

**SUBSTITUTE FOR
SENATE BILL NO. 672**

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
3 identity theft; **to address certain identity theft and security**
4 **breach practices;** to require notification of a security breach of a
5 database that contains certain personal information; to provide for
6 the powers and duties of certain state and local governmental
7 officers and entities; to prescribe penalties and provide remedies;
8 **to provide certain affirmative defenses;** and to repeal acts and



1 parts of acts.

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

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

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

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

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

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

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



1 (d) For its cybersecurity program under subdivision (a), the
2 covered entity attained and maintained a third-party certification
3 that is aligned with the current version of the industry-recognized
4 cybersecurity framework or standard to which the covered entity's
5 cybersecurity program reasonably conforms.

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

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

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

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

15 (d) The Federal Risk and Authorization Management Program
16 Security Assessment Framework.

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

19 (f) The International Organization for
20 Standardization/International Electrotechnical Commission 27000
21 Family Information Security Management Systems.

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

26 (i) The security requirements under the health insurance
27 portability and accountability act of 1996, Public Law 104-191, or
28 the regulations promulgated under that act, 45 CFR parts 160 and
29 164.



1 (ii) Title V of the Gramm-Leach-Bliley act, 15 USC 6801 to
2 6827.

3 (iii) The federal information security modernization act of
4 2014, Public Law 113-283.

5 (iv) The Federal Financial Institutions Examination Council's
6 Information Security Standards.

7 (h) The Payment Card Industry Data Security Standard.

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

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

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

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

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

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

18 (e) The resources available to the covered entity.

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

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



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

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

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

