IDENTITY THEFT PROTECTION ACT
Act 452 of 2004

AN ACT to prohibit certain acts and practices concerning identity theft; to require notification of a security breach of a database that contains certain personal information; to provide for the powers and duties of certain state and local governmental officers and entities; to prescribe penalties and provide remedies; and to repeal acts and parts of acts.

History: 2004, Act 452, Eff. Mar. 1, 2005;—Am. 2006, Act 566, Eff. July 2, 2007.

The People of the State of Michigan enact:

445.61 Short title.

Sec. 1. This act shall be known and may be cited as the "identity theft protection act".

History: 2004, Act 452, Eff. Mar. 1, 2005.

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) "False pretenses" includes, but is not limited to, a false, misleading, or fraudulent representation, writing, communication, statement, or message, communicated by any means to another person, that the maker of the representation, writing, communication, statement, or message knows or should have known is false or fraudulent. The false pretense may be a representation regarding a past or existing fact or circumstance or a representation regarding the intention to perform a future event or to have a future event performed.

(i) "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.

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

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

(*l*) "Interactive computer service" means an information service or system that enables computer access by multiple users to a computer server, including, but not limited to, a service or system that provides access to the internet or to software services available on a server.

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

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

(o) "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.

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

(q) "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, any other account password in combination with sufficient information to identify and access the account, automated or electronic signature, biometrics, stock or other security certificate or account number, credit card number, vital record, or medical records or information.

(r) "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.

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

(t) "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.

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

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

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

(x) "Webpage" means a location that has a uniform resource locator or URL with respect to the world wide web or another location that can be accessed on the internet.

History: 2004, Act 452, Eff. Mar. 1, 2005;—Am. 2006, Act 566, Eff. July 2, 2007;—Am. 2010, Act 318, Eff. Apr. 1, 2011.

445.65 Prohibited acts; violations; defense in civil action or criminal prosecution; burden of proof.

Sec. 5. (1) A person shall not do any of the following:

(a) With intent to defraud or violate the law, use or attempt to use the personal identifying information of another person to do either of the following:

(*i*) Obtain credit, goods, services, money, property, a vital record, a confidential telephone record, medical records or information, or employment.

(*ii*) Commit another unlawful act.

(b) By concealing, withholding, or misrepresenting the person's identity, use or attempt to use the personal identifying information of another person to do either of the following:

(*i*) Obtain credit, goods, services, money, property, a vital record, a confidential telephone record, medical records or information, or employment.

(*ii*) Commit another unlawful act.

(2) A person who violates subsection (1)(b)(*i*) may assert 1 or more of the following as a defense in a civil action or as an affirmative defense in a criminal prosecution, and has the burden of proof on that defense by a preponderance of the evidence:

(a) That the person gave a bona fide gift for or for the benefit or control of, or use or consumption by, the person whose personal identifying information was used.

(b) That the person acted in otherwise lawful pursuit or enforcement of a person's legal rights, including an investigation of a crime or an audit, collection, investigation, or transfer of a debt, child or spousal support obligation, tax liability, claim, receivable, account, or interest in a receivable or account.

(c) That the action taken was authorized or required by state or federal law, rule, regulation, or court order or rule.

(d) That the person acted with the consent of the person whose personal identifying information was used, unless the person giving consent knows that the information will be used to commit an unlawful act.

History: 2004, Act 452, Eff. Mar. 1, 2005;—Am. 2006, Act 246, Imd. Eff. June 30, 2006.

445.65a Definitions; prohibited acts; obtaining confidential telephone records by law enforcement agency or telecommunication provider.

Sec. 5a. (1) As used in this act:

(a) "Confidential telephone record" means any of the following:

(*i*) Information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a service offered by a telecommunication provider subscribed to by any customer of that telecommunication provider.

(*ii*) Information that is made available to a telecommunication provider by a customer solely by virtue of the relationship between the telecommunication provider and the customer.

(*iii*) Information contained in any bill related to the product or service offered by a telecommunication provider and received by any customer of the telecommunication provider.

(b) "Covered specialized mobile radio service" means a commercial mobile radio service that offers real-time, 2-way switched voice or data service and is interconnected with the public switched network utilizing an in-network switching facility.

(c) "IP-enabled voice service" means an interconnected voice over internet protocol service that enables real-time, 2-way voice communications, requires a broadband connection from the user's location using internet protocol-compatible equipment, and permits users generally to receive calls that originate on the public switched telephone network and to terminate calls to the public switched telephone network.

(d) "Telecommunication provider" means all of the following:

(*i*) A provider as that term is defined in section 102 of the Michigan telecommunications act, 1991 PA 179, MCL 484.2102.

(*ii*) A provider of IP-enabled voice service.

(*iii*) A provider of any telecommunication service.

(e) "Telecommunication service" means all of the following:

(*i*) A service as that term is defined in section 102 of the Michigan telecommunications act, 1991 PA 179, MCL 484.2102.

(*ii*) Cellular telephone service.

(*iii*) Broadband personal communication service.

(*iv*) Covered specialized mobile radio.

(2) A person shall not do any of the following:

(a) Knowingly procure, attempt to procure, or solicit or conspire with another to procure a confidential telephone record of any resident of this state without the authorization of the customer to whom the record pertains or by fraudulent, deceptive, or false means.

(b) Knowingly sell or attempt to sell a confidential telephone record of any resident of this state without the authorization of the customer to whom the record pertains.

(c) Receive a confidential telephone record of any resident of this state knowing that the record has been obtained without the authorization of the customer to whom the record pertains or by fraudulent, deceptive, or false means.

(3) This section does not prohibit any action by a law enforcement agency, or any officer, employee, or

agent of such agency, from obtaining confidential telephone records in connection with the performance of the official duties of the agency.

(4) This section does not prohibit a telecommunication provider from obtaining, using, disclosing, or permitting access to any confidential telephone record, either directly or indirectly, through its agents, subcontractors, affiliates, or representatives in the normal course of business. This section does not expand the obligations and duties of a telecommunication provider to protect confidential telephone records beyond those obligations and duties otherwise established by federal and state law.

History: Add. 2006, Act 246, Imd. Eff. June 30, 2006.

445.67 Additional prohibited acts.

Sec. 7. A person shall not do any of the following:

(a) Make any electronic mail or other communication under false pretenses purporting to be by or on behalf of a business, without the authority or approval of the business, and use that electronic mail or other communication to induce, request, or solicit any individual to provide personal identifying information with the intent to use that information to commit identity theft or another crime.

(b) Create or operate a webpage that represents itself as belonging to or being associated with a business, without the authority or approval of that business, and induces, requests, or solicits any user of the internet to provide personal identifying information with the intent to use that information to commit identity theft or another crime.

(c) Alter a setting on a user's computer or similar device or software program through which the user may access the internet and cause any user of the internet to view a communication that represents itself as belonging to or being associated with a business, which message has been created or is operated without the authority or approval of that business, and induces, requests, or solicits any user of the internet to provide personal identifying information with the intent to use that information to commit identity theft or another crime.

(d) Obtain or possess, or attempt to obtain or possess, personal identifying information of another person with the intent to use that information to commit identity theft or another crime.

(e) Sell or transfer, or attempt to sell or transfer, personal identifying information of another person if the person knows or has reason to know that the specific intended recipient will use, attempt to use, or further transfer the information to another person for the purpose of committing identity theft or another crime.

(f) Falsify a police report of identity theft, or knowingly create, possess, or use a false police report of identity theft.

History: 2004, Act 452, Eff. Mar. 1, 2005;—Am. 2010, Act 318, Eff. Apr. 1, 2011.

445.67a Prohibited acts; interactive computer service provider not liable for certain actions; civil action by attorney general or interactive computer service provider; exception; recovery of damages; investigation.

Sec. 7a. (1) A person shall not do any of the following:

(a) Make any electronic mail or other communication under false pretenses purporting to be by or on behalf of a business, without the authority or approval of the business, and use that electronic mail or other communication to induce, request, or solicit any individual to provide personal identifying information.

(b) Create or operate a webpage that represents itself as belonging to or being associated with a business, without the authority or approval of that business, and induces, requests, or solicits any user of the internet to provide personal identifying information.

(c) Alter a setting on a user's computer or similar device or software program through which the user may access the internet and cause any user of the internet to view a communication that represents itself as belonging to or being associated with a business, which message has been created or is operated without the authority or approval of that business, and induces, requests, or solicits any user of the internet to provide personal identifying information.

(2) An interactive computer service provider shall not be held liable under any provision of the laws of this state for removing or disabling access to an internet domain name controlled or operated by the registrar or by the provider, or to content that resides on an internet website or other online location controlled or operated by the provider, that the provider believes in good faith is used to engage in a violation of this act. This act does not apply to a telecommunications provider's or internet service provider's good faith transmission or routing of, or intermediate temporary storing or caching of, personal identifying information.

(3) The attorney general, or an interactive computer service provider harmed by a violation of subsection (1), may bring a civil action against a person who has violated that subsection.

(4) Subsection (1) does not apply to the following:

(a) A law enforcement officer while that officer is engaged in the performance of his or her official duties.

(b) Any other individual authorized to conduct lawful investigations while that individual is engaged in a lawful investigation.

(5) A person bringing an action under this section may recover 1 of the following:

(a) Actual damages, including reasonable attorney fees.

(b) In lieu of actual damages, reasonable attorney fees plus the lesser of the following:

(*i*) $5,000.00 per violation.

(*ii*) $250,000.00 for each day that a violation occurs.

(6) If the attorney general has reason to believe that a person has violated section 7(a), (b), or (c) or this section, the attorney general may investigate the business transactions of that person. The attorney general may require that person to appear, at a reasonable time and place, to give information under oath and to produce any documents and evidence necessary to determine whether the person is in compliance with the requirements of that section.

History: Add. 2010, Act 318, Eff. Apr. 1, 2011.

445.69 Certain violations as felony; penalty; consecutive sentences; defense in civil action or criminal prosecution; burden of proof; exception.

Sec. 9. (1) Subject to subsection (6), a person who violates section 5 or 7 is guilty of a felony punishable as follows:

(a) Except as otherwise provided in subdivisions (b) and (c), by imprisonment for not more than 5 years or a fine of not more than $25,000.00, or both.

(b) If the violation is a second violation of section 5 or 7, by imprisonment for not more than 10 years or a fine of not more than $50,000.00, or both.

(c) If the violation is a third or subsequent violation of section 5 or 7, by imprisonment for not more than 15 years or a fine of not more than $75,000.00, or both.

(2) Sections 5 and 7 apply whether an individual who is a victim or intended victim of a violation of 1 of those sections is alive or deceased at the time of the violation.

(3) This section does not prohibit a person from being charged with, convicted of, or sentenced for any other violation of law committed by that person using information obtained in violation of this section or any other violation of law committed by that person while violating or attempting to violate this section.

(4) The court may order that a term of imprisonment imposed under this section be served consecutively to any term of imprisonment imposed for a conviction of any other violation of law committed by that person using the information obtained in violation of this section or any other violation of law committed by that person while violating or attempting to violate this section.

(5) A person may assert as a defense in a civil action or as an affirmative defense in a criminal prosecution for a violation of section 5 or 7, and has the burden of proof on that defense by a preponderance of the evidence, that the person lawfully transferred, obtained, or attempted to obtain personal identifying information of another person for the purpose of detecting, preventing, or deterring identity theft or another crime or the funding of a criminal activity.

(6) Subsection (1) does not apply to a violation of a statute or rule administered by a regulatory board, commission, or officer acting under authority of this state or the United States that confers primary jurisdiction on that regulatory board, commission, or officer to authorize, prohibit, or regulate the transactions and conduct of that person, including, but not limited to, a state or federal statute or rule governing a financial institution and the insurance code of 1956, 1956 PA 218, MCL 500.100 to 500.8302, if the act is committed by a person subject to and regulated by that statute or rule, or by another person who has contracted with that person to use personal identifying information.

History: 2004, Act 452, Eff. Mar. 1, 2005;—Am. 2010, Act 315, Eff. Apr. 1, 2011;—Am. 2010, Act 318, Eff. Apr. 1, 2011.

445.71 Prohibited acts in conduct of trade or commerce; violation as misdemeanor; penalty; civil liability.

Sec. 11. (1) A person shall not do any of the following in the conduct of trade or commerce:

(a) Deny credit or public utility service to or reduce the credit limit of a consumer solely because the consumer was a victim of identity theft, if the person had prior knowledge that the consumer was a victim of identity theft. A consumer is presumed to be a victim of identity theft for the purposes of this subdivision if he or she provides both of the following to the person:

(*i*) A copy of a police report evidencing the claim of the victim of identity theft.

(*ii*) Either a properly completed copy of a standardized affidavit of identity theft developed and made available by the federal trade commission under 15 USC 1681g or an affidavit of fact that is acceptable to the

person for that purpose.

(b) Solicit to extend credit to a consumer who does not have an existing line of credit, or has not had or applied for a line of credit within the preceding year, through the use of an unsolicited check that includes personal identifying information other than the recipient's name, address, and a partial, encoded, or truncated personal identifying number. In addition to any other penalty or remedy under this act or the Michigan consumer protection act, 1976 PA 331, MCL 445.901 to 445.922, a credit card issuer, financial institution, or other lender that violates this subdivision, and not the consumer, is liable for the amount of the instrument if the instrument is used by an unauthorized user and for any fees assessed to the consumer if the instrument is dishonored.

(c) Solicit to extend credit to a consumer who does not have a current credit card, or has not had or applied for a credit card within the preceding year, through the use of an unsolicited credit card sent to the consumer. In addition to any other penalty or remedy under this act or the Michigan consumer protection act, 1976 PA 331, MCL 445.901 to 445.922, a credit card issuer, financial institution, or other lender that violates this subdivision, and not the consumer, is liable for any charges if the credit card is used by an unauthorized user and for any interest or finance charges assessed to the consumer.

(d) Extend credit to a consumer without exercising reasonable procedures to verify the identity of that consumer. Compliance with regulations issued for depository institutions, and to be issued for other financial institutions, by the United States department of treasury under section 326 of the USA patriot act of 2001, 31 USC 5318, is considered compliance with this subdivision. This subdivision does not apply to a purchase of a credit obligation in an acquisition, merger, purchase of assets, or assumption of liabilities or any change to or review of an existing credit account.

(2) A person who knowingly or intentionally violates subsection (1) is guilty of a misdemeanor punishable as follows:

(a) Except as otherwise provided in subdivisions (b) and (c), by imprisonment for not more than 93 days or a fine of not more than $1,000.00, or both.

(b) For a second violation, by imprisonment for not more than 93 days or a fine of not more than $2,000.00, or both.

(c) For a third or subsequent violation, by imprisonment for not more than 93 days or a fine of not more than $3,000.00, or both.

(3) Subsection (2) does not prohibit a person from being liable for any civil remedy for a violation of this act, the Michigan consumer protection act, 1976 PA 331, MCL 445.901 to 445.922, or any other state or federal law.

History: 2004, Act 452, Eff. Mar. 1, 2005;—Am. 2010, Act 315, Eff. Apr. 1, 2011.

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 do 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 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 as follows:

(a) Except as otherwise provided under subdivisions (b) and (c), by imprisonment for not more than 93 days or a fine of not more than $250.00 for each violation, or both.

(b) For a second violation, by imprisonment for not more than 93 days or a fine of not more than $500.00 for each violation, or both.

(c) For a third or subsequent violation, by imprisonment for not more than 93 days or a fine of not more than $750.00 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 July 2, 2006.

(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.

History: Add. 2006, Act 566, Eff. July 2, 2007;—Am. 2010, Act 315, Eff. Apr. 1, 2011.

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.

History: Add. 2006, Act 566, Eff. July 2, 2007.

445.72b Misrepresentation by advertisement or solicitation prohibited; violation as misdemeanor; penalty; civil remedy.

Sec. 12b. (1) A person shall not distribute an advertisement or make any other solicitation that misrepresents to the recipient that a security breach has occurred that may affect the recipient.

(2) A person shall not distribute an advertisement or make any other solicitation that is substantially similar to a notice required under section 12(5) or by federal law, if the form of that notice is prescribed by state or federal law, rule, or regulation.

(3) A person who knowingly or intentionally violates this section is guilty of a misdemeanor punishable as follows:

(a) Except as otherwise provided in subdivisions (b) and (c), by imprisonment for not more than 93 days or a fine of not more than $1,000.00 for each violation, or both.

(b) For a second violation, by imprisonment for not more than 93 days or a fine of not more than $2,000.00 for each violation, or both.

(c) For a third or subsequent violation, by imprisonment for not more than 93 days or a fine of not more than $3,000.00 for each violation, or both.

(4) Subsection (3) does not affect the availability of any civil remedy for a violation of this section or any other state or federal law.

History: Add. 2006, Act 566, Eff. July 2, 2007;—Am. 2010, Act 315, Eff. Apr. 1, 2011.

445.73 Verification of information; use of vital record.

Sec. 13. (1) A law enforcement agency or victim of identity theft may verify information from a vital record from a local registrar or the state registrar in the manner described in section 2881(2) of the public health code, 1978 PA 368, MCL 333.2881.

(2) A state registrar or local registrar that verifies information from a vital record under section 2881(2) of the public health code, 1978 PA 368, MCL 333.2881, for a law enforcement agency investigating identity theft may provide that law enforcement agency with all of the following information about any previous requests concerning that public record that is available to the registrar:

(a) Whether or not a certified copy or copies of the record were requested.

(b) The date or dates a copy or copies of the record were issued.

(c) The name of each applicant who requested the record.

(d) The address, e-mail address, telephone number, and other identifying information of each applicant who requested the record.

(e) Payment information regarding each request.

(3) A state registrar or local registrar that verifies information from a vital record under section 2881(2) of the public health code, 1978 PA 368, MCL 333.2881, for an individual who provides proof that he or she is a victim of identity theft may provide that individual with all of the following information about any previous requests concerning that public record that is available to the registrar:

(a) Whether or not a certified copy or copies of the record were requested.

(b) The date or dates a copy or copies of the record were issued.

(4) For purposes of subsection (3), it is sufficient proof that an individual is a victim of identity theft for a state registrar or local registrar to provide the information described in that subsection if he or she provides the registrar with a copy of a police report evidencing the claim that he or she is a victim of identity theft; and, if available, an affidavit of identity theft, in a form developed by the state registrar in cooperation with the attorney general for purposes of this subsection.

(5) A law enforcement agency may request an administrative use copy of a vital record from the state registrar in the manner described in section 2891 of the public health code, 1978 PA 368, MCL 333.2891.

(6) A law enforcement agency may request an administrative use copy of a vital record from a local registrar in the manner described in section 2891 of the public health code, 1978 PA 368, MCL 333.2891, if the request for the administrative use copy is in writing and contains both of the following:

(a) A statement that the law enforcement agency requires information from a vital record beyond the information the local registrar may verify under subsections (1) and (2).

(b) The agreement of the law enforcement agency that it will maintain the administrative use copy of the

vital record in a secure location and will destroy the copy by confidential means when it no longer needs the copy.

History: 2004, Act 452, Eff. Mar. 1, 2005.

445.75 Repeal of MCL 750.285.

Sec. 15. Section 285 of the Michigan penal code, 1931 PA 328, MCL 750.285, is repealed.

History: 2004, Act 452, Eff. Mar. 1, 2005.

445.77 Effective date.

Sec. 17. This act takes effect March 1, 2005.

History: 2004, Act 452, Eff. Mar. 1, 2005.

445.79 Property subject to forfeiture.

Sec. 19. (1) Except as provided in subsection (2), the following property is subject to forfeiture:

(a) Any personal or real property that has been used, possessed, or acquired in a felony violation of this act.

(b) Except as provided in subparagraphs (*i*) to (*iii*), a conveyance, including an aircraft, vehicle, or vessel, used or intended for use to transport, or in any manner to facilitate the transportation of, for the purpose of sale or receipt, property described in subdivision (a):

(*i*) A conveyance used by a person as a common carrier in the transaction of business as a common carrier is not subject to forfeiture unless it is determined that the owner or other person in charge of the conveyance is a consenting party or privy to a violation of this act.

(*ii*) A conveyance is not subject to forfeiture by reason of any act or omission established by the owner of that conveyance to have been committed or omitted without the owner's knowledge or consent.

(*iii*) A forfeiture of a conveyance encumbered by a bona fide security interest is subject to the interest of the secured party who neither had knowledge of nor consented to the act or omission.

(c) Books, records, computers, electronic equipment, and research products and materials, including microfilm, digital media, tapes, and data, used or intended for use in violation of this act.

(d) Any money, negotiable instruments, securities, or any other thing of value that is found in close proximity to any property that is subject to forfeiture under subdivision (a), (b), or (c) is presumed to be subject to forfeiture. This presumption may be rebutted by clear and convincing evidence.

(2) Property used to commit a violation of this act is not subject to forfeiture unless the owner of the property actively participates in or consents to the violation of this act.

(3) Property of any of the following providers is not subject to forfeiture under this act unless it is determined that the provider is a consenting party or privy to a violation of this act:

(a) A telecommunication provider.

(b) An internet service provider.

(c) A computer network service provider.

(d) An interactive computer service provider.

History: Add. 2010, Act 315, Eff. Apr. 1, 2011.

445.79a Seizure of forfeited property; seizure without process; circumstances.

Sec. 19a. Property that is subject to forfeiture under this act may be seized upon process issued by the circuit court having jurisdiction over the property. Seizure without process may be made under any of the following circumstances:

(a) The property is seized incident to a lawful arrest, pursuant to a search warrant, or pursuant to an inspection under an administrative inspection warrant.

(b) The property is the subject of a prior judgment in favor of this state in an injunction or forfeiture proceeding under this act.

(c) There is probable cause to believe that the property is directly or indirectly dangerous to health or safety.

(d) There is probable cause to believe that the property was used or is intended to be used in violation of this act.

(e) There is probable cause to believe that the property is the proceeds from activity in violation of this act.

History: Add. 2010, Act 314, Eff. Apr. 1, 2011.

445.79b Seizure without process of property not exceeding $50,000.00; procedure; powers of seizing agency; title; examination of seized money; return of money; burden of proof.

Sec. 19b. (1) If property is seized pursuant to section 19a, forfeiture proceedings shall be instituted promptly. If the property is seized without process as provided under section 19a and the total value of the

property seized does not exceed $50,000.00, the following procedure shall be used:

(a) The local unit of government that seized the property or, if the property was seized by the state, the state shall notify the owner of the property that the property has been seized and that the local unit of government or, if applicable, the state intends to forfeit and dispose of the property by delivering a written notice to the owner of the property or by sending the notice to the owner by certified mail. If the name and address of the owner are not reasonably ascertainable or delivery of the notice cannot be reasonably accomplished, the notice shall be published in a newspaper of general circulation in the county in which the property was seized, for 10 successive publishing days.

(b) Unless all criminal proceedings involving or relating to the property have been completed, the seizing agency shall immediately notify the prosecuting attorney for the county in which the property was seized or, if the attorney general is actively handling a case involving or relating to the property, the attorney general of the seizure of the property and the intention to forfeit and dispose of the property.

(c) Any person claiming an interest in property that is the subject of a notice under subdivision (a) may, within 20 days after receipt of the notice or of the date of the first publication of the notice, file a written claim signed by the claimant with the local unit of government or the state expressing his or her interest in the property. The person filing the claim shall give a bond to the local unit of government or the state in the amount of 10% of the value of the claimed property, but not less than $250.00 or greater than $5,000.00, with sureties approved by the local unit of government or the state containing the condition that if the property is ordered forfeited by the court the obligor shall pay all costs and expenses of the forfeiture proceedings. The local unit of government or, if applicable, the state shall transmit the claim and bond with a list and description of the property seized to the attorney general, the prosecuting attorney for the county, or the city or township attorney for the local unit of government in which the seizure was made. The attorney general, the prosecuting attorney, or the city or township attorney shall promptly institute forfeiture proceedings after the expiration of the 20-day period. However, unless all criminal proceedings involving or relating to the property have been completed, a city or township attorney shall not institute forfeiture proceedings without the consent of the prosecuting attorney or, if the attorney general is actively handling a case involving or relating to the property, the attorney general.

(d) If no claim is filed or bond given within the 20-day period as described in subdivision (c), the local unit of government or the state shall declare the property forfeited and shall dispose of the property as provided under section 19c. However, unless all criminal proceedings involving or relating to the property have been completed, the local unit of government or the state shall not dispose of the property under this subdivision without the written consent of the prosecuting attorney or, if the attorney general is actively handling a case involving or relating to the property, the attorney general.

(2) Property taken or detained under this act is not subject to an action to recover personal property, but is considered to be in the custody of the seizing agency subject only to this section or an order and judgment of the court having jurisdiction over the forfeiture proceedings. When property is seized under this act, the seizing agency may do any of the following:

(a) Place the property under seal.

(b) Remove the property to a place designated by the court.

(c) Take custody of the property and remove it to an appropriate location for disposition in accordance with law.

(d) Deposit money seized under this act into an interest-bearing account in a financial institution. As used in this subdivision, "financial institution" means a state or nationally chartered bank or a state or federally chartered savings and loan association, savings bank, or credit union whose deposits are insured by an agency of the United States government and that maintains a principal office or branch office located in this state under the laws of this state or the United States.

(3) Title to real property forfeited under this act shall be determined by a court of competent jurisdiction. A forfeiture of real property encumbered by a bona fide security interest is subject to the interest of the secured party who neither had knowledge of nor consented to the act or omission.

(4) An attorney for a person who is charged with a crime involving or related to the money seized under this act has 60 days within which to examine that money. This 60-day period begins to run after notice is given under subsection (1)(a) but before the money is deposited into a financial institution under subsection (2)(d). If the attorney general, prosecuting attorney, or city or township attorney fails to sustain his or her burden of proof in forfeiture proceedings under this act, the court shall order the return of the money, including any interest earned on money deposited into a financial institution under subsection (2)(d).

History: Add. 2010, Act 314, Eff. Apr. 1, 2011.

445.79c Forfeited property; powers of local government or state; appointment and authority

of receiver; payment of expenses.

Sec. 19c. (1) When property is forfeited under this act, the local unit of government that seized the property may do any of the following or, if the property is seized by or in the custody of the state, the state may do any of the following:

(a) Retain it for official use.

(b) Sell that which is not required to be destroyed by law and which is not harmful to the public. The proceeds and any money, negotiable instruments, securities, or any other thing of value as described in section 19(d) that are forfeited under this act shall be deposited with the treasurer of the entity having budgetary authority over the seizing agency and applied as follows:

(*i*) For the payment of proper expenses of the proceedings for forfeiture and sale, including expenses incurred during the seizure process, maintenance of custody, advertising, and court costs, except as otherwise provided in subsection (3).

(*ii*) The balance remaining after the payment of expenses shall be distributed by the court having jurisdiction over the forfeiture proceedings to the treasurer of the entity having budgetary authority over the seizing agency. If more than 1 agency was substantially involved in effecting the forfeiture, the court having jurisdiction over the forfeiture proceeding shall equitably distribute the money among the treasurers of the entities having budgetary authority over the seizing agencies. The money received by a seizing agency under this subparagraph and all interest and other earnings on money received by the seizing agency under this subparagraph shall be used to enhance law enforcement efforts as appropriated by the entity having budgetary authority over the seizing agency. A distribution made under this subparagraph shall serve as a supplement to, and not a replacement for, the funds budgeted on the date that the amendatory act that added this section takes effect for law enforcement efforts pertaining to this act.

(c) Take custody of the property and remove it for disposition in accordance with law.

(2) In the course of selling real property under subsection (1)(b), the court that has entered an order of forfeiture may, on motion of the agency to whom the property has been forfeited, appoint a receiver to dispose of the real property forfeited. The receiver shall be entitled to reasonable compensation. The receiver shall have authority to do all of the following:

(a) List the forfeited real property for sale.

(b) Make whatever arrangements are necessary for the maintenance and preservation of the forfeited real property.

(c) Accept offers to purchase the forfeited real property.

(d) Execute instruments transferring title to the forfeited real property.

(3) If a court enters an order of forfeiture, the court may order a person who claimed an interest in the forfeited property under section 19b(1)(c) to pay the expenses of the proceedings of forfeiture to the entity having budgetary authority over the seizing agency.

History: Add. 2010, Act 314, Eff. Apr. 1, 2011.