The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Rules

BILL:	SB 1324
INTRODUCER:	Senator Harrell
SUBJECT:	Digital Driver Licenses and Identification Cards
DATE:	April 19, 2021
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Proctor	Vickers	TR	**Favorable**
2.	Wells	Sadberry	AP	**Favorable**
3.	Proctor	Phelps	RC	**Pre-meeting**

I. Summary:

SB 1324 requires the Department of Highway Safety and Motor Vehicles (DHSMV) to establish a secure and uniform system for issuing optional digital proofs of driver licenses and identification cards. The DHSMV may contract with one or more private entities to develop an electronic credentialing system. The electronic credentialing system may not retain internet protocol addresses, geolocation data, or other information that describes the location, computer, computer system, or computer network from which a customer accesses the system.

The bill prohibits a private entity who contracts for data verification through an electronic credentialing system with the DHSMV from storing, selling, or sharing personal information collected by scanning a digital proof of driver license or identification card unless consent has been provided by the individual. The bill creates a civil penalty of up to $5,000 per occurrence for violations of these provisions.

Notwithstanding any law prescribing the design for, or information required to be displayed on, a driver license or identification card, a digital proof of driver license or identification may comprise a limited profile that includes only information necessary to conduct a specific transaction on the electronic credentialing system.

A person may not be issued a digital proof of driver license or identification card until the person satisfies all requirements for issuance of the respective driver license or identification card and has been issued a printed driver license or identification card. Related to false digital identification cards, the bill creates a third degree felony for a person who manufacturers a false card and a second degree misdemeanor for a person who possesses a false card, similar to current penalties related to false digital driver licenses.

The bill may have an insignificant fiscal impact on state government. The bill has an effective date of July 1, 2021.

II. Present Situation:

Digital Driver License

Eleven states are testing mobile driver's licenses or planning pilot projects, including Florida, Arkansas, Colorado, Oklahoma, Louisiana, Iowa, Delaware, Idaho, Maryland, Wyoming and the District of Columbia. New Jersey and Texas have passed legislation to start the process. "A digital driver's license would come in the form of a phone app protected by biometrics or a PIN. Instead of handing over a physical license to a police officer or store clerk, an individual could display the relevant information or send it electronically."[1]

Florida Digital Proof of Driver License

Current Florida law provides for the establishment of a digital proof of driver license. Specifically, current law requires the DHSMV to begin to review and prepare for the development of a secure and uniform system for issuing an optional digital proof of driver license. The statute authorizes the DHSMV to contract with one or more private entities to develop a digital proof of driver license system.[2]

The digital proof of driver license developed by the DHSMV or by an entity contracted by DHSMV must be in a format that allows law enforcement to verify the authenticity of the digital proof of driver license.[3] The DHSMV may adopt rules to ensure valid authentication of digital driver licenses by law enforcement.[4] A person may not be issued a digital proof of driver license until he or she has satisfied all of the statutory requirements relating to the issuance of a physical driver license.[5]

False Digital Proof of Driver License

Current law also establishes certain penalties for a person who manufacturers or possesses a false digital proof of driver license.[6] Specifically, a person who:

- Manufactures a false digital proof of driver license commits a third degree felony, punishable by up to five years in prison[7] and a fine not to exceed $5,000,[8] or punishable under the habitual felony offender statute.[9]
- Possesses a false digital proof of driver license commits a second degree misdemeanor, punishable by up to 60 days in prison[10] and a fine not to exceed $500.[11]

---

[1] Veronica Combs, *Mobile Driver's License Would Replace the Physical Card With a Digital Identity*, Tech Republic, April 15, 2020, https://www.techrepublic.com/article/mobile-drivers-license-would-replace-the-physical-card-with-a-digital-identity/ (last visited March 12, 2021).
[2] Section 322.032(1), F.S.
[3] Section 322.032(2), F.S.
[4] *Id.*
[5] Section 322.032(3), F.S.
[6] Section 322.032(4), F.S.
[7] Section 775.082, F.S.
[8] Section 775.083(1)(c), F.S.
[9] Section 775.084, F.S.
[10] *Supra* note 7.
[11] Section 775.083(1)(e), F.S.

AAMVA and Mobile Driver Licenses

The American Association of Motor Vehicle Administrators (AAMVA) has worked since 2012 to develop identity credential standards, cross-jurisdictional use, authentication, data privacy protection, and other uses of mobile driver licenses. AAMVA has collaborated with Underwriter Laboratories to establish international guidelines and interoperability for industry leaders to test their mobile driver license solutions with one another.[12]

Motorist Modernization

The DHSMV's Motorist Modernization Project is a multi-phased program to modernize legacy applications and processes. The Motorist Modernization Project has committed resources and approved funding to procure a mobile driver license solution as part of Phase II of the Motorist Modernization effort. The Fiscal Year 2020-2021 appropriation for Motorist Modernization Phase II was $9,877,400. Of this amount, $400,000 was allocated for mobile driver license. The mobile driver license includes a digital identification, which is a digital representation of a person's identity; however, the actual mobile driver license is a digital representation of a physical credential and driving privileges. The DHSMV has branded this effort as the "Florida Smart ID." Below is an overview of the Florida Smart ID timeline:

- Received legislative authority to implement in 2014;
- AAMVA standards completed in 2019;
- Vendor awarded contract in June 2020;
- Started work in July 2020; and
- Pilot program slated to start March 25, 2021, and planned to run for 90 days.[13]

Florida Smart ID

The Florida Smart ID has multiple interactions occurring between the systems components comprising the Florida Smart ID solution, including a credential service provider (CSP),[14] the Florida Smart ID device, and an associated verifier device.[15]

The CSP is the gateway or broker between the Florida Smart ID and verifier device interactions with the DHSMV. The CSP uses open data standards and public key infrastructure[16] to

[12] Department of Highway Safety and Motor Vehicles, *2021 Agency Legislative Bill Analysis SB 1324*, (March 5, 2021), p. 2 (on file with the Senate Committee on Transportation).
[13] *Id*. at p. 3.
[14] A credential service provider (CSP) is a trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass registration authorities and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use. National Information Technology Laboratory, Computer Security Resource Center, *Glossary*, https://csrc.nist.gov/glossary/term/credential_service_provider (last visited March 12, 2021).
[15] Kevin Jacobs, Legislative Affairs Director, Department of Highway Safety and Motor Vehicles, Email to Senate Committee on Transportation, *Mobile DL info*, February 23, 2021.
[16] "Public Key Infrastructure (PKI) is the combination of software, encryption technologies, and services that enables entities to protect the security of their communications and business transactions on networks. Using a combination of private (e.g., secret) key and public key cryptography, PKI enables a number of other security services, including data confidentiality, data integrity and non-repudiation. PKI integrates digital certificates, public key cryptography, and certification authorities into one complete network security architecture." U.S. General Services Administration, Fed ID Card, *What is PKI (Public Key*

accomplish the required communications and security. Interactions from the Florida Smart ID, the verifier device, and the CSP are performed over secure web communications.[17]

The Florida Smart ID is used by customers to present proof of identity or age. The application is downloaded from the Apple App or Google Play store and installed on a smart device, such as a smartphone or tablet. Once downloaded, a secure enrollment process occurs using the DHSMV's Virtual Office website. The DHSMV validates the identity and eligibility to activate the Florida Smart ID for use on the device.[18]

Once activated, the Florida Smart ID can be used to interact with retailer or law enforcement verifier devices. This interaction occurs at the consent of the customer and uses Bluetooth, near field communication,[19] or Wi-Fi Direct to communicate with the verifier device. The communication method is determined by a "handshake" between the devices where one device displays a QR code[20] to the other device's camera, which signals how the devices can communicate to each other. The customer selects the type of verification needed (proof of age or law enforcement) and presents a QR to be scanned by the verifier device.[21]

The Florida Smart ID Verifier application may also be integrated into a point of sale system for a seamless interaction with customers to verify a customer's identity or proof or age. When the customer's QR code is scanned, the required information displays on the verifier device. The interaction with the customer device does not store any data, which is protected using encryption within the process.[22]

Verification can be performed in an offline or online mode depending on the verification type. For example, age verification by a retailer is completely offline and does not need to "call back" or interact with the CSP, and would utilize methods, such as Bluetooth, to communicate with the customer's Florida Smart ID. Law enforcement online verification could interact with the CSP to receive the customer's most current driving record.[23]

Infrastructure) and why do I need it?, https://www.fedidcard.gov/faq/what-pki-public-key-infrastructure-and-why-do-i-need-it# (last visited March 12, 2021).

[17] *Supra* note 15.

[18] *Id*.

[19] Near field communication (NFC) is a set of short-range wireless technologies, typically requiring a distance of 4 cm or less to initiate a connection. Developers, *Documentation Guides, Near field communication overview*, https://developer.android.com/guide/topics/connectivity/nfc (last visited March 11, 2021).

[20] QR codes or quick response codes are two-dimensional codes that are scanned with a smartphone, connecting individuals to additional online content or information. They are made up of modules arranged on a contrasting background. Digital.gov, *QR Codes*, https://digital.gov/2013/02/14/qr-codes/ (last visited March 11, 2021).

[21] *Supra* note 15.

[22] *Id*.

[23] *Id*.

III. Effect of Proposed Changes:

Digital Proof of Driver License or Identification Card

The bill revises the current law related to DHSMV review and development of an optional digital proof of driver license to require the DHSMV to establish a secure and uniform system that also includes identification cards.[24]

Section 1 amends s. 322.032, F.S., to authorize the DHSMV to contract with one or more private entities to develop an electronic credentialing system, which is defined as a computer system accessed using a computer, a cellphone, or any other personal device which queries the DHSMV's driver license and identification card records, displays or transmits digital proofs of driver licenses and identification cards, and verifies the authenticity of those electronic credentials. The electronic credentialing system may not retain internet protocol addresses, geolocation data, or other information that describes the location, computer, computer system, or computer network from which a customer accesses the system.

A digital proof of driver license or identification card established by the DHSMV or by a contracted entity must be in a format that allows verification of the authenticity of the digital proof of driver license or identification card. The bill removes the limitation on the use of the digital proof of driver license or identification card to only law enforcement verification.

Unlike the requirements for a physical driver license or identification card, the bill allows a digital proof of driver license or identification card to comprise a limited profile that includes only information necessary to conduct a specific transaction on the electronic credentialing system.[25]

A person may not be issued a digital proof of driver license or identification card until the person satisfies all requirements for issuance of the respective driver license or identification card and has been issued a printed driver license or identification card. The electronic credentialing system must, upon each presentation of a digital driver license or identification card, display or transmit current records for the driver license or identification card. If a licensee's driving privilege is suspended, revoked, or disqualified, or if the person's driver license is otherwise canceled or expired, a digital proof of driver license may not be issued; however, a digital proof of identification card may be issued if the licensee is otherwise eligible for an identification card.

Personal Information

The DHSMV may use a telephone number submitted by a licensee or cardholder in connection with a digital driver license or identification card only for purposes of communication regarding the digital proof of driver license or identification card or the motor vehicle records of the licensee or cardholder.

[24] The bill defines the terms "digital proof of driver license" and "digital proof of identification card" to mean an electronic credential viewable on an electronic credentialing system.
[25] The bill defines the term "limited profile" to mean an electronic credential containing some, but not all, of the information displayed on a printed driver license or identification card.

The bill authorizes the DHSMV to enter into a contract with a private entity that authorizes online data calls or offline data verification through the electronic credentialing system that queries the DHSMV's driver license and identification card records, displays or transmits digital proofs of driver licenses or identification cards, or verifies the authenticity of such electronic credentials.

An individual may consent to allow a private entity to collect and store personal information obtained by scanning[26] the individual's digital proof of driver license or identification card. However, the individual must be informed of what information is collected and the purpose or purposes for which the information will be used. If the individual does not want the private entity to scan the digital proof of the individual's driver license or identification card, the private entity may manually collect personal information from the individual.

Except as provided above, a private entity that contracts with the DHSMV and that scans a digital proof of driver license or identification card may not store, sell, or share personal information collected from such scanning of the digital proof of driver license or identification card.

A private entity that violates these provisions is subject to a civil penalty not to exceed $5,000 per occurrence. However, this does not apply to a financial institution as defined in s. 655.005(1)(i), F.S.[27]

SB 1326, which is linked to this bill, creates public records exemptions for:
- Secure login credentials held by the DHSMV; and
- Internet protocol addresses, geolocation data, and other information held by the DHSMV which describes the location, computer, computer system, or computer network from which a user accesses a public-facing portal, and the dates and times that a user accesses a public-facing portal.

False Digital Proof of Identification Card

The bill establishes penalties for a person who manufacturers or possesses a false digital identification card. Specifically, a person who:
- Manufactures a false digital proof of identification card commits a third degree felony, punishable by up to five years in prison[28] and a fine not to exceed $5,000,[29] or punishable under the habitual felony offender statute.[30]

[26] The bill defines the term "scanning" to mean obtaining data from a digital proof of driver license or identification card in an electronic format.
[27] Section 655.005(1)(i), F.S., defines "financial institution" to mean a state or federal savings or thrift association, bank, savings bank, trust company, international bank agency, international banking corporation, international branch, international representative office, international administrative office, international trust entity, international trust company representative office, qualified limited service affiliate, credit union, or an agreement corporation operating pursuant to s. 25 of the Federal Reserve Act, 12 U.S.C. ss. 601 et seq. or Edge Act corporation organized pursuant to s. 25(a) of the Federal Reserve Act, 12 U.S.C. ss. 611 et seq.
[28] Section 775.082, F.S.
[29] Section 775.083(1)(c), F.S.
[30] Section 775.084, F.S.

- Possesses a false digital proof of identification card commits a second degree misdemeanor, punishable by up to 60 days in prison[31] and a fine not to exceed $500.[32]

Rulemaking Authority

The bill authorizes the DHSMV to adopt rules to ensure valid authentication of digital driver licenses and identification cards.

Other Related Changes

Section 2 amends s. 322.14, F.S., to clarify that upon successful completion of all required examinations and payment of the required fee the DHSMV will issue to every qualified applicant a *printed* driver license.

Section 3 amends s. 322.15, F.S., to provide that if a law enforcement officer or authorized representative of the DHSMV is unable to immediately verify the digital proof of driver license, upon the demand of the law enforcement officer or authorized representative of the DHSMV, the licensee must present or submit the licensee's printed driver license.

Section 4 reenacts s. 322.15(2), F.S., to incorporate changes made by the bill.

Effective Date

Section 5 provides an effective date of July 1, 2021.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

This bill does not change any current public records exemptions. SB 1326, which is linked to this bill, creates a public records exemption for certain information related to the credentialing system.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

[31] Section 775.082, F.S.
[32] Section 775.083(1)(e), F.S.

E. Other Constitutional Issues:

None identified.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

The bill may have an indeterminate fiscal impact on the private sector. Businesses who wish to provide electronic verification of Florida Smart ID will need the retail reader application installed on a mobile device that supports either the android or IOS operating systems. Additionally, if the business prefers to integrate the verification process into its point of sale systems rather than use a mobile device it would require development to be done by the business to integrate a retail reader application into the point of sale systems.[33]

The bill creates a civil penalty of up to $5,000 for each violation of provisions related to personal information and data collection.

C. Government Sector Impact:

State and local law enforcement agencies will need to train their members and update associated enforcement policies for the Florida Smart ID. This may have an indeterminate, likely insignificant fiscal impact on state and local government.[34]

The DHSMV has already undertaken development of the Florida Smart ID through existing law and therefore already has the resources to continue with the expanded requirements of the bill. Due to this, the fiscal impact on the DHSMV is minimal and can be handled within existing resources.[35]

The Criminal Justice Estimating Conference met on March 24, 2021, and estimated that the bill would have an impact of an increase of 10 or fewer prison beds (positive insignificant impact). The bill creates a third degree felony for manufacturing a false digital proof of driver license.

VI. Technical Deficiencies:

None.

[33] *Supra* note 12 at p. 7.
[34] *Id*. at p. 6.
[35] *Id*.

VII. Related Issues:

The bill authorizes the DHSMV to adopt rules to ensure valid authentication of digital driver licenses and identification cards.

VIII. Statutes Affected:

The bill substantially amends the following sections of the Florida Statutes: 322.032, 322.14, and 322.15.

The bill reenacts section 322.121 of the Florida Statutes.

IX. Additional Information:

A. Committee Substitute – Statement of Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

None.

B. Amendments:

None.