

**Testimony to the Pennsylvania House of Representatives
Committee on Transportation
October 28, 2025**

Chairman Neilson, Republican Chairman Benninghoff – thank you for the opportunity to testify today in support of House Bill 1970, which would authorize PennDOT to start issuing digital counterparts to the physical driver’s licenses and ID cards that Pennsylvanians have used for years.

My name is Jeremy Grant, and I have been working in a mix of government and industry roles in the digital identity space for more than 25 years. As background, I used to run the digital identity group at the U.S. government’s National Institute of Standards and Technology (NIST), and also led a White House initiative called the National Strategy for Trusted Identities in Cyberspace (NSTIC) that was focused on addressing deficiencies in the tools we use to prove who we are online that were leading to increased cybercrime, identity theft, and fraud. Today I serve as Managing Director in Venable’s Technology and Innovation practice in Washington DC.

I am here today on behalf of the Better Identity Coalition – an organization that was launched in 2018 to partner with policymakers to improve the way Americans establish, protect and verify their identities when they’re online. Our members are a diverse array of companies who are leaders in sectors like financial services, health, technology, fintech, payments, retail, and security.

In 2022, the Better Identity Coalition released a “Blueprint” for State Policymakers detailing ways that state governments can help deliver more secure, inclusive, privacy-preserving digital identity solutions.¹

The need for better digital identity solutions has become imperative in recent years. Today, the variety of services available online is greater than ever before, offering Pennsylvanians the ability engage in all sorts of transactions from a device in the palm of their hand. But conversely, the ability of businesses and governments to offer high-value transactions and services online is being tested more than ever, due in large part to the challenges of proving identity online.

¹ See https://www.betteridentity.org/s/Better_Identity_Coalition-State-Blueprint-Dec2022.pdf

The lack of a widely adopted easy, secure, reliable way for organizations to verify identities or attributes of people they are dealing with online creates friction in commerce, leads to increased fraud and theft, degrades privacy, and hinders the availability of many services online. While the market has responded with an array of products that aim to address the identity challenge for specific use cases, the tools available today are uneven in terms of accuracy and reliability, don't work well for everyone, and are increasingly coming under attack.

Digital driver's licenses – also known as “mobile” driver's licenses or mDLs – featured prominently in our Blueprint. This is by virtue of the fact that driver's licenses and state ID cards are by far the photo ID that is most commonly obtained by people in the US, and are thus the documents that are most commonly used to prove one's identity today in the physical world. We are thrilled to see Pennsylvania considering one of the core ideas in this Blueprint – following in the footsteps of more than a dozen states who have already launched mDLs.

mDLs are based around a relatively simple premise: most Pennsylvanians already went through a somewhat painful process at Driver and Vehicle Services to prove who they were to get a plastic driver's license or state ID card that they can use to prove who they are in the physical world. But when they need to prove who they are online, that card does not work. mDLs will allow Pennsylvania to help close the “identity gap” between the nationally recognized, authoritative credentials that work in the physical world – like driver's licenses, passports, and birth certificates – and the lack of any digital counterpart to those physical credentials that Pennsylvanians can use to protect and assert their identities online.

The initial focus of this bill

I will note that most of our praise for the idea of mDLs is around the online use cases, whereas this bill is initially focused on creating an mDL that would let consumers choose to store a digital version of their driver's license or state ID card in their smartphone just for in-person use cases. We think this is a fine place to start – and we encourage Pennsylvania to proceed down this path – but we think the real benefits will come not from the in-person use cases, but the ones that are emerging to support proving your identity in the online world.

Opening a bank account, applying for credit, engaging with your doctor, applying for government benefits – these are the use cases where organized criminals and hostile nation states look to exploit the identity gap, by leveraging stolen identity data and other tools like “deepfakes” powered by generative artificial intelligence (AI) that can increasingly defeat many of the legacy tools that government and industry rely on to try to determine if someone is who they claim to be online. mDLs – which rely on digitally signed, cryptographically protected data from the best authoritative source of identity in the state – are an ideal tool to get ahead of

these attackers, and better protect the identities of all Pennsylvanians when they need to prove who they are online.

For this reason, we would urge Pennsylvania to look beyond the ISO/IEC 18013-5 standard that is called out in the bill – which is focused on supporting in-person use cases of mDLs – and also include reference to the ISO/IEC 18013-7 standard, which supports the online use cases.

The Treasury Department’s Financial Crimes Enforcement Network (FinCEN) has noted that \$212 billion worth of suspicious financial transactions in 2021 was tied to some form of compromise of identity, and they have stated that in 2023, that number nearly doubled to \$394 billion.²

Beyond financial services, governments have been dealing with massive fraud in government benefits programs tied to compromises of identity; the Government Accountability Office (GAO) has reported that fraud losses tied to unemployment insurance (UI) benefits during the COVID pandemic totaled \$100-135 billion³.

Focusing on the online use cases would enable the state to better protect the identities of Pennsylvanians online – and the integrity of state benefit programs – at a time when identity theft and identity-related cybercrime have been soaring.

Privacy concerns

We are also glad to see that this bill includes a section to ensure that mDLs will preserve privacy – and in some cases enhance it – through both technical architecture, as well as new policies to govern the use of mDLs.

In state after state, we see that privacy is the biggest concern that people raise when it comes to mDLs, and bluntly, that is for a good reason: there are a lot of ways a digital driver’s licenses could harm privacy if they were not designed properly. For example, would a digital ID “phone home” to the state every time it is used, so that the state could track what people do with their ID? Could Pennsylvanians be forced to share their unlocked smart phone with law enforcement to prove their identity? Can Pennsylvanians choose to share only a subset of the information on their driver’s license with a bank or a hospital, rather than share every piece of data on it (as they often do today with their physical IDs).

² See https://www.fincen.gov/system/files/shared/FTA_Identity_Final508.pdf

³ See <https://www.gao.gov/products/gao-23-106696>

Here there is good news: the digital driver's licenses that this bill would authorize would have to adhere to set of policies and technical standards that would preserve and enhance the privacy of Pennsylvanians, rather than put it at risk. For example:

- Any architecture that would see mDLs "phone home" to the state in a way that would enable tracking is prohibited.
- The bill also includes important protections to ensure that law enforcement is prohibited from accessing the contents of someone's smart phone just because they are using that phone to present their ID, and ensuring that if law enforcement inadvertently sees other information, that information cannot be used as evidence against the holder of the ID.

Also, it is worth considering that in the physical world, someone showing their ID to another party exposes some information that in many cases should not be shared, such as height and weight. mDLs, in contrast, are great for privacy, in that they allow someone to choose what specific data about themselves to share (i.e., "Over 21") while hiding data that is irrelevant to the transaction.

We note that beyond these initial, critical protections, the National Institute of Standards and Technology (NIST) has launched a project to create a set of standards and best practices – working in partnership with both state DMVs and the private sector – to ensure that mDLs set a high bar for privacy and security wherever they are used.⁴ We would encourage Pennsylvania to participate in this project alongside other states including Maryland, Ohio, California, Georgia and New York, and/or seek to incorporate its outputs into the state's own mDL initiative.

Thank you again for taking the time to consider our views, and we look forward to answering your questions.

⁴ More information on the NIST project is at <https://www.nccoe.nist.gov/projects/digital-identities-mdl>