

CHERYL C. KAGAN
Legislative District 17
Montgomery County



Miller Senate Office Building
11 Bladen Street, Suite 2 West
Annapolis, Maryland 21401
301-858-3134 · 410-841-3134
800-492-7122 Ext. 3134
Fax 301-858-3665 · 410-841-3665
Cheryl.Kagan@senate.state.md.us

Vice Chair
Education, Health, and
Environmental Affairs Committee

Joint Audit Committee
Joint Committee on Federal Relations

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

SB712: Consumer Protection – Restrictions on Scanning or Swiping Driver’s Licenses

Senate Finance Committee

Wednesday, March 16, 2022 | 1pm

“A driver’s license is an identity thief’s paradise.” - Credit reporting giant, [Experian](#).

Twelve other states (*both red and blue*) have enacted reasonable consumer privacy legislation with regard to swiping our driver’s licenses: California (2015), Florida (2016), Georgia (2010), Hawaii (2012), Nebraska (2010), New Hampshire (2003), New Jersey (2017), Oregon (2015), Ohio (2015), Rhode Island (2004), Texas (2010), and Virginia (2020).

[SB712](#) would protect our private information, except in limited circumstances (see attached), by prohibiting the swiping of our driver's licenses (or MVA-issued identification cards). This is not a new bill. In 2019, [SB490](#) unanimously passed the Senate ([45-0](#)).

Why is this important? Our driver’s licenses have always included personal information such as birthdate, home address, height, weight, signature, photograph, etc. With the new *Real ID* driver’s license, even more [sensitive data](#) including fingerprints, biometric information, facial recognition templates, medical information, and court-ordered restrictions will be vulnerable.

Too many businesses are swiping our driver’s licenses. Whether the reasoning is justifiable or frivolous, we have no knowledge or control over how they may exploit or sell our personal information. And, we are all too familiar with security breaches.

Cybersecurity experts, such as [Risk Enterprise Management](#), say that collecting and storing driver’s license information puts consumers at significant risk for identity theft. Hacking has become extremely common, and cyberattacks are on the rise. In 2021, there were over [1,291 exposures](#) of personal data, including Android (100+ million people); Facebook (553 million users); and LinkedIn (700 million/93% of users). [IdentityForce found](#) that companies such as T-Mobile, CVS, and GEICO have experienced large-scale cyberattacks in the past year.

The best defense against a data breach is not collecting and storing the information in the first place! I urge a favorable report on SB712.

(Attachment)

SB712: Prohibitions and Allowances for Scanning Driver's Licenses (AS AMENDED)

Driver's Licenses (or MVA-issued ID's) MAY NOT be scanned:

- To obtain personally-identifying information beyond the basic (name, address, DOB, driver's license number);
- Nongovernmental entities:
 - Shall not retain data after an individual is no longer liable to/doing business with a company
 - May be civilly liable for unauthorized use of data
- For sale or transfer of any personal data collected.

Driver's Licenses (or MVA-issued ID's) MAY be scanned:

- As required by law;
- To verify age in limited circumstances:
 - Purchase of pseudoephedrine product or ephedrine product;
 - Purchase of alcohol;
 - Admission to premises restricted to persons 21 or older; and
 - Purchase of nicotine products.
- To transmit ID or driver's license number to a check service company for:
 - Approving/administering electronic fund transfers; or
 - Preventing fraud/criminal activity.
- A law enforcement officer acting on official duties; or
- In connection with deposit accounts, loans, or other financial instruments requested by the consumer.