Department of Legislative Services

Maryland General Assembly
2019 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

Senate Bill 490 (Senator Kagan)
Finance Economic Matters

Consumer Protection - Scanning or Swiping Identification Cards and Driver's Licenses - Prohibition

This bill prohibits a person from (1) using a "scanning device" to scan or swipe an identification card or a driver's license to obtain personal information; (2) retaining any information collected from scanning or swiping an identification card or a driver's license; or (3) selling or transferring any information collected from scanning or swiping an identification card or driver's license except as required by law. The bill also specifies the circumstances in which the scanning or swiping prohibitions do not apply. Violation of the bill is an unfair or deceptive trade practice under the Maryland Consumer Protection Act (MCPA), subject to MCPA's civil and criminal penalty provisions.

Fiscal Summary

State Effect: The bill's imposition of existing penalty provisions does not have a material impact on State finances or operations. The Office of the Attorney General, Consumer Protection Division, can handle the bill's requirements with existing resources.

Local Effect: The bill's imposition of existing penalty provisions does not have a material impact on local government finances or operations.

Small Business Effect: Minimal.

Analysis

Bill Summary: A "scanning device" is a bar code scanner, a magnetic stripe reader, or any other device (or combination of devices) that is capable of deciphering, in an electronically readable format, the information electronically encoded in a bar code or magnetic stripe.

A person *may* scan an identification card or driver's license in certain circumstances, including:

- to verify the authenticity of the identification card or driver's license;
- to verify the age or identity of the individual who possesses the identification card or driver's license;
- to record, retain, or transmit information as required by law;
- to transmit the name and identification card number or driver's license number to a check service company (1) for the purpose of approving negotiable instruments, electronic funds transfers, or other similar methods of payment or (2) to prevent fraud or other criminal activity; or
- to prevent fraud or other criminal activity if the information collected or retained is limited to specified information and (1) the individual returns an item or requests a refund or exchange for an item or (2) the person uses a fraud prevention service company or system.

The bill does not apply to a depository institution that uses a scanning device to scan or swipe an identification card or driver's license in connection with a deposit account, a loan, or another service or product requested by the individual. In addition, if done for a legitimate business purpose, the bill does not prohibit a person from (1) scanning *only* the name and address fields of an identification card or driver's license and retaining the information to fill in fields on specified forms for customer convenience or (2) photocopying the identification card or driver's license and retaining the photographic copy.

Current Law/Background:

Disclosure of Driver's License Information

State law does not specifically restrict or prohibit persons (including businesses) from asking individuals to inspect, scan, and/or store the information contained in driver's licenses. The Motor Vehicle Administration (MVA), however, must adhere to federal and State laws regarding the disclosure of information contained in driver's license records.

The federal Driver Privacy Protection Act (18 USC § 2721) prohibits state departments of motor vehicles from disclosing personal information about any individual without the express consent of that person. Personal information may be disclosed in specified circumstances, however. For example, legitimate businesses may use personal information contained on licenses during the normal course of business to verify the accuracy of personal information.

A "custodian" who possesses public records of MVA is prohibited from disclosing any personal information contained in those records for surveys, marketing, and solicitations, without the written consent of the person in interest. The purpose of the surveys, marketing, or solicitations must be approved by MVA. A custodian is an "official" custodian or any other authorized individual who has physical custody and control of a public record. An official custodian is an officer or employee of the State or a local government who is responsible for keeping a public record, regardless of whether the officer or employee has physical custody or control of the public record.

A custodian of public records of MVA that contain personal information is required to disclose personal information upon request by a legitimate business, as specified, for use in the normal course of business activity, but only to (1) verify the accuracy of the personal information or (2) obtain correction of inaccurate information, but only to prevent fraud, pursue legal remedies, or recover on a debt or security interest.

According to a 2015 New Jersey *Star-Ledger* investigation, driver's license barcodes contain sensitive personal information that can be used for nefarious purposes if the information falls into the wrong hands. In addition, scanning devices that are capable of reading the information on driver's licenses are widely available. At least some of the information contained in the barcodes is the same information found on the front of the card (*e.g.,* name, address, date of birth, etc.), which allows the information to be quickly verified. However, it is unclear what additional information may be contained on driver's license barcodes.

Maryland Personal Information Protection Act

Chapters 531 and 532 of 2007 (the Maryland Personal Information Protection Act, or MPIPA) required businesses to protect an individual's personal information and to provide notice of a security breach relating to an individual's personal information.

When a business is destroying a customer's, employee's, or former employee's records containing personal information, the business must take reasonable steps to protect against unauthorized access to or use of the personal information, taking specified considerations into account.

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 that are (1) appropriate to the nature of the disclosed information and (2) reasonably designed to help protect the information from unauthorized access, use, modification, disclosure, or destruction. This provision applies to a written contract that is entered into on or after January 1, 2009.

Unfair, Abusive, or Deceptive Trade Practices

An unfair, abusive, or deceptive trade practice under MCPA includes, among other acts, any false, falsely disparaging, or misleading oral or written statement, visual description, or other representation of any kind which has the capacity, tendency, or effect of deceiving or misleading consumers. The prohibition against engaging in any unfair, abusive, or deceptive trade practice encompasses the offer for or actual sale, lease, rental, loan, or bailment of any consumer goods, consumer realty, or consumer services; the extension of consumer credit; the collection of consumer debt; or the offer for or actual purchase of consumer goods or consumer realty from a consumer by a merchant whose business includes paying off consumer debt in connection with the purchase of any consumer goods or consumer realty from a consumer.

The Consumer Protection Division is responsible for enforcing MCPA and investigating the complaints of aggrieved consumers. The division may attempt to conciliate the matter, issue a cease and desist order, or file a civil action in court. A merchant who violates MCPA is subject to a fine of up to $10,000 for each violation and up to $25,000 for each repetition of the same violation. In addition to any civil penalties that may be imposed, any person who violates MCPA is guilty of a misdemeanor and, on conviction, is subject to a fine of up to $1,000 and/or imprisonment for up to one year.

Additional Information

Prior Introductions: SB 1047 of 2018, a nearly identical bill, received a hearing in the Senate Finance Committee, but no further action was taken. SB 470 of 2017, a similar bill, received an unfavorable report from the Senate Finance Committee.

Cross File: None.

Information Source(s): Office of the Attorney General (Consumer Protection Division); New Jersey *Star-Ledger*; Department of Legislative Services

Fiscal Note History: First Reader - February 25, 2019
sb/kdm Third Reader - March 25, 2019
Revised - Amendment(s) - March 25, 2019

Analysis by: Eric F. Pierce

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