Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Michigan

Mich. Comp. Laws § 445.63, 72 *et seq.*

S.B. 309 (signed into law December 30, 2006, Pub. Act. 566)

Effective July 2, 2007

S.B. No. 223 (signed into law December 21, 2010)

Effective April 1, 2011

H.B. 6406 (signed into law December 28, 2018)

Effective January 20, 2020

Application. Any individual, partnership, corporation, limited liability company, association, or other legal entity, or any department, board, commission, office, agency, authority, or other unit of state government of MI (collectively, Entity) that owns or licenses data including PI of a MI resident.

Security Breach Definition. The unauthorized access and acquisition of data that compromises the security or confidentiality of PI maintained by an Entity as part of a database of PI regarding multiple individuals.

- A good-faith but unauthorized acquisition of PI by an employee or other individual, where the access was related to the activities of the Entity, is not a breach of security unless the PI is misused or disclosed to an unauthorized person. In making this determination an Entity shall act with the care an ordinarily prudent Entity in a like position would exercise under similar circumstances.

Notification Obligation. An Entity that owns or licenses data including MI residents shall provide notice of the breach to each resident of MI if (i) the resident's unencrypted and unredacted PI was accessed and acquired by an unauthorized person or (ii) the resident's PI was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key.

- Notification is not required if the Entity determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents of MI.

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.

Notification to Consumer Reporting Agencies. If an Entity notifies 1,000 or more MI residents, the Entity shall, after notifying those residents, notify each nationwide consumer reporting agency without unreasonable delay of the number and timing of notices that the person or agency provided to residents of this state. This subsection does not apply if the person or agency is subject to Title V of the Gramm-Leach-Bliley Act.

Third-Party Data Notification. An Entity that maintains a database that includes data that the Entity 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 security breach, unless the Entity determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to one or more residents

of MI.

Timing of Notification. The notification shall be given without unreasonable delay following discovery of the breach, consistent with measures necessary to determine the scope of the breach of the security of a system or restore the integrity of the system.

Personal Information Definition. The first name or first initial and last name linked to one or more of the following data elements of a resident of MI:

- Social Security number;
- Driver's license number or state personal identification card number; or
- 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.

Notice Required. Notice may be provided by one of the following methods:

- Written notice sent to the recipient at the recipient's postal address in the records of the Entity;
- Telephonic notice given by an individual who represents the Entity if (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 Entity also provides notice pursuant to the above methods if the notice by telephone does not result in a live conversation between the individual representing the Entity and the recipient within 3 business days after the initial attempt to provide telephonic notice; or
- Written notice sent electronically to the recipient if (i) the recipient has expressly consented to receive electronic notice, (ii) the Entity has an existing business relationship with the recipient that includes periodic email communications and based on those communications the Entity reasonably believes that it has the recipient's current email address, or (iii) the Entity conducts its business primarily through Internet account transactions or on the Internet.

A notice under the statute shall:

- Be written in a clear and conspicuous manner, and shall clearly communicate the content required;
- Describe the security breach in general terms;
- Describe the type of PI that is the subject of the unauthorized access or use;
- If applicable, generally describe what the agency or person providing the notice has done to protect data from further security breaches;
- Include a telephone number where a notice recipient may obtain assistance or additional information; and
- Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft.

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $250,000 or that the Entity has to provide notice to more than 500,000 residents of MI. Substitute notice shall consist of all of the following:

- Email notice, if the Entity has email addresses for any of the residents of MI who are entitled to receive notice;
- Conspicuous posting on the Entity's website, if the Entity maintains one; and
- Notification to major statewide media, which notice shall include a telephone number or website address that a person may use to obtain additional assistance and information.

A public utility that sends monthly billing or account statements to its customers may provide notice of a security breach to its customers as provided under the statute or by providing all of the following:

- As applicable, email notice in accordance with the statute;
- Notice to the media reasonably calculated to inform the utility's customers of the breach;
- Conspicuous posting of notice of the security breach on the website of the utility; and
- Written notice sent in conjunction with the billing or account statement sent to the customer at his or her postal address in the utility's records.

Exception: Compliance with Other Laws.

- **Federal Interagency Guidance.** A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said interagency guidance, shall be deemed to be in compliance.
- **HIPAA-Covered Entities.** A provider of health care, health care service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed in compliance with this chapter.
- Entities subject to, or regulated under Michigan's insurance code are exempt from the state's data breach notification statute and instead will be governed by **HB 6491**/Public Act 690 of 2018, which goes into effect January 20, 2021.

Penalties. Provides for criminal penalties for notice of a security breach that has not occurred, where such notice is given with the intent to defraud. The offense is a misdemeanor, punishable by imprisonment for not more than 30 days or a fine of not more than $250 per violation (or both). (The penalty is the same for second and third violations, except that the fine increases to $500 per violation and $750 per violation, respectively.) Similarly, Entities who distribute an advertisement or make any other solicitation that misrepresents to the recipient that a security breach has occurred that may affect the recipient are punishable by imprisonment for not more than 93 days or a fine of not more than $1,000 per violation (or both). (The penalty is the same for second and third violations, except that the fine increases to $2,000 per violation and $3,000 per violation, respectively.)

Entities who fail to provide notice may be ordered to pay a civil fine of not more than $250 for each failure to provide notice, capped at $750,000 per security breach. These penalties do not affect the availability of civil remedies under state or federal law.

Other Key Provisions:

- **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation or jeopardize homeland or national security. Notification shall be given as soon as reasonably practicable after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security.
- Attorney General Enforcement.
- Provides that Entities may deliver notice pursuant to an agreement with another Entity, if the agreement does not conflict with MI law.