Act No. 315
Public Acts of 2010
Approved by the Governor
December 21, 2010
Filed with the Secretary of State
December 21, 2010
EFFECTIVE DATE: April 1, 2011

STATE OF MICHIGAN
95TH LEGISLATURE
REGULAR SESSION OF 2010

Introduced by Senators Basham, Jelinek and Jacobs

ENROLLED SENATE BILL No. 223

AN ACT to amend 2004 PA 452, entitled "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," by amending sections 9, 11, 12, and 12b (MCL 445.69, 445.71, 445.72, and 445.72b), sections 12 and 12b as added by 2006 PA 566, and by adding section 19.

The People of the State of Michigan enact:

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.

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.

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.

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.

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.

Enacting section 1. This amendatory act takes effect April 1, 2011.

Enacting section 2. This amendatory act does not take effect unless all of the following bills of the 95th Legislature are enacted into law:

(a) Senate Bill No. 225.

(b) Senate Bill No. 226.

(c) House Bill No. 4325.

Carol Morey Viventi

Secretary of the Senate

Richard J. Brown

Clerk of the House of Representatives

Approved .....

.....

Governor