HOUSE BILL NO. 6268

December 10, 2024, Introduced by Reps. McKinney, Grant, McFall and Scott and referred to the Committee on Insurance and Financial Services.

A bill to amend 1956 PA 218, entitled

"The insurance code of 1956,"

by amending sections 553, 561, and 563 (MCL 500.553, 500.561, and 500.563), as added by 2018 PA 690, and by adding sections 564 and 564a.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

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~~ **access** 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.~~

(*ii*) ~~(B) The access was related to activities of the person.~~**An event in which the licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.**

(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. 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),~~ **A licensee** shall provide a notice of ~~the~~ **a** 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~~ **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.~~

(3) ~~(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.

(4) ~~(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.

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

(a) For a notice provided under subsection ~~(5)(a)~~ **(4)(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),~~ **(4)(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.

(6) ~~(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.

(7) ~~(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.

(8) ~~(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.

(9) ~~(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.

(10) ~~(11)~~ Subject to subsection ~~(12),~~ **(11)**, 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.

(11) ~~(12)~~ The aggregate liability of a person for civil fines under subsection ~~(11)~~ **(10)** for multiple violations of subsection ~~(11)~~ **(10)** that arise from the same cybersecurity event must not exceed $750,000.00.

(12) ~~(13)~~ Subsections ~~(10)~~ **(9)** and ~~(11)~~ **(10)** do not affect the availability of any civil remedy for a violation of state or federal law.

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

(14) ~~(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.

(15) ~~(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.

(16) ~~(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), **and (k)**, 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~~ **under** 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. 564. (1) Except as otherwise provided in this subsection, the director may examine and investigate the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of this chapter. This power is in addition to the other powers the director has under this act. Any examination or investigation of a licensee under this section must be conducted in accordance with section 222.

(2) If the director believes that a licensee has been or is engaged in conduct in this state that violates this chapter, the director may take action that is necessary or appropriate to enforce this chapter.

Sec. 564a. If a licensee violates this chapter, the licensee may be subject to fines under section 150.