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.