

**SUBSTITUTE FOR  
HOUSE BILL NO. 6405**

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:**

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  
6 electronic form, if that acquisition is reasonably likely to cause  
7 substantial risk of identity theft or fraud to the state residents

1 to whom the information relates. Acquisition that occurs over a  
2 period of time that is committed by the same entity constitutes a  
3 breach. The term does not include any of the following:

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

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

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

15 (b) "Covered entity" means an individual or a sole  
16 proprietorship, partnership, government entity, corporation,  
17 limited liability company, nonprofit, trust, estate, cooperative  
18 association, or other business entity, that owns or licenses  
19 sensitive personally identifying information. The term also  
20 includes a state agency.

21 (c) "Data in electronic form" means any data that is stored  
22 electronically or digitally on any computer system or other  
23 database, including, but not limited to, recordable tapes and other  
24 mass storage devices.

25 (d) Except as provided in subdivision (e), "sensitive  
26 personally identifying information" means a state resident's first  
27 name or first initial and last name in combination with 1 or more

1 of the following data elements that relate to that state resident:

2 (i) A nontruncated Social Security number.

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

8 (iii) A financial account number, including, but not limited  
9 to, a bank account number, credit card number, or debit card  
10 number, in combination with any security code, access code,  
11 password, expiration date, or PIN, that is necessary to access the  
12 financial account or to conduct a transaction that will result in a  
13 credit or debit to the financial account.

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

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

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

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

26 (i) Information about a state resident that has been lawfully  
27 made public by a federal, state, or local government record or a

1 widely distributed media.

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

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

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

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

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

26 (2) For purposes of subsection (1), a covered entity shall  
27 consider all of the following in developing its reasonable security

1 measures:

2 (a) The size of the covered entity.

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

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

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

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

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

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

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

27 (e) Evaluation and adjustment of security measures to account

1 for changes in circumstances affecting the security of sensitive  
2 personally identifying information.

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

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

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

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

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

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

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

23           (b) Indications that the information has been downloaded or  
24 copied by an unauthorized person.

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

1 (d) Whether the information was publicly displayed.

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

7 (2) A covered entity shall provide notice under subsection (1)  
8 to state residents described in subsection (1) as expeditiously as  
9 possible and without unreasonable delay, taking into account the  
10 time necessary to allow the covered entity to conduct an  
11 investigation and determine the scope of the breach under section  
12 7. Except as provided in subsection (3), the covered entity shall  
13 provide notice within 45 days of the covered entity's determination  
14 that a breach has occurred.

15 (3) If a federal or state law enforcement agency determines  
16 that notice to state residents required under this section would  
17 interfere with a criminal investigation or national security, and  
18 delivers a request to the covered entity for a delay, a covered  
19 entity shall delay providing the notice for a period that the law  
20 enforcement agency determines is necessary. If the law enforcement  
21 agency determines that an additional delay is necessary, the law  
22 enforcement agency shall deliver a written request to the covered  
23 entity for an additional delay, and the covered entity shall delay  
24 providing the notice to the date specified in the law enforcement  
25 agency's written request, or extend the delay set forth in the  
26 original request for the additional period set forth in the written  
27 request.

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

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

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

1 accesses the account.

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

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

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

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

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

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

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

26 (a) Excessive cost to the covered entity of providing direct  
27 notification relative to the resources of the covered entity. For

1 purposes of this subdivision, the cost of direct notification to  
2 state residents is considered excessive if it exceeds \$250,000.00.

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

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

7 (a) If the covered entity maintains an internet website, a  
8 conspicuous notice posted on the website for a period of at least  
9 30 days.

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

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

17 Sec. 11. (1) If the number of state residents who a covered  
18 entity is required to notify under section 9 exceeds 750, the  
19 entity shall provide written notice of the breach to the department  
20 of technology, management, and budget as expeditiously as possible  
21 and without unreasonable delay. Except as provided in section 9(3),  
22 the covered entity shall provide the notice within 45 days of the  
23 covered entity's determination that a breach has occurred.

24 (2) Written notice to the department of technology,  
25 management, and budget under subsection (1) must include all of the  
26 following:

27 (a) A synopsis of the events surrounding the breach at the

1 time that notice is provided.

2 (b) The approximate number of state residents the covered  
3 entity is required to notify.

4 (c) Any services related to the breach the covered entity is  
5 offering or is scheduled to offer without charge to state  
6 residents, and instructions on how to use the services.

7 (d) How a state resident may obtain additional information  
8 about the breach from the covered entity.

9 (3) A covered entity may provide the department of technology,  
10 management, and budget with supplemental or updated information  
11 regarding a breach at any time.

12 (4) Information marked as confidential that is obtained by the  
13 department of technology, management, and budget under this section  
14 is not subject to the freedom of information act, 1976 PA 442, MCL  
15 15.231 to 15.246.

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

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

27 (2) After receiving notice from a third-party agent under

1 subsection (1), a covered entity shall provide notices required  
2 under sections 9 and 11. A third-party agent, in cooperation with a  
3 covered entity, shall provide information in the possession of the  
4 third-party agent so that the covered entity can comply with its  
5 notice requirements.

6 (3) A covered entity may enter into a contractual agreement  
7 with a third-party agent under which the third-party agent agrees  
8 to handle notifications required under this act.

9 Sec. 17. (1) Subject to subsection (2), a person that  
10 knowingly violates or has violated a notification requirement under  
11 this act may be ordered to pay a civil fine of not more than  
12 \$2,000.00 for each violation, or not more than \$5,000.00 per day  
13 for each consecutive day that the covered entity fails to take  
14 reasonable action to comply with the notice requirements of this  
15 act.

16 (2) A person's aggregate liability for civil fines under  
17 subsection (1) for multiple violations related to the same security  
18 breach shall not exceed \$250,000.00.

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

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

24 (5) To the extent that notification is required under this act  
25 as the result of a breach experienced by a third-party agent, a  
26 failure to inform the covered entity of the breach is a violation  
27 of this act by the third-party agent and the agent is subject to

1 the remedies and penalties described in this section.

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

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

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

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

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

25 Sec. 21. A covered entity or third-party agent shall take  
26 reasonable measures to dispose, or arrange for the disposal, of  
27 records that contain sensitive personally identifying information

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

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

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

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

16       (c) Timely provides a copy of the notice to the department of  
17 technology, management, and budget when the number of state  
18 residents the entity notified exceeds 750.

19       (2) Except as provided in subsection (3), an entity that is  
20 subject to or regulated under state laws, rules, regulations,  
21 procedures, or guidance on data breach notification that are  
22 established or enforced by state government, and are at least as  
23 thorough as the notice requirements provided by this act, is exempt  
24 from this act so long as the entity does all of the following:

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

27       (b) Provides notice to customers under the notice requirements

1 of those laws, rules, regulations, procedures, or guidance.

2 (c) Timely provides a copy of the notice to the department of  
3 technology, management, and budget when the number of state  
4 residents the entity notified exceeds 750.

5 (3) An entity that is subject to or regulated under the  
6 insurance code of 1956, 1956 PA 218, MCL 500.100 to 500.8302, is  
7 exempt from this act.

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

12 Enacting section 1. This act takes effect 90 days after the  
13 date it is enacted into law.

14 Enacting section 2. This act does not take effect unless all  
15 of the following bills of the 99th Legislature are enacted into  
16 law:

17 (a) House Bill No. 6406.

18 (b) House Bill No. 6491.