Act No. 690
Public Acts of 2018
Approved by the Governor
December 28, 2018

Filed with the Secretary of State
December 28, 2018

EFFECTIVE DATE: January 20, 2021

STATE OF MICHIGAN
99TH LEGISLATURE
REGULAR SESSION OF 2018

Introduced by Rep. Theis

ENROLLED HOUSE BILL No. 6491

AN ACT to amend 1956 PA 218, entitled "An act to revise, consolidate, and classify the laws relating to the insurance and surety business; to regulate the incorporation or formation of domestic insurance and surety companies and associations and the admission of foreign and alien companies and associations; to provide their rights, powers, and immunities and to prescribe the conditions on which companies and associations organized, existing, or authorized under this act may exercise their powers; to provide the rights, powers, and immunities and to prescribe the conditions on which other persons, firms, corporations, associations, risk retention groups, and purchasing groups engaged in an insurance or surety business may exercise their powers; to provide for the imposition of a privilege fee on domestic insurance companies and associations and the state accident fund; to provide for the imposition of a tax on the business of foreign and alien companies and associations; to provide for the imposition of a tax on risk retention groups and purchasing groups; to provide for the imposition of a tax on the business of surplus line agents; to provide for the imposition of regulatory fees on certain insurers; to provide for assessment fees on certain health maintenance organizations; to modify tort liability arising out of certain accidents; to provide for limited actions with respect to that modified tort liability and to prescribe certain procedures for maintaining those actions; to require security for losses arising out of certain accidents; to provide for the continued availability and affordability of automobile insurance and homeowners insurance in this state and to facilitate the purchase of that insurance by all residents of this state at fair and reasonable rates; to provide for certain reporting with respect to insurance and with respect to certain claims against uninsured or self-insured persons; to prescribe duties for certain state departments and officers with respect to that reporting; to provide for certain assessments; to establish and continue certain state insurance funds; to modify and clarify the status, rights, powers, duties, and operations of the nonprofit malpractice insurance fund; to provide for the departmental supervision and regulation of the insurance and surety business within this state; to provide for regulation over worker's compensation self-insurers; to provide for the conservation, rehabilitation, or liquidation of unsound or insolvent insurers; to provide for the protection of policyholders, claimants, and creditors of unsound or insolvent insurers; to provide for associations of insurers to protect policyholders and claimants in the event of insurer insolvencies; to prescribe educational requirements for insurance agents and solicitors; to provide for the regulation of multiple employer welfare arrangements; to create an automobile theft prevention authority to reduce the number of automobile thefts in this state; to prescribe the powers and duties of the automobile theft prevention authority; to provide certain powers and duties upon certain officials, departments, and authorities of this state; to provide for an appropriation; to repeal acts and parts of acts; and to provide penalties for the violation of this act," (MCL 500.100 to 500.8302) by adding chapter 5A.

The People of the State of Michigan enact:

CHAPTER 5A

DATA SECURITY

Sec. 550. This chapter does not create or imply a private cause of action for violation of its provisions and does not curtail a private cause of action that would otherwise exist in the absence of this chapter. Notwithstanding any other provision of law, this chapter establishes the exclusive standards, for this state, applicable to licensees for data security, the investigation of a cybersecurity event, and notification to the director.

Sec. 553. As used in this chapter:

(a) "Authorized individual" means 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.

(b) "Consumer" means an individual, including, but not limited to, an applicant, a policyholder, an insured, a beneficiary, a claimant, and a certificate holder, who is a resident of this state and whose nonpublic information is in a licensee's possession, custody, or control.

(c) "Cybersecurity event" means 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 does not include either of the following:

(i) The unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization.

(ii) The unauthorized access to data by a person if the access meets both of the following criteria:

(A) The person acted in good faith in accessing the data.

(B) The access was related to activities of the person.

(d) "Encrypted" means 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.

(e) "Information security program" means 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.

(f) "Information system" means 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.

(g) "Licensee" means a licensed insurer or producer, and other persons licensed or required to be licensed, authorized, or registered, or holding or required to hold a certificate of authority under this act. Licensee does not include a purchasing group or a risk retention group chartered and licensed in a state other than this state or a person that is acting as an assuming insurer that is domiciled in another state or jurisdiction.

(h) "Multi-factor authentication" means authentication through verification of at least 2 of the following types of authentication factors:

(i) Knowledge factors, such as a password.

(ii) Possession factors, such as a token or text message on a mobile phone.

(iii) Inherence factors, such as a biometric characteristic.

(i) "Nonpublic information" means electronic information that is not publicly available information and is any of the following:

(i) Business-related information of a licensee, the tampering with which, or unauthorized disclosure, access, or use of which, would cause a material adverse impact to the business, operations, or security of the licensee.

(ii) 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 1 or more of the following data elements:

(A) Social Security number.

(B) Driver license number or nondriver identification card number.

(C) Financial account number, or credit or debit card number.

(D) Any security code, access code, or password that would permit access to a consumer's financial account.

(E) Biometric records.

(iii) 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:

(A) The past, present, or future physical, mental, or behavioral health or condition of any consumer or a member of the consumer's family.

(B) The provision of health care to any consumer.

(C) Payment for the provision of health care to any consumer.

(j) "Publicly available information" means 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 has a reasonable basis to believe that information is lawfully made available to the general public if both of the following apply:

(i) The licensee has taken steps to determine that the information is of the type that is available to the general public.

(ii) If an individual can direct that the information not be made available to the general public, that the licensee's consumer has not directed that the information not be made available to the general public.

(k) "Risk assessment" means the risk assessment that each licensee is required to conduct under section 555(3).

(l) "Third-party service provider" means 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.

Sec. 555. (1) Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's 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, each licensee shall develop, implement, and maintain a comprehensive written information security program, based on the licensee's risk assessment, that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

(2) A licensee's information security program must be designed to do all of the following:

(a) Protect the security and confidentiality of nonpublic information and the security of the information system.

(b) Protect against any threats or hazards to the security or integrity of nonpublic information and the information system.

(c) Protect against unauthorized access to or use of nonpublic information, and minimize the likelihood of harm to any consumer.

(d) Maintain policies and procedures for the secure disposal on a periodic basis of any nonpublic information that is no longer necessary for business operations or for other legitimate business purposes.

(3) A licensee shall do all of the following:

(a) Designate 1 or more employees, an affiliate, or an outside vendor to act on behalf of the licensee that is responsible for the information security program.

(b) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers.

(c) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the nonpublic information.

(d) 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, including all of the following:

(i) Employee training and management.

(ii) Information systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal.

(iii) Detecting, preventing, and responding to attacks, intrusions, or other systems failures.

(e) 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.

(4) Based on its risk assessment, a licensee shall do all of the following:

(a) Design its information security program to mitigate the identified risks, commensurate with the size and complexity of the licensee, the nature and scope of the licensee's 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.

(b) Determine which of the following security measures are appropriate and implement those appropriate security measures:

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

(ii) Identifying and managing the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy.

(iii) Restricting physical access to nonpublic information to authorized individuals only.

(iv) 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.

(v) Adopting secure development practices for in-house developed applications utilized by the licensee.

(vi) Adding procedures for evaluating, assessing, or testing the security of externally developed applications used by the licensee.

(vii) Modifying the information system in accordance with the licensee's information security program.

(viii) Using effective controls, which may include multi-factor authentication procedures for employees accessing nonpublic information.

(ix) Regularly testing and monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems.

(x) Including audit trails within the information security program designed to detect and respond to cybersecurity events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee.

(xi) Implementing measures to protect against destruction, loss, or damage of nonpublic information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures.

(xii) Developing, implementing, and maintaining procedures for the secure disposal of nonpublic information in any format.

(c) Include cybersecurity risks in the licensee's enterprise risk management process.

(d) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared.

(e) Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in the risk assessment.

(5) If a licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum, do all of the following:

(a) Require the licensee's executive management or its delegates to develop, implement, and maintain the licensee's information security program.

(b) Require the licensee's executive management or its delegates to report in writing, at least annually, all of the following information:

(i) The overall status of the information security program and the licensee's compliance with this chapter.

(ii) 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 subparagraph, and recommendations for changes in the information security program.

(iii) If executive management delegates any of its responsibilities under this section, it shall oversee the development, implementation, and maintenance of the licensee's information security program prepared by a delegate and shall receive a report from the delegate complying with the requirements of the report to the board of directors.

(6) A licensee shall exercise due diligence in selecting its third-party service provider. A licensee shall 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.

(7) A licensee shall 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 the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

(8) As part of its information security program, each licensee shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromises 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 under this subsection must address all of the following areas:

(a) The internal process for responding to a cybersecurity event.

(b) The goals of the incident response plan.

(c) The definition of clear roles, responsibilities, and levels of decision-making authority.

(d) External and internal communications and information sharing.

(e) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls.

(f) Documentation and reporting regarding cybersecurity events and related incident response activities.

(g) The evaluation and revision as necessary of the incident response plan following a cybersecurity event.

(9) By February 15 of each year, each insurer domiciled in this state shall submit to the director a written statement, certifying that the insurer is in compliance with the requirements of this section. Each insurer shall maintain for examination by the department all records, schedules, and data supporting this certificate for 5 years. To the extent an insurer has identified areas, systems, or processes that require material improvement, updating, or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address the areas, systems, or processes. The documentation described in this subsection must be available for inspection by the director.

Sec. 557. (1) If the licensee learns that a cybersecurity event has or may have occurred, the licensee or an outside vendor or service provider, or both, designated to act on behalf of the licensee, shall conduct a prompt investigation.

(2) During the investigation under subsection (1), the licensee, or an outside vendor or service provider, or both, designated to act on behalf of the licensee, shall, at a minimum, do as much of the following as possible:

(a) Determine whether a cybersecurity event has occurred.

(b) Assess the nature and scope of the cybersecurity event.

(c) Identify any nonpublic information that may have been involved in the cybersecurity event.

(d) 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.

(3) The licensee shall maintain records concerning all cybersecurity events for at least 5 years from the date of the cybersecurity event and shall produce those records on demand of the director.

Sec. 559. (1) Each licensee shall 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 is in the possession of a licensee has occurred when either of the following criteria has been met:

(a) This state is the licensee's state of domicile, for an insurer, or this state is the licensee's home state, for an insurance producer as that term is defined in section 1201, and the cybersecurity event has a reasonable likelihood of materially harming either of the following:

(i) A consumer residing in this state.

(ii) Any material part of a normal operation of the licensee.

(b) The licensee reasonably believes that the nonpublic information involved is of 250 or more consumers residing in this state and is either of the following:

(i) A cybersecurity event impacting the licensee of which notice is required to be provided to any government body, self-regulatory agency, or other supervisory body under any state or federal law.

(ii) A cybersecurity event that has a reasonable likelihood of materially harming either of the following:

(A) Any consumer residing in this state.

(B) Any material part of the normal operation of the licensee.

(2) The licensee shall provide the information under this subsection in electronic form as directed by the director. The licensee has a continuing obligation to update and supplement initial and subsequent notifications to the director regarding material changes to previously provided information relating to the cybersecurity event. The licensee shall provide as much of the following information as possible:

(a) The date of the cybersecurity event.

(b) 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.

(c) How the cybersecurity event was discovered.

(d) Whether any lost, stolen, or breached information has been recovered and, if so, how this was done.

(e) The identity of the source of the cybersecurity event.

(f) Whether the licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when the notification was provided.

(g) A description of the specific types of information acquired without authorization. As used in this subdivision, "specific types of information" means particular data elements including, for example, types of medical information, types of financial information, or types of information allowing identification of the consumer.

(h) The period during which the information system was compromised by the cybersecurity event.

(i) The number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the director and update this estimate with each subsequent report to the director under this section.

(j) 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.

(k) A description of efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur.

(l) A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event.

(m) The name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.

(3) A licensee shall comply with this chapter, as applicable, and provide a copy of the notice sent to consumers under this chapter, if a licensee is required to notify the director under section 559.

(4) For a cybersecurity event in a system maintained by a third-party service provider, of which the licensee has become aware, the licensee shall treat the event as it would under this section. The computation of the licensee's deadlines begins on the day after the third-party service provider notifies the licensee of the cybersecurity event or the licensee otherwise has actual knowledge of the cybersecurity event, whichever is earlier. This chapter does 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 imposed under section 557 or notice requirements imposed under this section.

(5) For a cybersecurity event involving nonpublic information that is used by the licensee that is acting as an assuming insurer or in the possession, custody, or control of a licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected consumers, the assuming insurer shall 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 has occurred. The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under this section. For a cybersecurity event involving nonpublic information that is in the possession, custody, or control of a third-party service provider of a licensee that is an assuming insurer, the assuming insurer shall 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 has occurred. The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under this chapter.

(6) A licensee acting as an assuming insurer does not have other notice obligations relating to a cybersecurity event or other data breach under this section or any other law of this state.

(7) For a cybersecurity event involving nonpublic information that is in the possession, custody, or control of a licensee that is 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 is required under this chapter, the insurer shall notify the producers of record of all affected consumers of the cybersecurity event not later than the time at which notice is provided to the affected consumers. The insurer is excused from this obligation for any producer who is not authorized by law or contract to sell, solicit, or negotiate on behalf of the insurer, and in those instances in which the insurer does not have the current producer of record information for any individual consumer.

Sec. 561. (1) Unless the licensee determines that the cybersecurity event has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a licensee that owns or licenses data that are included in a database that discovers a cybersecurity event, or receives notice of a cybersecurity event under subsection (2), shall provide a notice of the cybersecurity event to each resident of this state who meets 1 or more of the following:

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

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

(2) Unless the licensee determines that the cybersecurity event has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a licensee that maintains a database that includes data that the licensee does not own or license that discovers a breach of the security of the database shall provide a notice to the owner or licensor of the information of the cybersecurity event.

(3) In determining whether a cybersecurity event is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state under subsection (1) or (2), a licensee shall act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances.

(4) A licensee shall provide any notice required under this section without unreasonable delay. A licensee may delay providing notice without violating this subsection if either of the following is met:

(a) A delay is necessary in order for the licensee to take any measures necessary to determine the scope of the cybersecurity event and restore the reasonable integrity of the database. However, the licensee shall provide the notice required under this subsection without unreasonable delay after the licensee completes the measures necessary to determine the scope of the cybersecurity event and restore the reasonable integrity of the database.

(b) A law enforcement agency determines and advises the licensee that providing a notice will impede a criminal or civil investigation or jeopardize homeland or national security. However, the licensee shall provide the notice required under this section without unreasonable delay after the law enforcement agency determines that providing the notice will no longer impede the investigation or jeopardize homeland or national security.

(5) A licensee shall provide any notice required under this section by providing 1 or more of the following to the recipient:

(a) Written notice sent to the recipient at the recipient's postal address in the records of the licensee.

(b) Written notice sent electronically to the recipient if any of the following are met:

(i) The recipient has expressly consented to receive electronic notice.

(ii) The licensee has an existing business relationship with the recipient that includes periodic electronic mail communications and based on those communications the licensee reasonably believes that it has the recipient's current electronic mail address.

(iii) The licensee conducts its business primarily through internet account transactions or on the internet.

(c) If not otherwise prohibited by state or federal law, notice given by telephone by an individual who represents the licensee if all of the following are met:

(i) The notice is not given in whole or in part by use of a recorded message.

(ii) The recipient has expressly consented to receive notice by telephone, or if the recipient has not expressly consented to receive notice by telephone, the licensee also provides notice under subdivision (a) or (b) if the notice by telephone does not result in a live conversation between the individual representing the licensee and the recipient within 3 business days after the initial attempt to provide telephonic notice.

(d) Substitute notice, if the licensee demonstrates that the cost of providing notice under subdivision (a), (b), or (c) will exceed $250,000.00 or that the licensee has to provide notice to more than 500,000 residents of this state. A licensee provides substitute notice under this subdivision by doing all of the following:

(i) If the licensee has electronic mail addresses for any of the residents of this state who are entitled to receive the notice, providing electronic notice to those residents.

(ii) If the licensee maintains a website, conspicuously posting the notice on that website.

(iii) Notifying major statewide media. A notification under this subparagraph must include a telephone number or a website address that a person may use to obtain additional assistance and information.

(6) A notice under this section must do all of the following:

(a) For a notice provided under subsection (5)(a) or (b), be written in a clear and conspicuous manner and contain the content required under subdivisions (c) to (g).

(b) For a notice provided under subsection (5)(c), clearly communicate the content required under subdivisions (c) to (g) to the recipient of the telephone call.

(c) Describe the cybersecurity event in general terms.

(d) Describe the type of personal information that is the subject of the unauthorized access or use.

(e) If applicable, generally describe what the licensee providing the notice has done to protect data from further security breaches.

(f) Include a telephone number where a notice recipient may obtain assistance or additional information.

(g) Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft.

(7) A licensee may provide any notice required under this section under an agreement between the licensee and another licensee, if the notice provided under the agreement does not conflict with this section.

(8) Except as provided in this subsection, after a licensee provides a notice under this section, the licensee shall notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the cybersecurity event without unreasonable delay. A notification under this subsection must include the number of notices that the licensee provided to residents of this state and the timing of those notices. This subsection does not apply if either of the following is met:

(a) The licensee is required under this section to provide notice of a cybersecurity event to 1,000 or fewer residents of this state.

(b) The licensee is subject to 15 USC 6801 to 6809.

(9) A licensee that is subject to and complies with the health insurance portability and accountability act of 1996, Public Law 104-191, 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 is considered to be in compliance with this section.

(10) A person that provides notice of a cybersecurity event in the manner described in this section when a cybersecurity event has not occurred, with the intent to defraud, is guilty of a misdemeanor punishable as follows:

(a) Except as otherwise provided under subdivisions (b) and (c), by imprisonment for not more than 93 days or a fine of not more than $250.00 for each violation, or both.

(b) For a second violation, by imprisonment for not more than 93 days or a fine of not more than $500.00 for each violation, or both.

(c) For a third or subsequent violation, by imprisonment for not more than 93 days or a fine of not more than $750.00 for each violation, or both.

(11) Subject to subsection (12), a person that knowingly fails to provide a notice of a cybersecurity event required under this section may be ordered to pay a civil fine of not more than $250.00 for each failure to provide notice. The attorney general or a prosecuting attorney may bring an action to recover a civil fine under this section.

(12) The aggregate liability of a person for civil fines under subsection (11) for multiple violations of subsection (11) that arise from the same cybersecurity event must not exceed $750,000.00.

(13) Subsections (10) and (11) do not affect the availability of any civil remedy for a violation of state or federal law.

(14) This section applies to the discovery or notification of a breach of the security of a database that occurs after December 31, 2019.

(15) This section does 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.

(16) This section deals with subject matter that is of statewide concern, and any charter, ordinance, resolution, regulation, rule, or other action by a municipal corporation or other political subdivision of this state to regulate, directly or indirectly, any matter expressly set forth in this section is preempted.

(17) As used in this section:

(a) "Data" means computerized information.

(b) "Identity theft" means a person doing any of the following:

(i) With intent to defraud or violate the law, using or attempting to use the personal information of another person to do either of the following:

(A) Obtain credit, goods, services, money, property, a vital record, a confidential telephone record, medical records or information, or employment.

(B) Commit another unlawful act.

(ii) By concealing, withholding, or misrepresenting the person's identity, using or attempting to use the personal information of another person to do either of the following:

(A) Obtain credit, goods, services, money, property, a vital record, a confidential telephone record, medical records or information, or employment.

(B) Commit another unlawful act.

(c) "Personal information" means the first name or first initial and last name linked to 1 or more of the following data elements of a resident of this state:

(i) A Social Security number.

(ii) A driver license number or state personal identification card number.

(iii) A demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts.

Sec. 563. (1) Any documents, materials, or other information in the control or possession of the department that is furnished by a licensee or an employee or agent of the licensee acting on behalf of the licensee under section 555(9), section 559(2)(b), (c), (d), (e), (h), (i), and (j), or that is obtained by the director in an investigation or examination by the director is confidential by law and privileged, is not subject to the freedom of information act, 1976 PA 442, MCL 15.231 to 15.246, is not subject to subpoena, and is not subject to discovery or admissible in evidence in any private civil action. However, the director is 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 shall not otherwise make the documents, materials, or other information public.

(2) Neither the director nor any person that received documents, materials, or other information while acting under the authority of the director is permitted or required to testify in any private civil action concerning any confidential documents, materials, or information under subsection (1).

(3) To assist in the performance of the director's duties under this chapter, the director may do any of the following:

(a) Share documents, materials, or other information, including the confidential and privileged documents, materials, or information subject to subsection (1), with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates, or its subsidiaries, and with state, federal, and international law enforcement authorities, if the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information.

(b) Receive documents, materials, or information, including otherwise confidential and privileged documents, materials, or information, from the National Association of Insurance Commissioners, its affiliates, or its subsidiaries, and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material, or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material, or information.

(c) Share documents, materials, or other information subject to subsection (1) with a third-party consultant or vendor if the consultant agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information.

(d) Enter into agreements governing sharing and use of information consistent with this subsection.

(4) A waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information does not occur as a result of disclosure to the director under this section or as a result of sharing as authorized under subsection (3).

(5) This chapter does not prohibit the director from releasing final, adjudicated actions that are open to public inspection pursuant to the freedom of information act, 1976 PA 442, MCL 15.231 to 15.246, to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates, or its subsidiaries.

(6) Any documents, materials, or other information in the possession or control of the National Association of Insurance Commissioners or a third-party consultant or vendor under this chapter is confidential by law and privileged, is not subject to the freedom of information act, 1976 PA 442, MCL 15.231 to 15.246, is not subject to subpoena, and is not subject to discovery or admissible in evidence in any private civil action.

Sec. 565. (1) A licensee that has fewer than 25 employees, including any independent contractors, is exempt from section 555.

(2) A licensee subject to and in compliance with the health insurance portability and accountability act of 1996, Public Law 104-191, and with regulations promulgated under that act, is not required to comply with this chapter except for the requirements under sections 559 and 561.

(3) An employee, agent, representative, or designee of a licensee, who is also a licensee, is exempt from section 555 and does not need to develop its own information security program to the extent that the employee, agent, representative, or designee is covered by the information security program of the other licensee.

(4) If a licensee ceases to qualify for the exception under subsection (1), the licensee has 180 days to comply with this chapter.

(5) This chapter takes effect on January 20, 2021. A licensee shall implement section 555 by January 20, 2022. However, a licensee has until January 20, 2023 to implement section 555(6).

Enacting section 1. This amendatory act does not take effect unless House Bill No. 6406 of the 99th Legislature is enacted into law.

Gary L Randall

Clerk of the House of Representatives

Jeffrey L Cobb

Secretary of the Senate

Approved ....

....

Governor

Compiler's note: House Bill No. 6406, referred to in enacting section 1, was filed with the Secretary of State December 28, 2018, and became 2018 PA 649, Eff. Jan. 20, 2020.