SB695 id swiping.docx (1).pdf
Uploaded by: Marceline White
Position: FAV

SB695: Consumer Protection - Driver's License and ID Card Swiping - Regulation

Position: Favorable

March 12, 2026

The Honorable Pam Beidle, Chair
Senate Finance Committee
3 East, Miller Senate Office Building
Annapolis, Maryland 21401
cc: Members, Senate Finance

Chair Beidle and Members of the Committee,

Economic Action Maryland Fund urges a favorable report on SB695, which would protect the personal information of Marylanders.

A driver's license contains an individual's core identifying information; name, address, birthdate, height, and weight. The magnetic strip works just like a credit card, and the information is easily swiped and stored, providing an easy avenue for identity theft. Indeed, someone's driver's license information can sell for over $150 on the dark web.[1]

Identity theft is on the rise, with credit card fraud the most common type of identity theft - over 500,000 cases were reported in the first three quarters of 2025.[2] New account fraud, where someone uses your personal information to open a new account, accounted for 90% of those cases. That type of fraud is fueled by access to someone's personal information, which is then used to open those new accounts.

Given the risks associated with swiping and saving personal information from someone's driver's licenses, 17 states have established some regulations on when a driver's license may be scanned and how the information may be retained and used.[3] Both New Jersey and Virginia have passed laws that regulate both. It is important that Maryland also take action to protect Marylanders.

For these reasons, we urge a favorable report on SB695.

Sincerely,
Marceline White, Executive Director

[1] https://www.identityforce.com/blog/drivers-license-fraud-identity-theft
[2] https://www.fool.com/money/research/identity-theft-credit-card-fraud-statistics/
[3] https://www.aclu.org/news/privacy-technology/state-barcode-laws

2209 Maryland Ave · Baltimore, MD 21218 | www.econaction.org
Marceline White · Marceline@EconAction.org | Jennifer Bevan-Dangel · Jennifer@EconAction.org

Sen. Kagan Testimony SB695_ ID Swiping.pdf
Uploaded by: Sen. Cheryl Kagan
Position: FAV

CHERYL C. KAGAN
Legislative District 17
Montgomery County

Vice Chair
Education, Energy, and
the Environment Committee

Joint Audit and Evaluation Committee
Joint Committee on Federal Relations

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

Miller Senate Office Building
11 Bladen Street, Suite 2 West
Annapolis, Maryland 21401
410-841-3134
800-492-7122 *Ext.* 3134
Cheryl.Kagan@senate.maryland.gov

SB695 Testimony: Driver's License and ID Card Swiping - Regulation
Senate Finance Committee
Thursday, March 12, 2026 1:00pm

Increasingly, retailers require ID card scans for routine transactions, allowing them to amass our personal information in large databases that are susceptible to misuse and cyberattacks. When a merchant scans your license, they collect a digital record of your personal information. This practice is intrusive and leaves consumers vulnerable to scams and identity theft when the interaction may only require temporary verification of age or identity.

In Maryland, a REAL ID driver's license, which has been issued in compliance with the federal REAL ID Act since 2011 and is required for TSA identification as of last May, contains personal data including name, home address, date of birth, license number, height, weight, organ-donor status, gender, veteran status, and disability status. While the system is designed to limit exposure of private data, no technology is completely immune from advancements, glitches, errors, misuse, or hacks.

The retail industry is particularly susceptible to these problems due to lack of employee training on data security, high staff turnover, and relatively weak cybersecurity practices-- especially when third-party vendors are involved. Recent retail data breaches over the past three years illustrate the risk to consumers:

- Under Armour (November 2025): 72 million individuals
- Etsy, TikTok Shop, Poshmark (March 2025): 1.6 million users
- Ahold Delhaize USA--Food Lion, Giant Food (November 2024): 2.2 million customers
- Hot Topic (October 2024): 57 million customers
- VF Corp - Timberland, The North Face, Vans (December 2023): 35.5 million individuals
- JD Sports (January 2023): 10 million consumers

Baltimore-based Under Armour leads this list of companies recently affected by cyber theft. As reported by the popular tracking website **haveibeenpwned.com**, "In January 2026, customer data from the incident was published publicly on a popular hacking forum, including email addresses. Many records also contained additional personal information such as names, dates of birth, genders, geographic locations and purchase information."

In its *X-Force 2025 Threat Intelligence Index*, IBM reported: "As retailers rely heavily on digital infrastructure to manage consumer data and facilitate transactions, they remain an attractive target for attackers seeking financial or operational disruption."

One of the best ways to protect sensitive personal information from being misused or stolen is to prevent it from being routinely captured and stored in the first place.

SB695 would prohibit a retail establishment from swiping a driver's license or ID card except for valid commercial purposes to complete a transaction:

- Commercial entities may not swipe driver licenses or ID cards except to:
    - verify authenticity of the ID card,
    - verify age for restricted goods or services,
    - prevent fraud or criminal activities, or
    - process financial transactions.
- If commercial entities do swipe driver's licenses or IDs, they may not store, share, or sell information collected.
- Information collected for verification may not be sold or shared, and fraud- or crime-prevention data must be deleted within 60 days.
- Governmental entities may only swipe with explicit consent, for lawful confiscation, to render emergency assistance, or with a court order.
- Law enforcement will still be able to swipe IDs and may record, retain, or transmit information while acting within the scope of their official duties.
- Individuals may recover actual damages or $1,000, whichever is greater, and courts may triple the award for willful violations, including attorney fees.

This bill updates our laws to address the current risk environment; reduces consumer exposure to identity theft; and aligns our State with national best practices that keep pace with technological change. In total, 17 states place either a restriction on ID scanning, data retention, or both.[1] States as diverse as Oregon, Nevada, Texas, Virginia, and Wyoming have enacted similar protections to ensure that personal information is handled responsibly.

SB695 is a common sense measure that protects consumers without interfering with legitimate business practices. I would like to amend **page 3, line 16**, after "company or," to read **"company or security system"** to ensure the language does not inadvertently limit security protocols at institutions.

I urge a favorable report with a one-word amendment.

[1] California and Georgia regulate when an ID may be scanned. Arizona, Maine, Massachusetts, Nebraska, North Carolina, Ohio, and Tennessee regulate data retention from ID scans. Florida, Hawaii, Illinois, New Hampshire, New Jersey, Oregon, Texas, and Virginia regulate both ID scanning and data retention.

SB 695 - CPD - ID swiping - Support.pdf
Uploaded by: Steve Sakamoto-Wengel
Position: FAV

CAROLYN A. QUATTROCKI
Chief Deputy Attorney General

LEONARD J. HOWIE III
Deputy Attorney General

CARRIE J. WILLIAMS
Deputy Attorney General

SHARON S. MERRIWEATHER
Deputy Attorney General

ZENITA WICKHAM HURLEY
Deputy Attorney General

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

ANTHONY G. BROWN
Attorney General

WILLIAM D. GRUHN
Division Chief

STEVEN M. SAKAMOTO-WENGEL
Executive Counsel to the Attorney General

PETER V. BERNS
General Counsel

CHRISTIAN E. BARRERA
Chief Of Staff

March 12, 2026

TO: The Honorable Pam Beidle, Chair
Finance Committee

FROM: Steven M. Sakamoto-Wengel
Executive Counsel to the Attorney General

RE: Senate Bill 695 – Consumer Protection –Driver's License and ID Card Swiping -- SUPPORT

The Consumer Protection Division of the Office of the Attorney General supports Senate Bill 695, sponsored by Senators Kagan and Gile, which would prohibit a person from using a scanning device or card reader to collect information from an individual's driver's license or identification card, unless the person has a legitimate reason for collecting that information. The bill would also limit the information the person may retain from an individual's license or identification card. Driver's licenses and identification cards contain significant personal information about an individual – information that can be used for identity theft or other nefarious purposes. Especially in light of the large number of data breaches, there is no reason why someone should collect and retain that personal information unless they have a legitimate reason for collecting such information as set forth in the bill.

Here is the experience of one of the Consumer Protection Division's employees:

> A senior apartment community in Baltimore City invited me to conduct a scams presentation for their residents. The security guard asked to see my ID—the operative word here is "see." The guard quickly scanned my driver's license before I could object to it. In an instant, my privacy was gone.
>
> I had no idea what data they were collecting, how they were storing it, who had access to this data about me, how long they would store it or what they were doing with my personal data.

> There was no posted notice alerting visitors about the apartment complex's ID scanning policy. There was no written privacy policy or any information about their data collection policy. No one asked for my consent or even informed me that my license would be scanned beforehand. I successfully challenged the apartment management to have my data removed from their system. While I was lucky, the average person cannot convince these organizations to delete their data, once it has been collected.

The Division believes that Senate Bill 695 is a reasonable measure that helps protect individuals' personal information against misuse and recommends that the Finance Committee issue a favorable report.

cc: The Honorable Cheryl Kagan
The Honorable Dawn Gile
Members, Finance Committee

SB0695 - MBA - FWA - GR26.pdf
Uploaded by: Evan Richards
Position: FWA

SB 695 – Consumer Protection - Driver's License and ID Card Swiping - Regulation
Committee: Senate Finance Committee
Date: March 12, 2026
Position: Favorable with Amendments

The Maryland Bankers Association (MBA) **SUPPORTS** SB 695 **WITH AMENDMENTS**. This legislation prohibits the swiping of a driver's license or ID card and prohibits the storing, selling, or sharing of personal information collected via a swipe under certain circumstances. While the MBA appreciates the exemptions placed into the bill for financial institutions, MBA believes a full exemption for financial institutions would provide clarity, consistency, and operational integrity in bank compliance.

Protecting customers' money is one of the most fundamental responsibilities of any bank. At its core, the financial system is built on trust—customers deposit their savings, paychecks, and investments with the expectation that their funds will be safe, accessible, and handled responsibly. When banks safeguard those funds effectively, they reinforce confidence not only in their institution but in the broader financial system that depends on stable deposits to function.

Banks rely on driver's licenses and identification cards every day to safeguard their customers. These tools are essential for preventing fraud, protecting sensitive financial information, and maintaining safe and compliant operations. SB 695 permits financial institutions to collect information for purposes such as processing deposits or loans, preventing fraud, and effecting, administering, or enforcing transactions. While these broad exemptions are valuable, compliance teams would still be required to verify that each instance of information collection fits within one of the specified categories. **Providing a complete carveout removes this regulatory ambiguity and reduces administrative burden, allowing banks to continue using identification tools efficiently and consistently to protect customers and their financial assets.**

Protecting customers' money isn't just a regulatory requirement—it's the foundation of the relationship between banks and the communities they serve. It enables trust, promotes stability, and ensures that customers can confidently rely on their financial institutions for security and support. A full exemption is essential for banks to efficiently verify customer identities and safeguard their funds without the uncertainty and operational risk created by piecemeal compliance requirements.

Accordingly, MBA urges the issuance of a **FAVORABLE** report **WITH AMENDMENTS** on SB 695.

The Maryland Bankers Association (MBA) represents FDIC-insured community, regional, and national banks, employing thousands of Marylanders and holding $194.8 billion in deposits in over 1,100 branches across our State. The Maryland banking industry serves customers across the State and provides an array of financial services including residential mortgage lending, business banking, estates and trust services, consumer banking, and more.

CHPA Amendment Request MD SB 695.pdf
Uploaded by: John McLuckie
Position: UNF

CHPA® | CONSUMER HEALTHCARE PRODUCTS ASSOCIATION

Taking healthcare personally.

March 10, 2026

The Honorable Senator Pamela Beidle
Chair, Senate Finance Committee
3 East Miller Senate Office Building
Annapolis, Maryland 21401

Re: SB 695 - Consumer Protection – Driver's License and ID Card Swiping – Regulation

Dear Chair Beidle,

On behalf of the Consumer Healthcare Products Association (CHPA), the Washington, D.C. based national trade organization representing the leading manufacturers of over-the-counter (OTC) medicines, dietary supplements, and OTC medical devices, thank you for the opportunity to comment on SB 695. While we support the bill's goal of strengthening consumer control over personal data, we must oppose it in its current form. Specifically, the bill conflicts with federal regulations governing controlled substances data collection. Adding language to ensure compliance with these federal requirements would resolve our concerns.

Federal and State Law

The Controlled Substances Act (CSA), also referred to as the Comprehensive Drug Abuse Prevention and Control Act, was enacted by Congress in 1970 with the aim of regulating the production, distribution, and utilization of controlled substances. As per 21 U.S.C. Section 830 of this Act, individuals or entities involved in transactions concerning listed chemicals (such as pharmacies selling allergy medications containing ephedrine or pseudoephedrine) are obligated to gather and retain identifiable personal records pertaining to these transactions and to share the data with law enforcement as required. Building upon this federal framework, many Maryland retailers utilize the Precursor Log Exchange (NPLEx) system, which provides real-time electronic monitoring of pseudoephedrine (PSE) sales across the state. Unfortunately, this bill does not provide an exemption for such transactions from its privacy provisions.

Amendment Recommendations

To avoid potential conflict with already existing federal law, CHPA recommends the following amendment to SB 695 as subpart VII, after line 24, on page 3:

> (VII) In order to comply with the requirements of the federal policy under the Controlled Substances Act Section on the Regulation of Listed Chemicals under 21 U.S.C. SEC. 830.

Conclusion

CHPA and its members are deeply committed to protecting our customers' privacy and data security. While we appreciate your focus on this important issue, the current version of this bill raises significant concerns. We remain open to constructive dialogue and collaboration to develop a more balanced approach that addresses all stakeholders' needs.

Respectfully submitted,

Carlos I. Gutiérrez
Vice President, State & Local Government Affairs
Consumer Healthcare Products Association
Washington, D.C.
cgutierrez@chpa.org | 202-429-3521