

Department of Legislative Services
Maryland General Assembly
2019 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

Senate Bill 30

(Chair, Finance Committee)(By Request - Departmental -
Maryland Insurance Administration)

Finance

Economic Matters

Insurance - Breach of Security of a Computer System - Notification Requirement

This departmental bill requires a “carrier” to notify the Insurance Commissioner of a “breach of the security of a system” if the carrier (1) conducts a specified investigation and (2) determines that the breach creates a likelihood that “personal information” has been or will be misused. Notice must be provided on a form and in a manner approved by the Commissioner and at the same time the carrier provides notice, as required under current law, to the Office of the Attorney General (OAG). Compliance with the bill does not relieve a carrier from a duty to comply with other requirements of State or federal law relating to the protection and privacy of “personal information.”

Fiscal Summary

State Effect: The bill does not substantively change State activities, operations, or finances.

Local Effect: None.

Small Business Effect: The Maryland Insurance Administration (MIA) has determined that this bill has minimal or no impact on small business (attached). The Department of Legislative Services concurs with this assessment. (The attached assessment does not reflect amendments to the bill.)

Analysis

Current Law: Under the Commercial Law Article, “breach of the security of a system” means the unauthorized acquisition of computerized data that compromises the security,

confidentiality, or integrity of the personal information maintained by a business. “Breach of the security of a system” does not include the good faith acquisition of personal information by an employee or agent of a business for the purposes of the business, provided that the personal information is not used or subject to further unauthorized disclosure.

“Personal information” means an individual’s first name or first initial and last name in combination with any one or more of the following data elements when not encrypted, redacted, or otherwise protected: (1) a Social Security number, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government; (2) a driver’s license or State identification card number; (3) an account number, a credit card number, or a debit card number, in combination with any required code or password that permits access to an individual’s financial account; (4) health information; (5) a health insurance policy or certificate number or subscriber identification number, in combination with a unique identifier that permits access to an individual’s health information; or (6) specified biometric data that can be used to uniquely authenticate the individual’s identity when the individual accesses a system or account. “Personal information” also includes a user name or email address in combination with a password or security question and answer that permits access to the account. “Personal information” does not include publicly available information that is lawfully made available, information that an individual has consented to have publicly disseminated or listed, or information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act.

Under the Maryland Personal Information Protection Act, to protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of a Maryland resident must implement and maintain reasonable and appropriate security procedures and practices. A business that uses a nonaffiliated third party as a service provider and discloses personal information about a Maryland resident under a written contract with the third party must require, by contract, that the third party implement and maintain reasonable security procedures and practices.

A business that owns or licenses computerized data that includes personal information of a Maryland resident, upon the discovery or notification of a breach of the security of a system, must conduct, in good faith, a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused as a result of the breach.

If, after the investigation, the business reasonably believes that the breach has resulted or will result in the misuse of personal information of a Maryland resident, the business must notify the individual of the breach. Prior to consumer notification, a business must notify OAG of the breach.

Background: Currently, a carrier is only required to notify OAG of a security breach and not MIA, the carrier's regulating agency. MIA advises that the bill is intended to better equip the administration to assist consumers and OAG in the event of a security breach.

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Maryland Department of Health; Maryland Insurance Administration; Department of Legislative Services

Fiscal Note History: First Reader - January 28, 2019
mag/ljm Third Reader - March 13, 2019
Revised - Amendment(s) - March 13, 2019

Analysis by: Jennifer B. Chasse

Direct Inquiries to:
(410) 946-5510
(301) 970-5510

ANALYSIS OF ECONOMIC IMPACT ON SMALL BUSINESSES

TITLE OF BILL: Commercial Law - Breach of a Security System – Notification Requirement

BILL NUMBER: SB 30

PREPARED BY: Maryland Insurance Administration

PART A. ECONOMIC IMPACT RATING

This agency estimates that the proposed bill:

WILL HAVE MINIMAL OR NO ECONOMIC IMPACT ON MARYLAND SMALL BUSINESS

OR

WILL HAVE MEANINGFUL ECONOMIC IMPACT ON MARYLAND SMALL BUSINESSES

PART B. ECONOMIC IMPACT ANALYSIS

This proposal serves to require insurance carriers to notify the Maryland Insurance Administration (MIA) in the event that a carrier experiences a breach of a security system.

Currently in the event of a breach of a security system of an insurance carrier, the carrier is only required by law to notify the Office of the Attorney General (OAG) and not its regulating agency, the MIA.

Carriers will have to generate a notice to the Maryland Insurance Administration (MIA) they did not have to before, but the MIA anticipates that cost to be minimal and should mirror the notice already required under the Commercial Law Article § 14-3501.