HOUSE BILL No. 4983

September 19, 2017, Introduced by Reps. Hammoud, Zemke, Gay-Dagnogo, Geiss, Wittenberg, Lucido, Schor, Chang and Jones and referred to the Committee on Communications and Technology.

A bill to amend 2004 PA 452, entitled

"Identity theft protection act,"

by amending section 12 (MCL 445.72), as amended by 2010 PA 315.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

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.

HOUSE BILL No. 4983

(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~~ **PROVIDE THE DATE OF THE BREACH AND 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~~ **AFTER** a person or agency provides a notice under this section, the person or agency shall **DO ALL OF THE FOLLOWING:**

(A) EXCEPT AS PROVIDED IN THIS SUBDIVISION, 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~~ **SUBDIVISION** 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~~ **SUBDIVISION** does not apply if either of the following is met:

(*i*) ~~(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.

(*ii*) ~~(b)~~ The person or agency is subject to 15 USC 6801 to 6809.

(B) POST THE NOTICE IN A PROMINENT AND CONSPICUOUS PLACE ON ITS INTERNET WEBSITE THAT IS FULLY ACCESSIBLE TO ITS CUSTOMERS AND THE PUBLIC. IN ADDITION, THE PERSON OR AGENCY SHALL ENSURE THAT THE WEBSITE INCLUDES THE FOLLOWING INFORMATION ABOUT ALL OF ITS SECURITY BREACHES SORTED CHRONOLOGICALLY ACCORDING TO THE DATE OF EACH BREACH:

(*i*) IF THE PERSON OR AGENCY PROVIDED NOTICE OF THE BREACH UNDER STATE OR FEDERAL LAW, A COPY OF THAT NOTICE.

(*ii*) IF THE PERSON OR AGENCY DID NOT PROVIDE NOTICE OF THE BREACH, THE DATE AND A GENERAL DESCRIPTION OF THE SECURITY BREACH; A DESCRIPTION OF THE TYPE OF PERSONAL INFORMATION THAT WAS THE SUBJECT OF THE UNAUTHORIZED ACCESS OR USE; AND A GENERAL DESCRIPTION OF ANY ACTION TAKEN BY THE PERSON OR AGENCY IN CONNECTION WITH THAT SECURITY BREACH TO PROTECT DATA FROM FURTHER UNAUTHORIZED ACCESS OR USE.

(C) IF THE PERSON OR AGENCY CONDUCTS BUSINESS IN THIS STATE AND IN CONNECTION WITH THAT BUSINESS REQUESTS PERSONAL IDENTIFYING

INFORMATION FROM AN INDIVIDUAL, NOTIFY THE INDIVIDUAL THAT INFORMATION ABOUT THE PERSON'S OR AGENCY'S SECURITY BREACH HISTORY IS AVAILABLE AT ITS WEBSITE DESCRIBED IN SUBDIVISION (B).

(D) PROVIDE ALL OF THE INFORMATION IT POSTS ON ITS WEBSITE UNDER SUBDIVISION (B) TO THE DEPARTMENT OF THE ATTORNEY GENERAL.

(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.

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