

Michigan Compiled Laws
Chapter 445 – Trade and Commerce
Identity Theft Protection Act

§ 445.63 Definitions.

Sec. 3.

As used in this act:

(a) "Agency" means a department, board, commission, office, agency, authority, or other unit of state government of this state. The term includes an institution of higher education of this state. The term does not include a circuit, probate, district, or municipal court.

(b) "Breach of the security of a database" or "security breach" means the unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals. These terms do not include unauthorized access to data by an employee or other individual if the access meets all of the following:

(i) The employee or other individual acted in good faith in accessing the data.

(ii) The access was related to the activities of the agency or person.

(iii) The employee or other individual did not misuse any personal information or disclose any personal information to an unauthorized person.

(c) "Child or spousal support" means support for a child or spouse, paid or provided pursuant to state or federal law under a court order or judgment. Support includes, but is not limited to, any of the following:

(i) Expenses for day-to-day care.

(ii) Medical, dental, or other health care.

(iii) Child care expenses.

(iv) Educational expenses.

(v) Expenses in connection with pregnancy or confinement under the paternity act, 1956 PA 205, MCL 722.711 to 722.730.

(vi) Repayment of genetic testing expenses, under the paternity act, 1956 PA 205, MCL 722.711 to 722.730.

(vii) A surcharge as provided by section 3a of the support and parenting time enforcement act, 1982 PA 295, MCL 552.603a.

(d) "Credit card" means that term as defined in section 157m of the Michigan penal code, 1931 PA 328, MCL 750.157m.

(e) "Data" means computerized personal information.

(f) "Depository institution" means a state or nationally chartered bank or a state or federally chartered savings and loan association, savings bank, or credit union.

(g) "Encrypted" means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing information by another method that renders the data elements unreadable or unusable.

(h) "Financial institution" means a depository institution, an affiliate of a depository institution, a licensee under the consumer financial services act, 1988 PA 161, MCL 487.2051 to 487.2072, 1984 PA 379, MCL 493.101 to 493.114, the motor vehicle sales finance act, 1950 (Ex Sess) PA 27, MCL 492.101 to 492.141, the secondary mortgage loan act, 1981 PA 125, MCL 493.51 to 493.81, the mortgage brokers, lenders, and servicers licensing act, 1987 PA 173, MCL 445.1651 to 445.1684, or the regulatory loan act, 1939 PA 21, MCL 493.1 to 493.24, a seller under the home improvement finance act, 1965 PA 332, MCL 445.1101 to 445.1431, or the retail installment sales act, 1966 PA 224, MCL 445.851 to 445.873, or a person subject to subtitle A of title V of the Gramm-Leach-Bliley act, 15 USC 6801 to 6809.

(i) "Financial transaction device" means that term as defined in section 157m of the Michigan penal code, 1931 PA 328, MCL 750.157m.

(j) "Identity theft" means engaging in an act or conduct prohibited in section 5(1).

(k) "Law enforcement agency" means that term as defined in section 2804 of the public health code, 1978 PA 368, MCL 333.2804.

(l) "Local registrar" means that term as defined in section 2804 of the public health code, 1978 PA 368, MCL 333.2804.

(m) "Medical records or information" includes, but is not limited to, medical and mental health histories, reports, summaries, diagnoses and prognoses, treatment and medication information, notes, entries, and x-rays and other imaging records.

(n) "Person" means an individual, partnership, corporation, limited liability company, association, or other legal entity.

(o) "Personal identifying information" means a name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including, but not limited to, a person's name, address, telephone number, driver license or state personal identification card number, social security

number, place of employment, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or the person's account password, stock or other security certificate or account number, credit card number, vital record, or medical records or information.

(p) "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) Social security number.

(ii) Driver license number or state personal identification card number.

(iii) 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.

(q) "Public utility" means that term as defined in section 1 of 1972 PA 299, MCL 460.111.

(r) "Redact" means to alter or truncate data so that no more than 4 sequential digits of a driver license number, state personal identification card number, or account number, or no more than 5 sequential digits of a social security number, are accessible as part of personal information.

(s) "State registrar" means that term as defined in section 2805 of the public health code, 1978 PA 368, MCL 333.2805.

(t) "Trade or commerce" means that term as defined in section 2 of the Michigan consumer protection act, 1971 PA 331, MCL 445.902.

(u) "Vital record" means that term as defined in section 2805 of the public health code, 1978 PA 368, MCL 333.2805.

§ 445.72 Notice of security breach; requirements.

Sec. 12.

(1) Unless the person or agency 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, 1 or more residents of this state, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach under subsection (2), shall provide a notice of the security breach 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 person with unauthorized access to the encryption key.

(2) Unless the person or agency 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, 1 or more residents of this state, a person or agency that maintains a database that includes data that the person or agency 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.

(3) In determining whether a security breach 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 person or agency shall act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances.

(4) A person or agency shall provide any notice required under this section without unreasonable delay. A person or agency may delay providing notice without violating this subsection if either of the following is met:

(a) A delay is necessary in order for the person or agency to take any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database. However, the agency or person shall provide the notice required under this subsection without unreasonable delay after the person or agency completes the measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database.

(b) A law enforcement agency determines and advises the agency or person that providing a notice will impede a criminal or civil investigation or jeopardize homeland or national security. However, the agency or person 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.

(5) Except as provided in subsection (11), an agency or person 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 agency or person.

(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 person or agency has an existing business relationship with the recipient that includes periodic electronic mail communications and based on those communications the person or agency reasonably believes that it has the recipient's current electronic mail address.

(iii) The person or agency 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 person or agency 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 person or agency 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 person or agency and the recipient within 3 business days after the initial attempt to provide telephonic notice.

(d) Substitute notice, if the person or agency demonstrates that the cost of providing notice under subdivision (a), (b), or (c) will exceed \$250,000.00 or that the person or agency has to provide notice to more than 500,000 residents of this state. A person or agency provides substitute notice under this subdivision by doing all of the following:

(i) If the person or agency 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 person or agency maintains a website, conspicuously posting the notice on that website.

(iii) Notifying major statewide media. A notification under this subparagraph shall include a telephone number or a website address that a person may use to obtain additional assistance and information.

(6) A notice under this section shall meet all of the following:

(a) For a notice provided under subsection (5)(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), clearly communicate the content required under subdivisions (c) to (g) to the recipient of the telephone call.

(c) Describe the security breach 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 agency or person 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.

(7) A person or agency may provide any notice required under this section pursuant to an agreement between that person or agency and another person or agency, if the notice provided pursuant to the agreement does not conflict with any provision of this section.

(8) Except as provided in this subsection, after a person or agency provides a notice under this section, the person or agency 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 security breach without unreasonable delay. A notification under this subsection shall include the number of notices that the person or agency 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 person or agency is required under this section to provide notice of a security breach to 1,000 or fewer residents of this state.

(b) The person or agency is subject to title V of the Gramm-Leach-Bliley act, 15 USC 6801 to 6809.

(9) A financial institution that is subject to, and has notification procedures in place that are subject to examination by the financial institution's appropriate regulator for compliance with, the interagency guidance on response programs for unauthorized access to customer information and customer notice prescribed by the board of governors of the federal reserve system and the other federal bank and thrift regulatory agencies, or similar guidance prescribed and adopted by the national credit union administration, and its affiliates, is considered to be in compliance with this section.

(10) A person or agency 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.

(11) A public utility that sends monthly billing or account statements to the postal address of its customers may provide notice of a security breach to its customers in the manner described in subsection (5), or alternatively by providing all of the following:

(a) As applicable, notice as described in subsection (5)(b).

(b) Notification to the media reasonably calculated to inform the customers of the public utility of the security breach.

(c) Conspicuous posting of the notice of the security breach on the website of the public utility.

(d) Written notice sent in conjunction with the monthly billing or account statement to the customer at the customer's postal address in the records of the public utility.

(12) A person that provides notice of a security breach in the manner described in this section when a security breach has not occurred, with the intent to defraud, is guilty of a misdemeanor punishable by imprisonment for not more than 30 days or a fine of not more than \$250.00 for each violation, or both.

(13) Subject to subsection (14), a person that knowingly fails to provide any notice of a security breach 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.

(14) The aggregate liability of a person for civil fines under subsection (13) for multiple violations of subsection (13) that arise from the same security breach shall not exceed \$750,000.00.

(15) Subsections (12) and (13) do not affect the availability of any civil remedy for a violation of state or federal law.

(16) This section applies to the discovery or notification of a breach of the security of a database that occurs on or after the effective date of the amendatory act that added this section.

(17) 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.

(18) 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.

§ 445.72a Destruction of data containing personal information required; violation as misdemeanor; fine; compliance; "destroy" defined.

Sec. 12a.

(1) Subject to subsection (3), a person or agency that maintains a database that includes personal information regarding multiple individuals shall destroy any data that contain personal information concerning an individual when that data is removed from the database and the person or agency is not retaining the data elsewhere for another purpose not prohibited by state or federal law. This subsection does not prohibit a person or agency from retaining data that contain personal information for purposes of an investigation, audit, or internal review.

(2) A person who knowingly violates this section is guilty of a misdemeanor punishable by a fine of not more than \$250.00 for each violation. This subsection does not affect the availability of any civil remedy for a violation of state or federal law.

(3) A person or agency is considered to be in compliance with this section if the person or agency is subject to federal law concerning the disposal of records containing personal identifying information and the person or agency is in compliance with that federal law.

(4) As used in this section, "destroy" means to destroy or arrange for the destruction of data by shredding, erasing, or otherwise modifying the data so that they cannot be read, deciphered, or reconstructed through generally available means.