Department of Legislative Services

Maryland General Assembly
2023 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 861 (Senator Kagan)
Finance

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 (ID) card or a driver's license to obtain certain personal information; (2) storing, recording, or retaining any information collected from scanning or swiping an ID card or a driver's license after the conclusion of each transaction; or (3) selling or transferring any information collected from scanning or swiping an ID 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, abusive, 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 (OAG), 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 or swipe an ID card or driver's license in certain circumstances, including:

- to verify the age of the individual who possesses the ID card or driver's license;
- to verify the authenticity of the ID card or driver's license before (1) selling or otherwise distributing specified products (*e.g.*, alcoholic beverages) or (2) granting admission to certain premises licensed to sell alcoholic beverages or where admission is restricted to individuals who are at least age 21;
- to record, retain, or transmit information as required by law; or
- to transmit the name and ID 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.

The bill does not prohibit a law enforcement officer from using a scanning device to scan or swipe an individual's ID card or driver's license to record, retain, or transmit information if the officer is acting within the scope of official duties.

In addition, the bill does not apply to a depository institution that uses a scanning device to scan or swipe an ID card or driver's license in connection with a deposit account, a loan, or another service or product requested by the individual.

Current Law:

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.

For example, 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.

Maryland Personal Information Protection Act

The Maryland Personal Information Protection Act (MPIPA) imposes certain duties on a business to protect an individual's personal information. A business in possession of personal information must implement and maintain reasonable security procedures and practices to protect the information from unauthorized access, use, modification, or disclosure. If a data breach occurs, the business must conduct, in good faith, a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been (or will be) misused. If the business determines that personal information likely has been (or will be) misused, the owner or licensee of the computerized data must notify an affected individual as soon as practicable, but not later than 45 days after the business discovers or is notified of the breach. For a business that only maintains personal data, the business must notify the owner or licensee of the breach as soon as practicable but not later than 10 days after the business discovers or is notified of the breach. Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security.

When a breach occurs, a business must also provide notice to OAG that includes (1) the number of Maryland residents affected by the breach; (2) a description of the breach, including when and how the breach occurred; (3) any steps the business has taken or plans to take relating to the breach; and (4) the form of notice and a sample of the notice that will be sent to individuals affected by the breach. The Act also establishes a specific notification process for breaches involving email account information.

Violation of MPIPA is an unfair, abusive, or deceptive trade practice under MCPA, subject to MCPA's civil and criminal penalty provisions.

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: Similar legislation has been introduced within the last three years. See SB 712 of 2022 and SB 34 and HB 752 of 2020.

Designated Cross File: None.

Information Source(s): Office of the Attorney General (Consumer Protection Division); Judiciary (Administrative Office of the Courts); Maryland Department of Transportation; Department of Legislative Services

Fiscal Note History: First Reader - March 13, 2023
km/jkb

Analysis by: Eric F. Pierce

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