

Cybersecurity Event Investigation

If a licensee learned that a cybersecurity event had or could have occurred, the licensee or an outside vendor or service provider, or both, designated to act on its behalf, would have to conduct a prompt investigation.

During the investigation, the licensee, or an outside vendor or service provider, or both, designated to act on behalf of the licensee, would have to, at a minimum, do as much of the following as possible:

-- Determine whether a cybersecurity event had occurred.
-- Assess the nature and scope of the cybersecurity event.
-- Identify any nonpublic information that could have been involved in the cybersecurity event.

-- Perform or oversee reasonable measures to restore the security of the information systems compromised in the cybersecurity event to prevent further unauthorized acquisition, release, or use of nonpublic information in the licensee's possession, custody, or control.

The licensee would have to maintain records concerning all cybersecurity events for at least five years from the date of the cybersecurity event and would have to produce those records on demand of the Director.

Notice of Cybersecurity Event

Each licensee would have to notify the Director as promptly as possible but not later than 10 business days after a determination that a cybersecurity event involving nonpublic information that was in the possession of a licensee had occurred when either of the following criteria had been met:

-- Michigan was the licensee's state of domicile, for an insurer, or Michigan was the licensee's home state, for an insurance producer, and the cybersecurity event had a reasonable likelihood of materially harming either of the following: 1) a consumer residing in the State, or 2) any material part of a normal operation of the licensee.
-- The licensee reasonably believed that the nonpublic information involved was of 250 or more consumers residing in the State and was either of the following: 1) a cybersecurity event affecting the licensee of which notice was required to be provided to any government body, self-regulatory agency, or other supervisory body under any State or Federal law, or 2) a cybersecurity event that had a reasonable likelihood of materially harming either any consumer residing in the State or any material part of the normal operation of the licensee.

The licensee would have to provide the information in electronic form as directed by the Director. The licensee would have a continuing obligation to update and supplement initial and subsequent notifications to the Director regarding material changes to previously provided information. The licensee would have to provide as much of the following information as possible:

-- The date of the cybersecurity event.
-- A description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any.
-- How the cybersecurity event was discovered.
-- Whether any lost, stolen, or breached information had been recovered and, if so, how this was done.
-- The identity of the source of the cybersecurity event.
-- Whether the licensee had filed a police report or had notified any regulatory, government, or law enforcement agencies and, if so, when the notification was provided.
-- A description of the specific types of information acquired without authorization.
-- The period during which the information system was compromised by the cybersecurity event.
-- The number of total consumers in the State affected by the cybersecurity event, as estimated, with an update to this estimate included with each subsequent report to the Director.
-- The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed.
-- A description of efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur.

-- A copy of the licensee's privacy policy and a statement outlining the steps the licensee would take to investigate and notify consumers affected by the cybersecurity event.
-- The name of a contact person who was both familiar with the cybersecurity event and authorized to act for the licensee.

For a cybersecurity event in a system maintained by a third-party service provider, of which the licensee had become aware, the licensee would have to treat the event as it would under these provisions unless the third-party service provider provided the notice required to the Director. The computation of the licensee's deadlines would begin on the day after the third-party service provider notified the licensee of the cybersecurity event or the licensee otherwise had actual knowledge of the cybersecurity event, whichever was earlier. The bill would not prevent or abrogate an agreement between a licensee and another licensee, a third-party service provider, or any other party to fulfill any of the investigation requirements or notice requirements.

For a cybersecurity event involving nonpublic information that was used by the licensee that was acting as an assuming insurer or in the possession, custody, or control of a licensee that was acting as an assuming insurer and that did not have a direct contractual relationship with the affected consumers, the assuming insurer would have to notify its affected ceding insurers and the director of its state of domicile within 10 business days after making the determination that a cybersecurity event had occurred. The ceding insurers that had a direct contractual relationship with affected consumers would have to fulfill the consumer notification requirements. For a cybersecurity event involving nonpublic information that was in the possession, custody, or control of a third-party service provider of a licensee that was an assuming insurer, the assuming insurer would have to notify its affected ceding insurers and the director of its state of domicile within 10 business days after receiving notice from its third-party service provider that a cybersecurity event had occurred. The ceding insurers that had a direct contractual relationship with affected consumers would have to fulfill the consumer notification requirements imposed under Chapter 5A.

A licensee acting as an assuming insurer would not have other notice obligations relating to a cybersecurity event or other data breach or any other law of the State.

For a cybersecurity event involving nonpublic information that was in the possession, custody, or control of a licensee that was an insurer or its third-party service provider for which a consumer accessed the insurer's services through an independent insurance producer, and for which consumer notice was required, the insurer would have to notify the producers of record of all affected consumers of the cybersecurity event not later than the time at which notice was provided to the affected consumers. The insurer would be excused from this obligation for any producer who was not authorized by law or contract to sell, solicit, or negotiate on behalf of the insurer, and in those instances in which the insurer did not have the current producer of record information for any individual consumer.

Notice to Residents

Unless the licensee determined that the security breach had not or was not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents of the State, a licensee that owned or licensed data that were included in a database that discovered a security breach, or received notice of a breach, would have to provide a notice of the breach to each resident of the State who met one or more of the following:

-- That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person.

-- That resident's personal information was accessed and acquired in encrypted form by a licensee with unauthorized access to the encryption key.

Unless the licensee determined that the security breach had not or was not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents of the State, a licensee that maintained a database that included data that the licensee did not own or license that discovered a breach of the security of the database would have to provide a notice to the owner or licensor of the information of the breach.

In determining whether a security breach was not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more State residents, a licensee would have to act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances.

A licensee would have to provide any notice required these provisions without unreasonable delay. A licensee could delay providing notice without violating this requirement if either of the following were met:

-- A delay was necessary in order for the licensee to take any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database.
-- A law enforcement agency determined and advised the licensee that providing a notice would impede a criminal or civil investigation or would jeopardize homeland or national security.

However, in either case, the licensee would have to provide the notice required without unreasonable delay after the licensee completed those measures or the law enforcement agency determined that providing the notice would no longer impede the investigation or jeopardize homeland or national security.

A licensee would have to provide any notice required under these provisions by providing one or more of the following to the recipient:

-- Written notice sent to the recipient at the recipient's postal address in the licensee's records.
-- Written notice sent electronically to the recipient if any of the following were met: 1) the recipient had expressly consented to receive electronic notice, 2) the licensee had an existing business relationship with the recipient that included periodic electronic mail (e-mail) communications and, based on those communications, the licensee reasonably believed that it had the recipient's current e-mail address, or 3) the licensee conducted its business primarily through internet account transactions or on the internet.
-- If not otherwise prohibited by State or Federal law, notice given by telephone by an individual who represented the licensee if all of the following were met: 1) the notice was not given in whole or in part by use of a recorded message, and 2) the recipient had expressly consented to receive notice by telephone, or if the recipient had not consented, the licensee also provided notice if the notice by telephone did not result in a live conversation between the individual representing the licensee and the recipient within three business days after the initial attempt to provide telephonic notice.
-- Substitute notice, if the licensee demonstrated that the cost of providing notice under these provisions would exceed $250,000 or that the licensee had to provide notice to more than 500,000 residents of the State.

A licensee would provide substitute notice by doing all of the following:

-- If the licensee had e-mail addresses for any of the residents of the State who were entitled to receive the notice, providing electronic notice to those residents.
-- If the licensee maintained a website, conspicuously posting the notice on that website.
-- Notifying major statewide media, and including a telephone number or a website address that a person could use to obtain additional assistance and information.

Certain notices described above would have to meet further criteria under Chapter 5A. A notice under these provisions also would have to do all of the following:

-- Describe the security breach in general terms.
-- Describe the type of personal information that was the subject of the unauthorized access or use.
-- If applicable, generally describe what the licensee providing the notice had done to protect data from further security breaches.
-- Include a telephone number where a notice recipient could obtain assistance or additional information.
-- Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft.

A licensee could provide any notice required under these provisions under an agreement between the licensee and another licensee, if the notice provided under the agreement did not conflict with these provisions.

Except as otherwise provided, after a licensee provided a notice under these provisions, it would have to notify each consumer reporting agency that compiled and maintained files on consumers on a nationwide basis of the security breach without unreasonable delay. The notification would have to include the number of notices that the licensee provided to residents of the State and the timing of those notices. This would not apply if either of the following were met:

-- The licensee was required to provide notice of a security breach to 1,000 or fewer residents of the State.
-- The licensee was subject to 15 USC 6801 to 6809 (which governs the protection of nonpublic personal information).

A licensee that was subject to and complied with the Health Insurance Portability and Accountability Act (HIPAA), and with regulations promulgated under that Act, 45 CFR Parts 160 and 164, for the prevention of unauthorized access to customer information and customer notice would be considered to be in compliance with these provisions.

(45 CFR Part 160 concerns general administrative requirements regarding administrative data standards. Part 164 governs certain security and privacy standards for protected health information.)

Violations & Penalties

A person who provided notice of a security breach in the manner described in these provisions when a breach had not occurred, with the intent to defraud, would be guilty of a misdemeanor punishable as follows:

-- Except as otherwise provided, by up to 53 days' imprisonment or a fine of not more than $250 for each violation, or both.
-- For a second violation, by up to 93 days' imprisonment or a fine of not more than $500 for each violation, or both.

-- For a third or subsequent violation, by up to 93 days' imprisonment or a fine of not more than $750 for each violation, or both.

A person who knowingly failed to provide a notice of a security breach as described in these provisions would be ordered to pay a civil fine of not more than $250 for each failure to provide notice. The Attorney General or a prosecuting attorney could bring an action to recover a civil fine under these provisions. The aggregate liability of a person for civil fines for multiple violations that arose from the same security breach could not exceed $750,000.

These provisions do not affect the availability of any civil remedy for a violation of State or Federal law. These provisions apply to the discovery or notification of a breach of the security of a database that occurred after December 31, 2019.

These provisions would not apply to the access or acquisition by a person or agency of Federal, State, or local government records or documents lawfully made available to the general public.

In addition, these provisions deal with subject matter that was of statewide concern, and any charter, ordinance, resolution, regulation, rule, or other action by a municipal corporation or other political subdivision of the State to regulate, directly or indirectly, any matter expressly set forth in these provisions would be preempted.

Director Duties

Any documents, materials, or other information in the control or possession of DIFS that was furnished by a licensee or its employee or agent acting on its behalf under certain provisions of Chapter 5A, or that was obtained by the Director in an investigation or examination would be confidential by law and privileged, would not be subject to the Freedom of Information Act, would not be subject to subpoena or discorvery, and would not be admissible in evidence in any private civil action. However, the Director would be authorized to use the documents, materials, or other information in the furtherance of any regulatory or legal action brought as a part of the Director's duties. The Director would have to not make the documents, materials, or other information public without the prior written consent of the licensee.

Neither the Director nor any person that received documents, materials, or other information while acting under his or her authority would be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information.

To assist in the performance of the Director's duties under the bill, the Director could do any of the following:

-- Share documents, materials, or other information, including confidential and privileged documents, materials, or information, with other State, Federal, and international regulatory agencies, with the National Association of Insurance Commissioners (NAIC), its affiliates, or its subsidiaries, and with State, Federal, and international law enforcement authorities, if the recipient agreed in writing to maintain the confidentiality and privileged status of the document, material, or other information.
-- Receive documents, materials, or information, including otherwise confidential and privileged documents, materials, or information, from the NAIC, its affiliates, or its subsidiaries, and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and maintain as confidential or privileged any document, material, or information received with notice or the understanding that it was confidential or privileged under the laws of the jurisdiction that was the source of the document, material, or information.

-- Share documents, materials, or other information with a third-party consultant or vendor if the consultant agreed in writing to maintain the confidentiality and privileged status of the document, material, or other information.
-- Enter into agreements governing sharing and use of information consistent with these provisions.

A waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information would not occur as a result of disclosure to the Director under these provisions or as a result of sharing as authorized above.

Chapter 5A would not prohibit the Director from releasing final, adjudicated actions that were open to public inspection under the Freedom of Information Act to a database or other clearinghouse service maintained by the NAIC, its affiliates, or its subsidiaries.

Any documents, materials, or other information in the possession or control of the NAIC or a third-party consultant or vendor would be confidential by law and privileged, would not be subject to the Freedom of Information Act, would not be subject to subpoena or discovery, and would not admissible in evidence in any private civil action.

Exempt Entities

A licensee that met any of the following criteria would be exempt from Chapter 5A's requirement to develop, implement, and maintain a comprehensive written information security program, among other things listed above:

-- The licensee had fewer than 50 employees, including any independent contractors.
-- The licensee had less than $10.0 million in gross annual revenue.
-- The licensee had less than $25.0 million in year-end total assets.

If a licensee ceased to qualify for an exception listed above, the licensee would have 180 days to comply with Chapter 5A.

A licensee subject to and in compliance with the HIPPA and with regulations promulgated under that Act, would not be required to comply with Chapter 5A except for certain requirements pertaining to notification of a cybersecurity event or breach.

An employee, agent, representative, or designee of a licensee, who was also a licensee, would be exempt from Chapter 5A's requirement to develop, implement, and maintain a comprehensive written information security program, among other things listed above, and would not need to develop its own information security program to the extent that the employee, agent, representative, or designee was covered by the information security program of the other licensee.

Legislative Analyst: Drew Krogulecki

FISCAL IMPACT

The bill would have an indeterminate negative fiscal impact on the Department of Insurance and Financial Services (DIFS). The bill creates a number of responsibilities for the DIFS Director that could result in increased administrative costs. However, the magnitude of these costs would be highly dependent on the number of licensees who experienced security events prompting review and action by DIFS. Existing appropriations likely would be to cover the majority of these costs.

Otherwise, the bill would have no fiscal impact on the State or local government. Licensed insurers are currently subject to the Identity Theft Protection Act. Per MCL 445.72, 445.72a, and 445.72b, all misdemeanor offenses and civil fines outlined in the bill would remain the same as current law.

Fiscal Analyst: Elizabeth Raczkowski
Abbey Frazier

SAS\S1718\s6491sa