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: 8-23-22

RATIONALE

A database security breach occurs when there is unauthorized access to data held by an entity, such as a business. These breaches can result in data compromises, such as the theft of an individual's social security number. According to the Identity Theft Resource Center (ITRC), a nonprofit organization that provides information to consumers concerning identity crime, the number of data compromises increased by 68% in 2021, for a total of 1,862 compromises. The ITRC specifies that most of these compromises occurred because of cyberattacks on private businesses' databases. One way for a business to prevent successful cyberattacks is to adopt and maintain a cybersecurity program, and some people believe that businesses should be encouraged to do so. Accordingly, it has been suggested that a business be offered an affirmative defense to a tort cause of action brought because of a breach if the business demonstrated that its cybersecurity program met certain requirements.

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

ARGUMENTS

(Please note: The arguments contained in this analysis originate from sources outside the Senate Fiscal Agency. The Senate Fiscal Agency neither supports nor opposes legislation.)

Supporting Argument

Legislation should encourage businesses to adopt cybersecurity programs for the prevention of data security breaches. However, the approach that legislation uses to encourage businesses is important, and previous legislation has taken the wrong approach. For example, House Bills 4186 and 4187 of the 2019-20 Legislative Session would have required businesses to implement security measures, such as cybersecurity programs, or otherwise be in violation of the proposed language. This approach, based on negative consequences for noncompliance, may have ignored the significant costs associated with adopting those measures. According to a 2020 survey concerning cybersecurity measures initiated by Deloitte, a consulting firm, businesses spend approximately $2,691 on cybersecurity per full-time employee.[1] These costs can be prohibitive, especially for smaller businesses. The approach ultimately did not have enough business or political support to make it through the legislative process, evidenced by the Governor's pocket veto after the end of the Session.

Legislation offering an incentive to adopt cybersecurity programs for the prevention of data security breaches is a better approach. Encouraging businesses in this way acknowledges the expenses associated with cybersecurity programs and provides businesses with the flexibility to achieve and maintain cybersecurity in a manner that works for them. The bill would offer an affirmative defense for certain tort causes of action associated with the failure to implement reasonable information security controls. This would encourage businesses, without the use of negative consequences, to adopt and implement cybersecurity measures and to protect their customers' personal data from compromise.

Opposing Argument

Equifax, a consumer credit reporting agency, announced in 2017 that its consumer database was breached, and that the security breach exposed the personal information of 147 million people. The Federal Trade Commission (FTC), which regulates business practices in the United States,

[1] "Reshaping the Cybersecurity Landscape", www.deloitte.com. Retrieved 8-19-2022.

could not bring enforcement action against Equifax under Section 5 (Unfair or Deceptive Acts or Practices) of the FTC Act and so many consumers that had personal information exposed in the data breach joined class action lawsuits. According to testimony before the Senate Committee on Energy and Technology, attorneys for the class action lawsuits established their cases on states' cybersecurity statutes, Section 5 of the FTC Act, and tort causes of action, such as negligence. Equifax moved to dismiss the tort cause of action, arguing that it had significant cybersecurity standards in place, however, the court denied the motion. Equifax eventually settled with the FTC, the Consumer Protection Financial Bureau, and 50 US states and territories before trial. As part of the settlement agreement, people affected by the data breach may file claims for certain expenses associated with the data breach.

Although Equifax eventually settled the case, the court's denial of the motion to dismiss the tort cause of action demonstrates the value of this claim to consumers affected by database security breaches. The bill would offer an affirmative defense against a tort cause of action, such as negligence, to certain entities that met its prescribed cybersecurity program requirements. If passed before the Equifax incident, this affirmative defense could have inhibited affected Michigan consumers from filing claims for expenses associated with the exposure of their personal information from large companies that can afford to provide meaningful data protections for their customers. Data breaches continue to increase, and the affirmative defense offered by the bill could limit potential compensation for consumers affected in the future.

Legislative Analyst: Tyler P. 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\s672a

This analysis was prepared by nonpartisan Senate staff for use by the Senate in its deliberations and does not constitute an official statement of legislative intent.