SENATE BILL NO. 672

October 05, 2021, Introduced by Senators SCHMIDT, HOLLIER, HORN, BULLOCK and VANDERWALL and referred to the Committee on Energy and Technology.

A bill to amend 2004 PA 452, entitled "Identity theft protection act,"
(MCL 445.61 to 445.79d) by amending the title, as amended by 2006 PA 566, and by adding section 12c.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

1 TITLE
2 An act to prohibit certain acts and practices concerning identity theft; to address certain identity theft and security breach practices; 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;
to provide certain affirmative defenses; and to repeal acts and
parts of acts.

Sec. 12c. (1) A covered entity is entitled to an affirmative
defense to any tort cause of action that alleges that the covered
entity's failure to implement reasonable information security
controls resulted in a security breach if the covered entity
demonstrates all of the following:

(a) The covered entity established, maintained, and reasonably
complied with a written cybersecurity program that contains
administrative, technical, and physical safeguards for the
protection of personal information and personal identifying
information that reasonably conforms to the current version of an
industry-recognized cybersecurity framework or standard described
in subsection (2) or a combination of the current versions of
industry-recognized cybersecurity frameworks or standards described
in subsection (2).

(b) The covered entity's cybersecurity program is designed to
do all of the following:

(i) Protect the security and confidentiality of personal
information and personal identifying information.

(ii) Protect against anticipated threats or hazards to the
security or integrity of personal information and personal
identifying information.

(iii) Protect against unauthorized access to and acquisition of
personal information and personal identifying information that is
likely to result in a material risk of identity theft to the
individual to whom the personal information and personal identifying information relate.

(c) The scale and scope of the covered entity's cybersecurity program is appropriate based on the factors in subsection (3).

(2) An industry-recognized cybersecurity framework or standard means any of the following, as applicable:

(a) The Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology.

(b) The National Institute of Standards and Technology's Special Publication 800-171.

(c) The National Institute of Standards and Technology's Special Publications 800-53 and 800-53a.


(e) The Center for Internet Security Critical Security Controls for Effective Cyber Defense.


(g) If the covered entity is regulated by this state, the federal government, or both, or is otherwise subject to any of the laws or regulations listed in this subdivision, any of the following, as applicable:

(i) The security requirements under the health insurance portability and accountability act of 1996, Public Law 104-191, or the regulations promulgated under that act, 45 CFR parts 160 and 164.

(ii) Title V of the Gramm-Leach-Bliley act, 15 USC 6801 to


(h) The Payment Card Industry Data Security Standard.

(i) The Information Systems Audit and Control Association's Control Objectives for Information Related Technology.

(3) A covered entity's cybersecurity program is appropriate if it is based on all of the following factors:

(a) The size and complexity of the covered entity.

(b) The nature and scope of the activities of the covered entity.

(c) The sensitivity of the information to be protected.

(d) The cost and availability of tools to improve information security and reduce vulnerabilities.

(e) The resources available to the covered entity.

(4) When a final revision to an industry-recognized cybersecurity framework or standard listed in subsection (2) is published or when an industry-recognized cybersecurity framework or standard under subsection (2) is amended, a covered entity whose cybersecurity program reasonably conforms to that framework or standard shall reasonably conform to the revised or amended framework or standard not later than 1 year after the publication date of the revision or amendment.

(5) This section does not provide a private right of action, including a class action, with respect to any act or practice under this section.

(6) It is the strong policy of this state to apply the laws of
this state to entities that do business in this state in order to incentivize conformance to a recognized cybersecurity standard or framework.

(7) If there is a choice of law provision in an agreement that designates this state as the governing law, this section must be applied, if applicable, to the fullest extent possible in a civil action brought against a person regardless of whether the civil action is brought in this state or another state.

(8) As used in this section, "covered entity" means a person that accesses, maintains, communicates, or processes personal information or personal identifying information in or through 1 or more systems, networks, or services located in or outside of this state.