Senate Fiscal Agency
P.O. Box 30036
Lansing, Michigan 48909-7536

BILL ANALYSIS

Telephone: (517) 373-5383
Fax: (517) 373-1986

Senate Bill 672 (Substitute S-2 as passed by the Senate)
Sponsor: Senator Wayne A. Schmidt
Committee: Energy and Technology

Date Completed: 3-15-22

CONTENT

The bill would amend the Identity Theft Protection Act to do the following:

-- Specify that a covered entity would be entitled to an affirmative defense to any tort cause of action that alleged that the covered entity's failure to implement reasonable information security controls resulted in a security breach if the covered entity demonstrated that its cybersecurity program met requirements prescribed by the bill, as applicable.
-- Specify that the bill would not provide a private right of action, including a class action, with respect to any act or practice under the bill.
-- Specify that if there were a choice of law provision in an agreement that designated the State as the governing law, the bill would have to be applied, if applicable, to the fullest extent possible in a civil action brought against a person regardless of whether the civil action was brought in the State or another state.

Cybersecurity Program Requirements

Under the bill, a covered entity would be entitled to an affirmative defense to any tort cause of action that alleged that the covered entity's failure to implement reasonable information security controls resulted in a security breach if the covered entity demonstrated that its cybersecurity program met the requirements described below, as applicable. "Covered entity" would mean a person that accesses, maintains, communicates, or processes personal information or personal identifying information in or through one or more systems, networks, or services located in or outside of the State.

A covered entity would be entitled to the affirmative defense described above if it demonstrated that it established, maintained, and reasonably implemented and complied with a written cybersecurity program that contained administrative, technical, and physical safeguards for the protection of personal information and personal identifying information that reasonably conformed to the current version of an industry-recognized cybersecurity framework or standard described below, or a combination of the current versions of industry-recognized cybersecurity frameworks or standards described below.

In addition, the covered entity's cybersecurity program would have to be designed to do the following:

-- Protect the security and confidentiality of personal information and personal identifying information.
-- Protect against anticipated threats or hazards to the security or integrity of personal information and personal identifying information.

-- Protect against unauthorized access to and acquisition of personal information and personal identifying information that was likely to result in a material risk of identity theft to the individual to whom the information related.

The scale and scope of the covered entity's cybersecurity program would have to be appropriate. A covered entity's program would be appropriate if it were based on all of the following factors:

-- The size and complexity of the covered entity.
-- The nature and scope of the activities of the covered entity.
-- The sensitivity of the information to be protected.
-- The cost and availability of tools to improve information security and reduce vulnerabilities.
-- The resources available to the covered entity.

The bill also specifies that, except as otherwise provided below, a covered entity's cybersecurity program would have to attain and maintain a third-party certification that was aligned with the current version of the industry-recognized cybersecurity framework or standard to which its cybersecurity program reasonably conformed. If a covered entity were a financial institution and did not meet the requirement described above, the covered entity would be subject to regular examination or audit by a State or Federal regulatory agency that had oversight over the covered entity.

Recognized Cybersecurity Frameworks & Standards

The bill specifies that an industry recognized cybersecurity framework or standard would mean any of the following, as applicable:

-- The Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology (NIST).
-- The NIST's Special Publications 800-171, 800-53, and 800-53a.
-- The Federal Risk and Authorization Management Program Security Assessment Framework.
-- The Center for Internet Security Critical Security Controls for Effective Cyber Defense.
-- The International Organization for Standardization/International Electrotechnical Commission 27000 Family Information Security Management Systems.
-- The Payment Card Industry Data Security Standard.
-- The Information Systems Audit and Control Association's Control Objectives for Information Related Technology.

In addition, if the covered entity were regulated by the State, the Federal government, or both, or was otherwise subject to any of the laws or regulations listed below, an industry recognized cybersecurity framework or standard would mean any of the following, as applicable:

-- The security requirements under the Health Insurance Portability and Accountability Act, or applicable Federal regulations.
-- Title V of the Gramm-Leach-Bliley Act.
-- The Federal Information Security Modernization Act.
-- The Federal Financial Institutions Examination Council's Information Security Standards.

When a final revision to an industry-recognized cybersecurity framework or standard listed above was published or if the framework or standard were amended, a covered entity whose cybersecurity program reasonably conformed to that framework or standard would have to

reasonably conform to the revised or amended framework or standard within one year after date the revision or amendment was published.

Applicability & Other Provisions

The bill specifies that it would not provide a private right of action, including a class action, with respect to any act or practice under the bill.

If there were a choice of law provision in an agreement that designated the State as the governing law, the bill would have to be applied, if applicable, to the fullest extent possible in a civil action brought against a person regardless of whether the civil action was brought in the State or another state.

The bill also states that "[i]t 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".

Proposed MCL 445.72c

Legislative Analyst: Tyler VanHuyse

FISCAL IMPACT

The bill likely would have no fiscal impact on State or local government. The bill would not generate or spend State or local funds, and it would be more likely than not to discourage the filing of civil complaints for negligence against covered entities.

Fiscal Analyst: Michael Siracuse

SAS\S2122\s672sb