DHS mDL RFI Response by NACS

This joint response to the Department of Homeland Security's (DHS)Request for Information (RFI) regarding Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Mobile Driver's Licenses (86 FR 20320) is made by the National Association of Convenience Stores (NACS), representing more than 152,000 petroleum/convenience retailers in the United States, and Conexxus, Inc., the technology standards body for the petroleum/convenience industry (Respondents). Each responding individual is doing so on behalf of each organization in their capacity as an "Interested Person".

The position of Respondents, is summarized below:

- We applaud DHS's migration to digital identification document technologies in order to increase convenience and reduce physical identification document fraud.
- We are concerned that the mDL standard (ISO18013-Part 5), if adopted as written, will have negative privacy, total cost of ownership, transparency, and tracking impacts for our industry and its customers.
- We are concerned about the deployment costs to the retail industry, which would be required to shoulder a large part of the costs of the mDL standard due to it's design around a narrow use case, thereby creating acceptance friction; thereby creating a significant barrier to adoption of mDLs by the public.
- As an alternative, Respondents have successfully deployed similar technology using the W3C Verifiable Credentials standards in the nationwide age and product verification program (TruAge™) available to 152,000+ retail locations across the United States. Unlike mDL, this program focuses on standards-based strong customer privacy, extremely low deployment costs to retailers, active anti-tracking features, elimination of PII in transactions through tokenization, as well as online/offline and Web-based usage.
- We recommend enabling alternative technologies, such as W3C Verifiable Credentials, to be used for the all of the same purposes of mobile driver's licenses and other identity documentation to enable a competitive vendor ecosystem, demonstrable interoperability, defining standardized credential issuance and verification protocols, broader deployment across a variety of identity documentation use cases, reduced deployment costs for industry and customers, and a more open and inclusive standardization process than what the ISO mDL standard provides.

Background on the TruAge program and relevance to mDL

NACS is an international trade association representing the convenience industry with more than 1,500 retail and another 1,500 supplier companies (including manufacturers and vendors of age-restricted products) as members, the majority of whom are based in the United States. The industry employed about 2.34 million workers and generated more than $548.2 billion in total sales in 2020, representing nearly 3 percent of U.S. gross domestic product. The industry processes more than 160 million retail sales transactions every single day; a large percentage of those require the use of a driver's license to perform age verification. That means about half of the U.S. population visits our retail members on a daily basis. In fact, ninety-three percent of Americans live within 10 minutes of one of our locations. The average time a customer spends in one of our stores is about three and one-half minutes and the industry is focused on ensuring that every customer's needs are met as efficiently as possible – saving them time and money.

NACS has led efforts to restrict youth access to age-restricted products for the past half century:

- 1971: NACS introduced the c-store industry's first age-verification training video;
- 1985: NACS kicked off the national launch of "I.D. Please: It's the Law" program to prevent sales of alcohol to minors;
- 1990: NACS was a founding member of the We Card program, providing employee training and educational programs that prevent age-restricted product sales to minors and promote responsible retailing, consistently driving down youth availability in retail. We Card is supporting NACS in its effort to bring TruAge™ to market;
- 2010: NACS supported enactment of the Prevent All Cigarette Trafficking (PACT) Act, which regulates the online sale and delivery of tobacco products and closed loopholes for minors to acquire tobacco products;
- 2020: NACS supported enactment of the Preventing Online Sales of E-Cigarettes to Children Act, which requires online e-cigarettes sellers to ensure delivery carriers verify the age of recipients upon delivery.

The use of a driver's license has always been a critical part of our initiatives; we have a great interest in the future of mobile driver's license technologies and how it impacts our member's (both retailers and product manufacturers/vendors) operations.

The volume of transactions that the convenience store industry quickly processes is impressive; at the same time stores also need to ensure that all sales are conducted legally and responsibly. About 50 percent of all transactions inside convenience stores (excluding fuel transactions) include an age-restricted product like alcohol, tobacco, vaping products, lottery tickets, and others. Convenience stores are leaders in age verification: Convenience stores sell approximately 32 percent of all age-restricted items in the United States. With that in mind, the industry has made it a priority to continually improve its ability to verify the age of purchasers – and to do so while respecting and protecting their privacy.

The latest result of those industry efforts is TruAge™, a groundbreaking digital identification solution that enhances current age-verification systems at retail points of sale and protects user privacy.

NACS worked with its standards-setting partner, Conexxus, and Digital Bazaar, a recognized leader in open standard digital identity, to develop TruAge™. The system uses a customer's Driver's License to onboard the individual onto the system and then, once onboarded, uses pseudonymous age verification tokens to confirm their age. When confirming age and identity, one-time-use tokens are downloaded to the customer's mobile device to confirm legal age to purchase age-restricted products. With payments and commerce going digital, TruAge™ uses similar digital technology to verify the age of purchasers of age-restricted products; leveraging the numerous face-to-face authentications made at retail..

A standard driver's license contains over 33 separate pieces of information that can be accessed in current age verification practices. Importantly, TruAge™ only uses 4 of them: the document identification number, issuing authority, date of birth, and whether the ID is current or expired – none of this information can be used to identify the consumer without some bad actor obtaining access to the appropriate DMV database. That makes TruAge™ effective while minimizing privacy and data security risks.

This solution allows for reliable verification of age while maximizing the protection of privacy and minimizing any risk of data theft – a key societal challenge in the digital economy we live in today. The system works for all types of purchases from in-person transactions to those conducted on the Internet and via mobile apps. In addition, TruAge™ is an open-standard age-verification solution. It is free to retailers, consumers, and point-of-sale providers with no hardware upgrades required at the point of sale (unlike the requirement in ISO 18013-5 for specific function, stand-alone mDL Readers), which represents a tremendous impediment to adoption when every retailer already has huge investment in existing POS systems, most of which for convenience store retailers are integrated POS. TruAge™ is also designed to work in offline situations through digital signatures and contemplates communications disruptions that could, with less capable systems, inhibit consumer satisfaction and adoption.

In our view, widespread consumer and business adoption is important to the value and reliability of this solution. Therefore, all relevant intellectual property will be placed in the public domain in order to remove barriers to adoption.

This is the model of what reliable verification systems that respect privacy can look like. By describing it below, we hope that this information provides the DHS with useful background that will help foster public policy supporting this type of solution to every stakeholder's benefit.

How TruAge™ Works

There are a couple of different ways that age can be verified by the TruAge™ system. For example, when a customer is purchasing an age-restricted product(s), the checkout process is similar to the traditional carding approach, but faster, safer, and more reliable. What happens is:

1. After the cashier scans an age-restricted item, the point-of-sale system prompts for verification of age – the system will not let the cashier proceed without a verification.
2. The cashier then scans the barcode on the back of the customer's driver's license and does a visual check to ensure that the person making the purchase matches the ID photograph.
3. Finally, the system confirms that the customer is old enough to make the purchase, sending a

randomly generated, single-use token that serves as validation of a verified age. The token also serves as a reference for forensically determining "who" purchased the item. This is a safeguard built into the program in the rare case that law enforcement needs to determine who made the purchase, and as a deterrent to social sourcing to youth; the biggest contributor to underage use.

Alternatively, a store may have an app that integrates with TruAge™ or the store may use the TruAge™ app. In these cases what happens is:

1. After the cashier scans an age-restricted item, the point-of-sale system prompts for verification.
2. The customer opens the app on his/her smartphone to unlock a single-use QR code for the cashier to scan.
3. Finally, the system confirms that the customer is old enough to make the purchase, sending a randomly generated, single-use token that serves as validation of a verified age.
4. This feature is also available for the consumer to use online, with TruAge™ - compliant websites; this e-commerce version provides consumers and retailers with a fast and cost-effective means to verify age for all mobile and online transactions.

In both cases, the purchase data is also verified against a central "open to buy" database, enabling systemic limitations on purchase quantities that reduces the ability of "social sellers" to purchase products legally, for after sale distribution illegally.

TruAge™ incorporates emerging industry standards on identity championed by the World Wide Web Consortium (W3C), the Department of Homeland Security SVIP program, and other standards-setting bodies, to assure privacy while increasing reliability of age verification. Most importantly, it preserves the relationship between the consumer and identity issuer without the risk of a private third party having to be involved, therefore returning identity control to the consumer.

The system uses ID-validation and age-calculation procedures that are not available with a standard ID card. The digital version of TruAge™ provides single-use digital tokens that eliminate all personal information needed to verify age in any transaction—a capability that satisfies emerging privacy regulations and reduces the risk of identity theft.

Protecting Privacy

TruAge™ has been designed with privacy in mind. The only personal information used during a transaction is a digitally signed "token" (a randomly generated code) of a customer's age. Because it is a token, it is useless to anyone seeking to breach the system for user information.

In addition, the customer's driver's license number, issuing authority number, birthdate, and document expiration date are multi-party encrypted and stored in a vault. This safeguard is built into the system to restrict the system to verifying a purchaser's age, not who they are.

This vault is entirely separate from the database used to facilitate transactions at the retail point-of-sale. In other words, someone trying to hack a consumer's identity would literally have to hack into three different databases (two that are operated by NACS under its program, as well as the relevant DMV's database.

Importantly, the system is built to identify age, not identity. Law enforcement will be able to obtain the information in the vault following an appropriate legal process -- that would be the only access to a consumer's personal information because it would not be connected to the transactions at the time of the sale. This process is only available under subpoena and requires the cooperation of the government issuer.

The system also provides the ability to keep information on the number of purchases in order to comply with federal, state, or local laws that set maximum purchases of a product over a period of time. But, this too is done with an anonymous token and age. Personally identifiable information is not tracked across purchases when these limitations are put in place. When using TruAge™, all personally identifiable information is eliminated from the transaction.

As stated above, data breaches involve hacking into one database that contains personally identifiable information. Under this system, two separate databases would need to be compromised, plus randomly-generated tokens would need to be decrypted, plus a government database would need to be breached to compromise a person's identity.

This program has been designed to comply with the most stringent existing and emerging consumer privacy regulations such as the General Data Protection Regulation (GDPR), which regulates data protection and privacy in the EU, and the California Consumer Privacy Act, the Virginia Consumer Data Protection Act, and the Colorado Privacy Act. As described earlier, TruAge™ is purposefully designed to limit any consumer's personal information and only use it in a fully protected process that prevents theft of identity. The way this system is designed can be a model for other use cases requiring different types of identity verification.

Status of the Program

TruAge™ is already being used and is demonstrating its success. It has been used in several stores in West Virginia, Pennsylvania, and Colorado as initial tests. It has also proven its interoperability with the emerging digital Permanent Resident Card being developed by DHS/UCIS under the DHS/SVIP program. There will be future pilots conducted at stores in Texas in the third quarter of this year with a wider launch of the program in the fourth quarter. The goal is for TruAge™ to be universally accepted at all physical stores and by online retailers nationwide where age-restricted products are sold. That will make the program more effective and more convenient for consumers.

Most importantly, after analyzing the mDL standard and speaking with mDL vendors, it has become clear to us that deployment of mDL readers into the retail sector is an unsupported and unnecessary cost at present. Upgrading deployed infrastructure is an expensive proposition for a single use case (reading driver's licenses). The petroleum/convenience industry processes far more than just driver's licenses; we process military identification cards, tribal identification cards, and passports from every country in the world. Given that mDL cannot meet these use cases, and W3C Verifiable Credentials are designed for broader use cases, the choice to our industry is clear. We may process mDLs in the future if the infrastructure deployment costs drop to acceptable levels, but if we do, it would only be to onboard into the tokenized age verification system. That is, we would scan the mDL once, obtain verification from the issuing jurisdiction, and then rely on tokenized age expressed in W3C Verifiable Credentials after that point.

Now that we have provided background on the TruAge™ program and how we have contemplated the usage of mDL in that scenario, we will answer the specific questions asked by DHS in the RFI.

1. Security Generally. Provide comments on what security risks, including data interception, alteration, and reproduction, may arise from the use of mDLs by Federal agencies for official purposes, which includes accessing Federal facilities, boarding federally-regulated commercial aircraft, and entering nuclear power plants.

a. Explain what digital security functions or features are available to detect, deter, and mitigate the security risks from mDL transactions, including the advantages and disadvantages of each security feature.

In general, we believe the mDL provides adequate security features for all contemplated uses, although it remains to be seen how the mDL would interface with the DOD's/GSA's Common Access Card for building/system access. The challenge will be with the broader adoption of the technology due to the cost of issuance, deployment of mDL Reader infrastructure, "phone-home" nature of the technology, and the other concerns that the ACLU raised in its Identity Crisis paper [https://www.aclu.org/sites/default/files/field_document/20210517-digitallicense.pdf].

While NACS is not completely aligned with the ACLU paper, the recommendations related to access to phones, unlinkable presentations, granular control, standardized provisioning processes, avoidance of "phone home", and restrictions on ID demands are expected to resonate with the DHS Privacy Office.

b. Provide comments on how mDL transactions could introduce new cybersecurity threat vectors into the IT systems of Federal agencies by, for example, transmitting malicious code along with the mDL Data.

We are not aware of any such threats at this time.

c. Sections 37.15 and 37.17 of 6 CFR part 37 set forth specific requirements for physical security features for DL/ID and other requirements for the surface of DL/ID. Provide

comments on what requirements are necessary to provide comparable security assurances for mDLs.

The only hard requirement to combat fraud is a cryptographic digital signature over the attributes of the mDL being shared and a trusted list of mDL issuers. There are other soft requirements, such as ensuring the person presenting the credential is the one that the credential was issued to, especially in online scenarios.

2. Privacy Generally. Provide comments on what privacy concerns or benefits may arise from mDL transactions, and how DHS should or should not address those concerns and benefits in the REAL ID context. Explain what digital security functions or features are available to protect the privacy of any personally identifiable information submitted in mDL transactions, including the advantages and disadvantages of each security feature.

The ACLU raised a number of concerns that we agree with in their Identity Crisis paper [https://www.aclu.org/sites/default/files/field_document/20210517-digitallicense.pdf]. The digital security functions and features available to mDL tend to be unique to the format and not generalized. This highlights the one-off nature of the mDL solution and the challenge the technology will face when the processing of other identity document formats becomes a requirement, like it is already for the retail industry. Our desire is to have a stable and flexible digital credentialing format, such as the W3C Verifiable Credentials global standard, that is capable of expressing identity document formats beyond a driver's license. Having such a format as well as open protocols for processing that format will reduce deployment and operational costs for our industry. In addition, the W3C Verifiable Credentials data format enables a variety of privacy-preserving technologies, such as BBS+ Signatures that enable selective disclosure, which can be used to protect the customer's privacy in a way that is not supported by the mDL standard.

3. Industry Standards. Executive Order 12866 directs Federal agencies to use performance-based standards whenever feasible. DHS is considering including technical standards for mDL transactions in its proposed rule, drawing heavily on standards under development by the industry, to support compatibility and technical interoperability across all interested Federal agencies nationwide. If commenters believe an industry standard should be chosen, provide comments on how DHS should choose the correct standard(s) for mDLs, and on the appropriate baseline standard(s) that DHS should impose.

This is an important question and cuts to the heart of the issue. Not all open standards undergo a continuous public review process. For example, the ISO process tends to favor large vendors and does not allow the general public to provide commentary throughout the standardization process (unless an organization pays to join the standards development body). As a result, the standards tend to favor the needs of large vendors. Indeed, Conexxus has joined INCITS (the developer of the mDL) and has reviewed and commented by both ISO 18013-5 and ISO 23220, which is intended to be a complimentary standard for identification documents other than mDLs;

Conexxus sponsored a W3C Verifiable Credential use cases for ISO 23220, which we believe has been included in Part 2 of that standard; but increasingly, the INCITS technical committee has been attempting to make ISO 23220 integrate completely with ISO 18013, so we have serious concerns about the eventual utility of ISO 23220 (even with a W3C use case), on top of our direct concerns about ISO 18013-5.

To contrast the operating model, the World Wide Web Consortium and the Internet Engineering Task Force perform almost all of their work in full view of the public (at no cost to participate). The public can engage at any point in the standardization process, which results in a broader review and feedback process. While this should not be a rigid requirement, it should be a consideration as it tends to lead to more thoroughly vetted and generalized technologies. Generalized technologies tend to have lower deployment and operational costs because they are used by a larger number of vendors across a variety of industries.

Additionally, demonstrable end-to-end interoperability is often overlooked when discussing open standards. Open standards typically provide some level of optionality. When this optionality is used inconsistently, it can result in reduced to no practical interoperability. It is important that public test suites demonstrating true end-to-end interoperability are provided such that a competitive marketplace of vendors can emerge rather than a small handful of large vendors that tend to use closed standards processes to protect their established business lines. This is what Respondents have done in the TruAge™ application of the W3C Verifiable Credentials open standard.

NACS recommends that the DHS consider the W3C Verifiable Credential global standards for use in mobile driver's licenses for these reasons.

4. Industry Standard ISO/IEC 18013-5: Communication Interfaces Between mDL Device and Federal Agency, and Federal Agency and DMV. DHS may adopt certain requirements that may be established in forthcoming international industry standards that specify digital security mechanisms and protocols with respect to the communication interface between a mobile device and a Federal agency, and the communication interface between a Federal agency and a DMV.

a. Provide comments on what concerns commenters have regarding such standards and DHS's adoption of their requirements. In particular, explain whether commenters believe the current drafts of industry standard ISO/IEC 18013-5 are mature enough to support secure and widespread deployment of mDLs.

The security of ISO/IEC 18013-5 is not in question; it is adequate. The widespread deployment costs of mDL is what is of great concern. As an industry, we have participated in the standardization of ISO/IEC 18013-5 and have been dismayed at the rush a number of vendors placed on the process. It is clear that existing and dominant vendor business models had a strong part to play in the design and standardization process of mDL. This has resulted in an mDL standard that will be of unacceptable cost to the retail industry to deploy at scale.

Alternatively, the W3C Verifiable Credentials standard provides a more reasonable path for adoption of not just driver's licenses, but other forms of identification documents. We recommend that the DHS does not rush to adopt ISO/IEC 18013-5, but rather promotes at least two competing open standards with demonstrable interoperability and sees how each is being adopted in the marketplace before rushing to implement any particular solution. The DHS/SVIP program is doing this important work and our suggestion is to support them in that process.

b. Explain the impact on stakeholders and mDL issuance if such standards are not approved in a timely manner.

NACS and its member organizations will be impacted negatively by the adoption of a standard by the US Federal Government that we cannot support financially. If the choice is between mDL and no digital identification document standard at present, we are forced to choose the latter because it is the only financially viable option for our industry.

We recommend that DHS wait to see how the W3C Verifiable Credentials standard can be used to issue privacy respecting mobile driver's licenses and perform an evaluation with at least two open standards in the marketplace. Rushing to adopt the ISO 18013-5 technology too early in the process will not have a positive outcome for our industry.

c. Quantify the initial and ongoing costs to a stakeholder to implement these standards.

The initial costs to the petroleum/convenience industry are in the form of hardware to support mDL Readers. Given that we have 152,000+ retail locations, and assuming an average cost of $250 for each mDL Reader with two checkout registers per store and an installation fee of $500 per reader, the initial costs for hardware upgrades would be over $228M USD, plus the cost of point of sale software development and integration. Moreover, our discussions with AAMVA and mDL vendors have led to the conclusion that the industry can expect to pay a fee of $0.35 per individual across 3-6 stores per year, assuming infrequent yearly checks for validity. Our industry encounters roughly 110M individuals per year that purchase age restricted products, which could result in age-related transaction processing fee increases upwards of $115M - $231M USD/year, which will be passed on to the consumer in higher cost products.

These upgrade costs and transaction fees are unacceptably high to the retail industry and is why we have taken the approach that we have with the TruAge™ solution, which replaces the industry upgrade cost with a free point-of-sale software upgrade (no new hardware needed) and reduces the costs to thousandths of a penny ($0.00001) at scale; these costs are covered by manufacturers of age-restricted products.

d. Provide comments on what, if any, key areas related to mDLs are not covered in these standards that DHS should consider addressing by regulation.Start Printed Page 20326

The following key areas related to mDLs are not covered:

- What is the standard protocol that prevents vendor lock-in at the DMV for issuing a mDL?
- What is the standard protocol that prevents vendor lock-in at the DMV and DHS/TSA for verifying a mDL?
- What is the standard communication protocol for presenting an mDL to any website and receiving an mDL from the DMV website?
- What is the GENERALIZED standard cryptographic protocol for performing selective disclosure? Has it been vetted by a standardization organization that specializes in cryptography such as the Internet Research Task Force Cryptographic Forum Research Group?
- What is the GENERALIZED standard communication protocol for displaying a mDL (e.g., as a QR Code)?

e. Identity what, if any, alternative standards or requirements DHS should consider.

DHS should consider the W3C Verifiable Credentials standard for the issuance, holding, and verification of mobile driver's licenses. The DHS/SVIP program along with DHS/USCIS and DHS/CBP has experience with W3C Verifiable Credentials and the protocols for issuing, presenting, and verifying, and we urge DHS to have a discussion with those organizational components.

5. Industry Standard ISO/IEC 23220-3: Communication Interface Between DMV and mDL Device. DHS understands that forthcoming international industry standard ISO/IEC 23220-3 may specify digital security mechanisms and protocols with respect to the communication interface between a DMV and a mobile device, specifically concerning provisioning methods, data storage, and related actions. Although DHS may seek to adopt certain requirements anticipated to appear in this standard, the Department understands that this standard may not be finalized for several years.

a. Explain whether commenters believe the current drafts of standard ISO/IEC 23220-3 are mature enough to support secure and widespread deployment of mDLs.

No, the current drafts are not ready for widespread deployment especially given that many of the communication interfaces being considered are not deployable in a cost effective manner into the retail sector. Many of our member's retail stores do not support the type of wireless readers that mDL requires due to the costs associated with upgrading our infrastructure (Apple Pay and Google Pay is not broadly supported for the same reasons).

b. With the ongoing development of ISO/IEC 23220-3, provide comments on what, if any, alternative standards or requirements DHS should consider before the standard is finalized.

DHS should compare and contrast the work happening in ISO/IEC 23220-3 with the work being performed in full view of the public at the W3C on Verifiable Credentials issuance, storage, and verification protocols. Namely, the work being performed by the W3C Credentials Community Group and the W3C Verifiable Credentials Working Group.

6. Provisioning. DHS understands that provisioning may be conducted in-person, remotely, or via other methods.

a. Explain the security and privacy risks, from the perspective of any stakeholder, presented by in-person, remote, or other provisioning methods.

Remote provisioning methods are concerning if they are not verified by an in-person component at some point in the process. The TruAge™ solution allows for remote provisioning of age tokens which remain unactivated until the individual is verified in person by matching them to their physical driver's license.

b. Provide comments on the security protocols that would be required for DMVs to mitigate security and privacy risks presented by in-person, remote, or other provisioning methods, and to ensure at a high level of certainty that a REAL ID compliant mDL is securely provisioned to the rightful owner of the identity and the target mDL device, for in-person or remote applications.

For the purposes of REAL ID, protocols would need to utilize some form of digital signature that is bound to the individual that is being issued a mobile driver's license in addition to the digital signature from the issuing authority. The W3C Verifiable Credentials standard provides a mechanism called a Verifiable Presentation that enables the holder of a mobile driver's license to establish that they authorized the release of the document to a requesting party.

c. Provide comments on whether mDL Data should include data fields populated with information concerning the method of provisioning used.

We would be concerned if mDL Data included the provisioning method used as that seems to imply that some mDLs are more trustworthy than others. Having multiple levels of assurance on a mobile driver's license would make supporting such a system even more costly than our current projections due to added in-person vetting complexity at the point of sale.

d. Provide estimated costs for a DMV to implement in-person or remote provisioning. Costs may include IT contracts, hiring full or part-time IT staff, as well as software and hardware.

We have no opinion on this matter at this point in time.

7. Storage. DHS understands that mobile device hardware- and software-based security architectures can be used to secure mDL Data on a mobile device.

a. Provide comments on the advantages and disadvantages, with respect to security, functionality, and interoperability, of the different mobile security architectures for protecting, storing and assuring integrity of mDL Data.

So long as a mobile driver's license contains a digital signature from the issuer, then protection of the data itself from tampering is not a concern. If the presentation of a mobile driver's license requires a digital signature from the holder, and we strongly support such a requirement, then the protection of the cryptographic material used to generate the signature by the holder of the mobile driver's license when presenting it to a verifier is an important consideration. Using a mobile device's secure enclave, or cloud-based HSM devices to protect key material should be a requirement for use cases that require strong authentication, such as when boarding an airplane or entering a government facility.

b. Explain whether a hardware- or software-based solution, or both, would provide the requisite security in a competitively-neutral manner.

Due to the nature of the HSM industry, hardware-based solutions tend to increase deployment costs and create market competition problems. That said, some use cases require hardware-based solutions. The retail industry that performs age verification does not require hardware-based solutions and deployment cost is a significant factor for us. For that reason, our industry does not require a hardware-based solution if such a solution places the final solution out of reach from a deployment and operational cost perspective.

8. Data Freshness. Provide comments regarding whether and to what extent security risks concerning data validity and freshness can be mitigated by defining the frequency by which mDL Data should synchronize with its DMV database.

At present, the "phone home" nature of the mDL standard is deeply concerning, as outlined in the ACLU's Identity Crisis paper [https://www.aclu.org/sites/default/files/field_document/20210517-digitallicense.pdf]. Any sort of communication between the requesting party and/or verifier and the issuer of the mobile driver's license creates a privacy and tracking risk that deeply concerns our industry.

a. Provide comments regarding what data synchronization periods commenters believe are appropriate for mDL transactions. Explain the advantages and disadvantages of a longer or shorter periods.

It is not clear what is meant by "data synchronization period". Once a mobile driver's license is issued, it is expected that it is valid for the validity period. One drawback of the mDL standard is the lack of a clear synchronization or "credential refresh" feature. The W3C Verifiable Credentials standard provides such consent-based feature, called "credentialRefresh", that could be used to provide refreshing instructions should a mobile driver's license be suspended or revoked. Note also that the W3C Verifiable Credentials standard has mechanisms for expressing the current status of a credential, such as a mobile driver's license, in a privacy-preserving manner.

b. Provide estimated costs to a stakeholder to implement the data synchronization periods stated above.

We do not have any comments on this item at this time.

9. IT Security Infrastructure. Provide comments on whether IT security infrastructure, such as Public Key Infrastructure, would provide the level of privacy and security sufficient to implement a secure and trusted operating environment, for both offline and online use cases, and if not, explain what alternative approaches would be better.

a. Identify any what additional or alternative IT security infrastructure (e.g., a public key distributor or aggregator such as a trusted public certificate list, Federal PKI) that would be required to facilitate trusted mDL transactions between mDL holders, verifying entities, and issuing authorities.

A list of authorized issuers published by a trusted entity, such as AAMVA or the US Federal Government, would be adequate in addressing the need to trust the issuers in a mobile driver's license ecosystem.

A list of authorized vendor applications would be concerning if there was not an open accreditation process that involves demonstrable interoperability that invites broad participation by vendors not traditionally in the mobile driver's license ecosystem; the lack of such a process would indicate that the market may be headed towards vendor lock-in.

A list of authorized presenters, in this case, citizens and residents, would be an intractable problem and rather than having such a thing, mechanisms such as the W3C Decentralized Identifier work might be considered as a way of having nation-scale dependence on one or more distributed global PKI infrastructures that ensures the appropriate level of security, while not placing any single vendor in the position of maintaining that list on behalf of state or federal governments (which would lead to vendor lock-in).

b. Provide estimated costs for a DMV or Federal agency to implement necessary IT security infrastructure. Costs may include IT contracts, hiring full or part-time IT staff, as well as software and hardware.

We have no insight into DMV and Federal agency operating costs and are unable to provide an opinion on this at present.

10. Alternative IT Security Solutions. Provide comments on whether DHS should consider privacy or security solutions adopted in other industries, such as finance (e.g., mobile payments), automotive/telecommunications (e.g., vehicle-to-vehicle or

"V2V"/"V2X" communications), or medical (e.g., electronic prescriptions for controlled substances), that rely on digital identity and/or secure device-to-device transactions. Explain what those solutions are and how they could be adapted or implemented for Federal mDL use cases.

The supply chain, education, banking, and insurance industries are actively pursuing W3C Verifiable Credential solutions. We suggest that DHS explore that avenue before deploying any nation-wide solution.

11. Offline and Online Data Transfer Modes. DHS understands that mDL Data may be transferred to a Federal agency via offline and online modes.

a. Explain the security and privacy risks, from the perspective of any stakeholder, presented by both offline and online data transfer modes.

The TruAge™ program is designed to work with no network connection as some of our member retail stores are located in remote regions without stable access to the Internet. Our offline mode utilizes W3C Verifiable Credentials encoded as compact QR Codes, which are digitally signed, readable using industry standard legacy point-of-sale 2D-code scanning hardware, and verifiable in offline scenarios. These single use age tokens are designed to actively combat tracking and are a privacy-first approach to ensuring that we comply with existing state and federal regulations not only when it comes to age-restricted products but also when it comes to the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Virginia Consumer Data Protection Act (VCDPA), Canada's Consumer Privacy Protection Act (CPPA), and other emerging regulation related to customer privacy.

Our understanding of the mDL standard is that many of these protections are not in place for mDL transactions, and while it is possible to perform some level of data minimization, the broad usage of mDL at retail concerns our industry as it could easily be abused to perform pervasive tracking of retail customers without their consent.

b. Provide comments on the security protocols that would be required to mitigate security and privacy risks presented by both offline and online data transfer modes.

Security protocols that are missing from mDL include generalized selective disclosure protocols, the generation of pseudonymous one-time use tokens that actively combat tracking, protocols that do not require a "phone home" for the proper operation of the system, and a more general design that will be used by a broader industry outside of the driver's license vertical (i.e., non-mDL documents) to ensure proper public vetting of security and privacy concerns related to the technology.

12. Unattended Online mDL Verification. Provide comments on what capabilities or technologies are available to enable unattended online mDL verification by Federal agencies. Explain the possible advantages and disadvantages of each approach.

a. Explain the security and privacy risks, from the perspective of any stakeholder, presented by unattended online mDL verification.

Unattended verification, practically speaking, presumes the use of biometric technology to ensure that the entity presenting the document is who the identity document was issued to. Due to new regulations concerning consumer privacy and the use of biometric technology by both government and private industry, we are concerned about the broad implications of unattended identification that uploads customer data to unidentified third parties that may have questionable security procedures related to processing the customer's biometric information. We are actively working with several biometric vendors for aftermarket solutions that will meet emerging privacy standards, while leveraging TruAge™ technology for self-service operations.

b. Provide comments on the security protocols that would be required for DMVs to mitigate security and privacy risks presented by unattended online mDL verification.

There are few standards in the industry that would meet an appropriate level of safety from a privacy perspective and we urge the DHS to provide guidance in this area to industry to create certifications for processing of biometric data. There are certifications for PCI compliance (handling payment card data) and ISO27001/ISO 27701 compliance (security, privacy, and operational procedures), we expect some are needed for biometric processing. If such procedures are created, we expect them to perform "match/no match" functions and ideally, wholly handled in secure computing enclaves where there is no chance for the biometric information to be accessible by individuals and corporations that wish to monetize or track what must remain as deeply personal information.

The recent privacy compromises with Amazon's Ring device [https://www.cnbc.com/2020/01/09/ring-fired-four-employees-for-watching-customer-video-feeds.html] provides insight into the sort of dangers that unattended and/or remote verification creates.

13. Costs to Individuals. Provide comments on the estimated costs, including savings, to an individual to obtain an mDL, including:

a. Time and effort required to obtain the mDL.

At present, we see the time and effort required to obtain an mDL as a minimal and acceptable addition to the time and effort required to obtain a physical driver's license, which will be true for any form of digital identification documentation that is meant to replace existing physical documentation.

b. Fees charged by DMVs.

Our understanding is that, at least in some states, there will be an extra fee charged by DMVs to receive an mDL and that there exists a fairly significant problem related to the value generated for an individual by making that purchase. For example, our industry cannot deploy mDL at scale in retail stores and will therefore not be accepting mDL at the point of sale for the foreseeable future. We may allow mDLs to be used when onboarding into the TruAge™ system in an online setting if it is possible for us to verify the mobile driver's license in store, but as we have explained above, doing so is unacceptably expensive to our industry at present.

This creates a fundamental adoption problem for the mDL standard and we expect that these costs are going to be increasingly shifted to consumers, the states, and the federal government given that a number of entities in the retail industry are unwilling to subsidize the investment in mDLs. To contrast this with the TruAge™ program; our industry has made the necessary investment and has greatly reduced the cost of deploying digital identification document infrastructure using our existing infrastructure as well as public and open global standards with broad applicability that are presently being evaluated by DHS/SVIP, DHS/USCIS, and DHS/CBP.

c. Any charges for inclusion of additional information on an mDL, such as HAZMAT endorsements, hunting, fishing, or boating licenses.

Inclusion of information in a digital format requires no additional charges other than the ones that already exist for physical documentation.

14. Considerations for mDL Devices Other than Smartphones. Provide comments on whether provisioning an mDL on, or accessing an mDL from, a device other than a smartphone (e.g., a smartwatch accessing mDL Data from a smartphone paired to it, or a mobile device authorized to access mDL Data stored remotely), poses security or privacy considerations different than provisioning an mDL on, or accessing an mDL from, a smartphone. Explain such security or privacy considerations and how they can be mitigated.

With the usage of appropriate digital signature technology, the storage and/or presentation device should be of no concern to the underlying security or privacy of the system. The device and presentation format shouldn't matter so long as the underlying digital payload being delivered results in the same verifiable information in every scenario. Protection of cryptographic material, both for the issuer and the holder, are the most important security consideration when contemplating different devices.

15. Obstacles to mDL Acceptance. Describe any obstacles to public or industry acceptance of mDLs that DHS should consider in developing its regulatory requirements. Provide comments on recommendations DHS should consider addressing such obstacles, including how to educate the public about security and privacy aspects of digital identity and mDLs.

As we explained in our response to question 13b (and throughout this response), there remains a fundamental adoption problem for the mDL standard. The present cost to the petroleum/convenience industry is far too high to adopt the technology for our day-to-day processes. We expect the same problem to apply to similar industries, such as bars, restaurants, and entertainment venues. We have, however, identified a mechanism that does work for us for our day-to-day identity document processing needs and we have made the necessary industry investment in TruAge™. The deployment of TruAge™ greatly reduces the cost of deploying digital identification document infrastructure by re-using our existing POS infrastructure as well as by using public and open global standards with broad applicability that other industries are investing in, such as the Supply Chain and Education sector.

We are eager to see the work performed by DHS/SVIP and DHS/USCIS on the digital permanent resident card and other forms of W3C Verifiable Credentials move forward, which utilize standards and technologies that will be more cost effective for our industry to adopt and deploy than those provided by the present mDL solution.

Faithfully submitted on July 29, 2021 by:

General Counsel, NACS
Title

If you have further questions, the following individuals are available to engage:

NACS - Gray Taylor, Age Verification Program Manager - gtaylor@conexxus.org
Conexxus - David Ezell, Director of New Initiatives - dezell@conexxus.org