

**SENATE 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 protect and promote the safety 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:**

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

3           Sec. 3. As used in this act:

4           (a) "Breach of security" or "breach" means the unauthorized  
5 acquisition of sensitive personally identifying information in



1 electronic form, if that acquisition is reasonably likely to cause  
2 substantial risk of identity theft or fraud to the state residents  
3 to whom the information relates. Acquisition that occurs over a  
4 period of time that is committed by the same entity constitutes 1  
5 breach. The term does not include any of the following:

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

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

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

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

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



1 (d) Except as provided in subdivision (e), "sensitive  
2 personally identifying information" means either of the following:

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

6 (A) A nontruncated Social Security number.

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

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

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

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

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



1 (e) "Sensitive personally identifying information" does not  
2 include any of the following:

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

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

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

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

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

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



1 (2) For purposes of subsection (1), a covered entity or third-  
2 party agent shall consider all of the following in developing its  
3 reasonable security measures:

4 (a) The size of the covered entity or third-party agent.

5 (b) The amount of sensitive personally identifying information  
6 that is owned or licensed by the covered entity or maintained,  
7 processed, or accessed by the third-party agent in connection with  
8 providing services to a covered entity, and the type of activities  
9 for which the sensitive personally identifying information is  
10 accessed, acquired, or maintained by or on behalf of the covered  
11 entity.

12 (c) The covered entity's or third-party agent's cost to  
13 implement and maintain the security measures to protect against a  
14 breach of security relative to its resources.

15 (3) This section does not apply to a covered entity or third-  
16 party agent that is subject to or regulated under federal laws or  
17 regulations that require the use of reasonable security measures  
18 designed to protect sensitive personally identifying information  
19 against a breach of security as long as the covered entity or  
20 third-party agent complies with those federal laws or regulations.

21 (4) As used in this section, "reasonable security measures"  
22 means security measures that are reasonable for a covered entity or  
23 third-party agent to implement and maintain, including  
24 consideration of all of the following:

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

29 (b) Identification of internal and external risks of a breach



1 of security.

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

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

8 (e) Evaluation and adjustment of security measures to account  
9 for changes in circumstances affecting the security of sensitive  
10 personally identifying information.

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

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

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

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

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

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

28 (a) Indications that the information is in the physical  
29 possession and control of an unauthorized person, such as a lost or



1 stolen computer or other device containing information.

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

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

8 (d) Whether the information was publicly displayed.

9 Sec. 9. (1) If a covered entity that owns or licenses  
10 sensitive personally identifiable information determines under  
11 section 7 that a breach has occurred, the covered entity must  
12 provide notice of the breach to each state resident whose sensitive  
13 personally identifiable information was acquired in the breach.

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

22 (3) If a federal or state law enforcement agency determines  
23 that notice to state residents required under this section would  
24 interfere with a criminal investigation or national security, and  
25 delivers a written or electronic request to the covered entity for  
26 a delay, a covered entity shall delay providing the notice for a  
27 period that the law enforcement agency determines is necessary. If  
28 the law enforcement agency determines that an additional delay is  
29 necessary, the law enforcement agency shall deliver a written or



1 electronic request to the covered entity for an additional delay,  
2 and the covered entity shall delay providing the notice to the date  
3 specified in the law enforcement agency's request for additional  
4 delay, or extend the delay set forth in the original request for  
5 the additional period set forth in the request for additional  
6 delay.

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

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

24 (b) In the case of a breach that involves sensitive personally  
25 identifying information for login credentials of an electronic mail  
26 account furnished by the covered entity, the covered entity shall  
27 not comply with this section by providing the notification to that  
28 electronic mail address, but may, instead, comply with this section  
29 by providing notice by another method described in subdivision (a)



1 or (c), or by providing clear and conspicuous notice delivered to  
2 the state resident online if the resident is connected to the  
3 online account from an internet protocol address or online location  
4 from which the covered entity knows the state resident customarily  
5 accesses the account.

6 (c) Except as provided in subdivision (a) or (b), the covered  
7 entity shall comply with this section by providing a notice, in  
8 writing, sent to the mailing address of the state resident in the  
9 records of the covered entity, or by electronic mail notice sent to  
10 the electronic mail address of the state resident in the records of  
11 the covered entity. The notice shall include, at a minimum, all of  
12 the following:

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

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

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

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

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

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



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

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

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

10 (a) If the covered entity maintains an internet website, a  
 11 conspicuous notice posted on the website for a period of at least  
 12 30 days.

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

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

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

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



1 practicable.

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

8 (3) A covered entity may enter into a contractual agreement  
9 with a third-party agent under which the third-party agent and  
10 covered entity agree as to which party will be responsible for  
11 notifications to state residents required under this act, and the  
12 cost thereof, when the third-party agent experiences a breach of  
13 security.

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

23 Sec. 17. (1) Subject to subsection (2), a person that  
24 knowingly violates or has violated a notification requirement under  
25 this act may be ordered to pay a civil fine of not more than  
26 \$2,000.00 for each violation, or not more than \$5,000.00 per day  
27 for each consecutive day that the covered entity fails to take  
28 reasonable action to comply with the notice requirements of this  
29 act.



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

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

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

9 (5) To the extent that notification is required under this act  
10 as the result of a breach experienced by a third-party agent, a  
11 failure to inform the covered entity of the breach is a violation  
12 of this act by the third-party agent and the agent is subject to  
13 the remedies and penalties described in this section.

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

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

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

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

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



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

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

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

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

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

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

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

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



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

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

7 Sec. 25. This act deals with subject matter that is of  
8 statewide concern and any charter, ordinance, resolution,  
9 regulation, rule, or other action by a municipal corporation or  
10 other political subdivision of this state to regulate, directly or  
11 indirectly, any matter expressly set forth in this act is  
12 preempted.

13 Enacting section 1. This act takes effect January 20, 2022.

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

