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

BILL ANALYSIS

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

House Bill 6491 (Substitute S-3 as reported)
Sponsor: Representative Lana Theis
House Committee: Insurance
Senate Committee: Finance

CONTENT

The bill would create Chapter 5A (Data Security) under the Insurance Code, which would do the following:

-- Require a licensee to develop, implement, and maintain a comprehensive written information security program that contained administrative, technical, and physical safeguards for the protection of nonpublic information and its information system.
-- List criteria an information security program would have to meet.
-- Specify further requirements a licensee would have to adhere to regarding security and security protocols.
-- Require the board of directors or an appropriate committee of the board, if the licensee had a board, to require the licensee's executive management to develop, implement, and maintain its information security program; and require its executive management to report at least annually in writing certain information.
-- Require a licensee to monitor, evaluate, and adjust, as appropriate, the information security program consistent with certain changes listed in the bill.
-- Require each licensee to establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromised certain information or systems, and list what the plan would have to address.
-- Require each insurer domiciled in the State, by February 15 of each year, to submit to the Director of the Department of Insurance and Financial Services (DIFS) a written statement, certifying that the insurer was in compliance with Chapter 5A.
-- Require each insurer to maintain for examination by the DIFS all records, schedules, and data supporting the certificate for five years.
-- Require the licensee or an outside vendor or service provider, or both, designated to act on behalf of the licensee, to conduct a prompt investigation if the licensee learned that a cybersecurity event had or could have occurred.
-- Require the licensee to maintain records concerning all cybersecurity events for at least five years from the date of the event.
-- Require each licensee to notify the Director within 10 business days after a determination that a cybersecurity event had occurred involving nonpublic information that was in the possession of a licensee.
-- Specify other notification conditions pertaining to a cybersecurity event involving nonpublic information.
-- Require a licensee that owned or licensed data that were included in a database that discovered a security breach, or received notice of a security breach, to provide a notice of the security breach to each resident of the State if certain conditions were met.
-- List the methods by which a licensee could provide notice of a security breach to a resident of the State.

-- Require a licensee to notify each consumer reporting agency that compiled and maintained files on consumers on a nationwide basis of a security breach under certain circumstances.
-- Specify that a person who provided notice of a security breach when a security breach had not occurred, with the intent to defraud, would be guilty of a misdemeanor punishable as described in Chapter 5A.
-- Specify that a person who knowingly failed to provide a notice of a security breach would be ordered to pay a civil fine.
-- Specify that certain notification provisions would preempt any charter, ordinance, resolution, regulation, rule, or other action by a municipal corporation or other political subdivision of the State to regulate those matters.
-- Specify that any documents, materials, or other information in the control or possession of the DIFS or its Director relating to Chapter 5A would be confidential by law and privileged.
-- List actions the Director could take to assist in the performance of his or her duties under Chapter 5A.
-- List the entities that would be exempt from Chapter 5A or certain provisions specified in Chapter 5A.

Chapter 5A would take effect on January 20, 2021. A licensee would have to implement provisions regarding the information security program and other specified licensee requirements by January 20, 2022. However, a licensee would have until January 20, 2023, to require a third-party service provider to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that were accessible to, or held by, the third-party service provider.

Legislative Analyst: Drew Krogulecki

FISCAL IMPACT

The bill would have an indeterminate negative fiscal impact on the Department of Insurance and Financial Services (DIFS). The bill would create a number of responsibilities for the DIFS Director that could result in increased administrative costs. However, the magnitude of these costs would depend on the number of licensees who experienced security events prompting review and action by DIFS. Existing appropriations likely would be sufficient to cover the majority of these costs.

Otherwise, the bill would have no fiscal impact on the State or local government. Licensed insurers are currently subject to the Identity Theft Protection Act. Per Michigan Compiled Laws 445.72, 445.72a, and 445.72b, all misdemeanor offenses and civil fines outlined in the bill would remain the same as current law.

Date Completed: 12-17-18

Fiscal Analyst: Abbey Frazier
Elizabeth Raczkowski