SUBSTITUTE FOR

HOUSE BILL NO. 4187

A bill to require certain entities to provide notice to certain persons in the event of a breach of security that results in the unauthorized acquisition of sensitive personally identifying information; to provide for the powers and duties of certain state governmental officers and entities; and to prescribe penalties and provide remedies.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

Sec. 1. This act shall be known and may be cited as the "data breach notification act".

Sec. 3. As used in this act:

(a) "Breach of security" or "breach" means the unauthorized acquisition of sensitive personally identifying information in electronic form, if that acquisition is reasonably likely to cause

substantial risk of identity theft or fraud to the state residents to whom the information relates. Acquisition that occurs over a period of time that is committed by the same entity constitutes 1 breach. The term does not include any of the following:

(*i*) A good-faith acquisition of sensitive personally identifying information by an employee or agent of a covered entity, unless the information is used for a purpose unrelated to the business of the covered entity or is subject to further unauthorized use.

(*ii*) A release of a public record that is not otherwise subject to confidentiality or nondisclosure requirements.

(*iii*) An acquisition or release of data in connection with a lawful investigative, protective, or intelligence activity of a law enforcement or intelligence agency of this state or a political subdivision of this state.

(b) "Covered entity" means an individual or a sole proprietorship, partnership, government entity, corporation, limited liability company, nonprofit, trust, estate, cooperative association, or other business entity, that has more than 50 employees and owns or licenses sensitive personally identifying information, or a franchisee of any of the foregoing. The term also includes a state agency.

(c) "Data in electronic form" means any data that is stored electronically on a computer system, database, or other technology, including, but not limited to, recordable tapes and other mass storage devices. As used in this subdivision, "electronically" means a method using electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(d) Except as provided in subdivision (e), "sensitive

personally identifying information" means either of the following:

(*i*) A state resident's first name or first initial, and last name, in combination with 1 or more of the following data elements that relate to that state resident:

(A) A nontruncated Social Security number.

(B) A nontruncated driver license number, enhanced driver license number, state personal identification card number, enhanced state personal identification card number, passport number, military identification number, or other unique identification number issued on a government document that is used to verify the identity of a specific individual.

(C) A financial account number, including, but not limited to, a bank account number, credit union account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, PIN, or similar security information, that is necessary to access the financial account or to conduct a transaction that will result in a credit or debit to the financial account.

(D) A state resident's medical or mental history, treatment, or diagnosis issued by a health care professional.

(E) A state resident's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the state resident.

(*ii*) A username or electronic mail address, in combination with a password, security question and answer, or similar information, that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information.

(e) "Sensitive personally identifying information" does not

include any of the following:

(*i*) Information about a state resident that has been lawfully made public by a federal, state, or local government record or a widely distributed media.

(*ii*) Information that is truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify a state resident or that otherwise renders the information unusable, including encryption of the data or device containing the sensitive personally identifying information, unless the covered entity knows or reasonably believes that the encryption key or security credential that could render the personally identifying information readable or usable has been breached together with the information.

(f) "State agency" means an agency, board, bureau, commission, department, division, or office of this state that owns, acquires, maintains, stores, or uses data in electronic form that contains sensitive personally identifiable information.

(g) "State resident" means an individual who is a resident of this state.

(h) "Third-party agent" means an entity that maintains, processes, or is otherwise permitted to access, sensitive personally identifying information in connection with providing services to a covered entity under an agreement with the covered entity.

Sec. 5. (1) Each covered entity and third-party agent shall implement and maintain reasonable security measures designed to protect sensitive personally identifying information against a breach of security.

(2) For purposes of subsection (1), a covered entity shall

consider all of the following in developing its reasonable security measures:

(a) The size of the covered entity.

(b) The amount of sensitive personally identifying information that is owned or licensed by the covered entity and the type of activities for which the sensitive personally identifying information is accessed, acquired, or maintained by or on behalf of the covered entity.

(c) The covered entity's cost to implement and maintain the security measures to protect against a breach of security relative to its resources.

(3) As used in this section, "reasonable security measures" means security measures that are reasonable for a covered entity to implement and maintain, including consideration of all of the following:

(a) Designation of an employee or employees to coordinate the covered entity's security measures to protect against a breach of security. An owner or manager may designate himself or herself for purposes of this subdivision.

(b) Identification of internal and external risks of a breach of security.

(c) Adoption of appropriate information safeguards that are designed to address identified risks of a breach of security and assess the effectiveness of those safeguards.

(d) Retention of service providers, if any, that are contractually required to maintain appropriate safeguards for sensitive personally identifying information.

(e) Evaluation and adjustment of security measures to account for changes in circumstances affecting the security of sensitive

personally identifying information.

Sec. 7. (1) If a covered entity determines that a breach of security has or may have occurred, the covered entity shall conduct a good-faith and prompt investigation that includes all of the following:

(a) An assessment of the nature and scope of the breach.

(b) Identification of any sensitive personally identifying information that was involved in the breach and the identity of any state residents to whom that information relates.

(c) A determination of whether the sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person.

(d) Identification and implementation of measures to restore the security and confidentiality of the systems, if any, compromised in the breach.

(2) In determining whether sensitive personally identifying information has been acquired by an unauthorized person without valid authorization, the following factors may be considered:

(a) Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information.

(b) Indications that the information has been downloaded, copied, or otherwise acquired or transferred by an unauthorized person.

(c) Indications that the information was used in an unlawful manner by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(d) Whether the information was publicly displayed.

Sec. 9. (1) If a covered entity that owns or licenses

sensitive personally identifiable information determines under section 7 that a breach has occurred, the covered entity must provide notice of the breach to each state resident whose sensitive personally identifiable information was acquired in the breach.

(2) A covered entity shall provide notice under subsection (1) to state residents described in subsection (1) as expeditiously as possible and without unreasonable delay. Except as provided in subsection (3), the covered entity shall provide any notice required under this section no later than 45 days after the covered entity completes the measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database.

(3) If a federal or state law enforcement agency determines that notice to state residents required under this section would interfere with a criminal investigation or national security, and delivers a written or electronic request to the covered entity for a delay, a covered entity shall delay providing the notice for a period that the law enforcement agency determines is necessary. If the law enforcement agency determines that an additional delay is necessary, the law enforcement agency shall deliver a written or electronic request to the covered entity for an additional delay, and the covered entity shall delay providing the notice to the date specified in the law enforcement agency's request for additional delay, or extend the delay set forth in the original request for the additional period set forth in the request for additional delay.

(4) Except as provided in subsection (5), a covered entity shall provide notice to a state resident under this section in compliance with 1 of the following, as applicable:

(a) In the case of a breach of security that involves a username or password, in combination with any password or security question and answer that would permit access to an online account, and no other sensitive personally identifying information is involved, the covered entity may comply with this section by providing the notification in electronic or other form that directs the state resident whose sensitive personally identifying information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the covered entity and all other accounts for which the state resident whose sensitive personally identifying information has been breached uses the same username or electronic mail address and password or security question or answer.

(b) In the case of a breach that involves sensitive personally identifying information for login credentials of an electronic mail account furnished by the covered entity, the covered entity shall not comply with this section by providing the notification to that electronic mail address, but may, instead, comply with this section by providing notice by another method described in subdivision (a) or (c), or by providing clear and conspicuous notice delivered to the state resident online if the resident is connected to the online account from an internet protocol address or online location from which the covered entity knows the state resident customarily accesses the account.

(c) Except as provided in subdivision (a) or (b), the covered entity shall comply with this section by providing a notice, in writing, sent to the mailing address of the state resident in the records of the covered entity, or by electronic mail notice sent to

the electronic mail address of the state resident in the records of the covered entity. The notice shall include, at a minimum, all of the following:

(*i*) The date, estimated date, or estimated date range of the breach.

(*ii*) A description of the sensitive personally identifying information that was acquired by an unauthorized person as part of the breach.

(*iii*) A general description of the actions taken by the covered entity to restore the security and confidentiality of the personal information involved in the breach.

(*iv*) A general description of steps a state resident can take to protect himself or herself from identity theft, if the breach creates a risk of identity theft.

(*v*) Contact information that the state resident can use to contact the covered entity to inquire about the breach.

(5) A covered entity that is required to provide notice to any state resident under this section may provide substitute notice in lieu of direct notice, if direct notice is not feasible because of any of the following:

(a) Excessive cost to the covered entity of providing direct notification relative to the resources of the covered entity. For purposes of this subdivision, the cost of direct notification to state residents is considered excessive if it exceeds $250,000.00 or if notice must be provided to more than 500,000 state residents.

(b) Lack of sufficient contact information for the state resident who the covered entity is required to notify.

(6) For purposes of subsection (5), substitute notice must include both of the following:

(a) If the covered entity maintains an internet website, a conspicuous notice posted on the website for a period of at least 30 days.

(b) Notice in print and in broadcast media, including major media in urban and rural areas where the state residents who the covered entity is required to notify reside.

(7) If a covered entity determines that notice is not required under this section, the entity shall document the determination in writing and maintain records concerning the determination for at least 5 years.

Sec. 13. If a covered entity discovers circumstances that require that it provide notice under section 9 to more than 1,000 state residents at a single time, the entity shall also notify, without unreasonable delay, each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the timing, distribution, and content of the notices.

Sec. 15. (1) If a third-party agent experiences a breach of security in the system maintained by the agent, the agent shall notify the covered entity of the breach of security as quickly as practicable.

(2) After receiving notice from a third-party agent under subsection (1), a covered entity shall provide the notice required under section 9. A third-party agent, in cooperation with a covered entity, shall provide information in the possession of the third-party agent so that the covered entity can comply with its notice requirements.

(3) A covered entity may enter into a contractual agreement with a third-party agent under which the third-party agent and

covered entity agree as to which party will be responsible for notifications to state residents required under this act, and the cost thereof, when the third-party agent experiences a breach of security.

(4) If a covered entity has not entered into a contractual agreement described in subsection (3) with a third-party agent and the third-party agent has not fulfilled its data security or privacy obligations under its customer or service agreement with the covered entity, the covered entity may seek reimbursement from the third-party agent, informally or through a civil action, for actual costs, including labor, associated with providing notices related to the breach of security experienced by the third-party agent.

Sec. 17. (1) Subject to subsection (2), a person that knowingly violates or has violated a notification requirement under this act may be ordered to pay a civil fine of not more than $2,000.00 for each violation, or not more than $5,000.00 per day for each consecutive day that the covered entity fails to take reasonable action to comply with the notice requirements of this act.

(2) A person's aggregate liability for civil fines under subsection (1) for multiple violations related to the same security breach shall not exceed $750,000.00.

(3) The attorney general has exclusive authority to bring an action to recover a civil fine under this section.

(4) It is not a violation of this act to refrain from providing any notice required under this act if a court of competent jurisdiction has directed otherwise.

(5) To the extent that notification is required under this act

as the result of a breach experienced by a third-party agent, a failure to inform the covered entity of the breach is a violation of this act by the third-party agent and the agent is subject to the remedies and penalties described in this section.

(6) The remedies under this section are independent and cumulative. The availability of a remedy under this section does not affect any right or cause of action a person may have at common law, by statute, or otherwise.

(7) This act shall not be construed to provide a basis for a private right of action.

Sec. 19. (1) State agencies are subject to the notice requirements of this act. A state agency that acquires and maintains sensitive personally identifying information from a state government employer, and that is required to provide notice to any state resident under this act, must also notify the employing state agency of any state residents to whom the information relates.

(2) A claim or civil action for a violation of this act by a state agency is subject to 1964 PA 170, MCL 691.1401 to 691.1419.

(3) By February 1 of each year, the department of technology, management, and budget shall submit a report to the governor, the senate majority leader, and the speaker of the house of representatives that describes the nature of any reported breaches of security by state agencies or third-party agents of state agencies in the preceding calendar year along with recommendations for security improvements. The report shall identify any state agency that has violated any of the applicable requirements in this act in the preceding calendar year.

Sec. 21. A covered entity or third-party agent shall take reasonable measures to dispose, or arrange for the disposal, of

records that contain sensitive personally identifying information within its custody or control when retention of the records is no longer required under applicable law, regulations, or business needs. Disposal shall include shredding, erasing, or otherwise modifying the sensitive personally identifying information in the records to make it unreadable or undecipherable through any reasonable means consistent with industry standards.

Sec. 23. (1) An entity that is subject to or regulated under federal laws, rules, regulations, procedures, or guidance on data breach notification established or enforced by the federal government is exempt from this act as long as the entity does all of the following:

(a) Maintains procedures under those federal laws, rules, regulations, procedures, or guidance.

(b) Provides notice to consumers under those federal laws, rules, regulations, procedures, or guidance.

(2) Except as provided in subsection (3), an entity that is not subject to or regulated under federal laws, rules, regulations, procedures, or guidance described in subsection (1), but is subject to or regulated under state laws, rules, regulations, procedures, or guidance on data breach notification that are established or enforced by state government, and are at least as thorough as the notice requirements provided by this act, is exempt from this act as long as the entity does all of the following:

(a) Maintains procedures under those state laws, rules, regulations, procedures, or guidance.

(b) Provides notice to customers under the notice requirements of those state laws, rules, regulations, procedures, or guidance.

(3) An entity that is subject to or regulated under the

insurance code of 1956, 1956 PA 218, MCL 500.100 to 500.8302, is exempt from this act.

(4) An entity that owns, is owned by, or is under common ownership with an entity described in subsection (1), (2), or (3) and that maintains the same cybersecurity procedures as that other entity is exempt from this act.

Sec. 25. This act 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 act is preempted.

Enacting section 1. This act takes effect June 20, 2021.

Enacting section 2. This act does not take effect unless House Bill No. 4186 of the 100th Legislature is enacted into law.