HOUSE BILL No. 6522

September 14, 2006, Introduced by Reps. Angerer, Sheltrown, Zelenko, Lemmons, Jr., Gonzales, Clemente, Miller, Bennett, Byrum, Polidori, Farrah, Anderson, Tobocman, Kolb, Lipsey, Byrnes, Mayes, Gleason, Condino, Accavitti, Clack, Murphy, Cushingberry, Vagnozzi, McDowell, Williams, Kathleen Law, Hopgood, Hood, Hunter, Donigan, Adamini, Alma Smith, Sak, Brown, Virgil Smith, Bieda, Gillard, Dillon and Lemmons, III and referred to the Committee on Judiciary.

A bill to require certain notices regarding unauthorized access to personal identifying information; to establish procedures for notice; and to provide remedies and civil sanctions.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

Sec. 1. This act shall be known and may be cited as the "information privacy protection act".

Sec. 2. The legislature finds all of the following:

(a) The privacy and financial security of individuals is increasingly at risk due to the ever more widespread collection of personal information by both the private and public sectors.

(b) Credit card transactions, magazine subscriptions, telephone numbers, real estate records, motor vehicle

HOUSE BILL No. 6522

registrations, consumer surveys, warranty registrations, credit reports, and websites are all sources of personal information and form the source material for identity thieves.

(c) Identity theft is 1 of the fastest growing crimes committed in the United States and this state.

(d) Criminals who steal personal information such as social security numbers use the information to open credit card accounts, write bad checks, buy cars, and commit other financial crimes with other people's identities.

(e) Identity theft is costly to the marketplace and to consumers.

(f) Residents of this state are entitled to notice of unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of their private personal information.

Sec. 3. As used in this act:

(a) "Data" includes any of the following:

(*i*) Computerized data.

(*ii*) Noncomputerized data that is maintained or stored on paper, microfilm, or other form of record-keeping or storage medium.

(b) "Major credit reporting agency" means a consumer reporting agency that compiles and maintains files on a nationwide basis as defined in 15 USC 1681a(p).

(c) "Person" means an individual, partnership, limited liability company, association, corporation, public or nonpublic elementary or secondary school, trade school, vocational school,

community or junior college, college, university, state or local governmental agency or department, or other legal entity.

(d) "Personal identifying information" means that term as defined in section 3 of the identity theft protection act, 2004 PA 452, MCL 445.63.

(e) "Security breach" means an unauthorized acquisition of data that compromises the security, confidentiality, or integrity of the personal identifying information of 1 or more individuals maintained by a person. The term includes an unauthorized acquisition of encrypted records or data containing personal identifying information if the encryption key is also acquired. The term also includes the unauthorized photocopying or facsimile or other paper-based transmission of documents containing personal identifying information. The term does not include good-faith acquisition of personal identifying information by an employee or agent of the person related to the legitimate activities of the person if the personal identifying information is not used or subject to further unauthorized disclosure.

Sec. 4. (1) A person that owns, uses, or maintains data that includes personal identifying information concerning a resident of this state shall provide notice of a security breach to that resident under this section after the person is notified of the security breach, discovers the security breach, or discovers evidence from which a reasonable person would conclude that a security breach has occurred.

(2) A notice provided under this section shall include both of the following:

(a) To the extent possible, a description of the categories of personal identifying information that was, or is reasonably believed to have been, acquired by an unauthorized person.

(b) A toll-free telephone number or website that the recipient of the notice may use to contact the person or an agent of the person and from which the recipient may learn all of the following:

(*i*) The types of information the person maintained or stored about the recipient or about individuals in general.

(*ii*) Whether or not the person maintained or stored information about the recipient.

(*iii*) The toll-free contact telephone numbers and addresses for the major credit reporting agencies.

(3) If a person discovers circumstances that require the person to provide notice under this section to more than 500 individuals at 1 time, the person shall also notify all of the major credit reporting agencies within 48 hours.

(4) A person shall provide any notice required under this section in the most expedient time possible and without unreasonable delay, unless 1 or both of the following apply:

(a) Delay is necessary to determine the scope of the security breach and restore the reasonable integrity of the data system.

(b) A law enforcement agency determines that providing notice will impede a criminal investigation. However, the person shall provide the notice after the law enforcement agency determines that disclosure will not compromise the investigation.

(5) A person shall provide notice required under this section by any of the following methods:

(a) Written notice sent by first-class mail, address correction requested.

(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 101 of title I of the electronic signatures in global and national commerce act, 15 USC 7001.

(c) Substitute notice, if the person demonstrates that the cost of providing notice under subdivision (a) or (b) will exceed $250,000.00, that the person has to provide notice to more than 500,000 individuals, or that the person does not have sufficient contact information for the individuals or licensees it is required to notify under that subsection. A person provides substitute notice under this subdivision by doing all of the following:

(*i*) Providing notice by e-mail to those individuals for whom the agency or person has e-mail addresses.

(*ii*) If the person maintains a website, conspicuously posting the notice on that website.

(*iii*) Notifying major statewide media. A notification under this subparagraph shall include the toll-free telephone number or website described in subsection (2)(b).

(*iv*) If the person maintains, as part of an information security policy for the treatment of personal identifying information, its own notification procedures for security breaches that are consistent with the time requirements of this section, notifying the individuals in accordance with those procedures.

Sec. 5. (1) An individual injured by a violation of section 4 may bring a civil action against the person that violated section 4

and recover his or her actual damages or $500.00, whichever is greater.

(2) The attorney general or a county prosecuting attorney may bring an action against a person that violated section 4 and recover a civil fine in 1 of the following amounts, whichever is less:

(a) An amount equal to $500.00 for each violation of section 4 by the person.

(b) An amount equal to $250,000.00 for each day that a violation occurs.

(3) If the attorney general or an individual, class of individuals, or county prosecuting attorney prevails in an action described in this section, the court shall award that prevailing party actual costs and reasonable attorney fees in connection with the action.

(4) An individual described in subsection (1) or the attorney general may bring a class action on behalf of individuals whose personal identifying information was the subject of a security breach.

Sec. 6. (1) A notifying person may bring an action against any person who unlawfully obtains or benefits from personal identifying information obtained from data maintained or stored by the notifying person.

(2) The court may award a notifying person that prevails in an action described in this section damages that include, but are not limited to, the reasonable costs of providing notice, reasonable attorney fees and actual costs in connection with the action, and

punitive damages if the court finds them appropriate.

(3) As used in this section:

(a) "Costs of providing notice" includes, but is not limited to, the costs of labor, materials, and postage and any other costs reasonably related to providing a notice under this act.

(b) "Notifying person" means a person that is required to provide notice under this act.

Sec. 7. (1) The rights, liabilities, and remedies created by this act are in addition to any others provided by law.

(2) A waiver of any right to receive notice under this act is contrary to public policy and is void and unenforceable.

Enacting section 1. This act takes effect January 1, 2007.