15100943D

SENATE BILL NO. 814

Offered January 14, 2015

Prefiled January 2, 2015

A BILL to amend the Code of Virginia by adding in Title 2.2 a chapter numbered 4.3, consisting of sections numbered 2.2-435.9 and 2.2-435.10, and by adding in Title 59.1 a chapter numbered 50, consisting of sections numbered 59.1-550 through 59.1-553, relating to electronic identity management; standards; liability.

Patron—Watkins

Referred to Committee on General Laws and Technology

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding in Title 2.2 a chapter numbered 4.3, consisting of sections numbered 2.2-435.9 and 2.2-435.10, and by adding in Title 59.1 a chapter numbered 50, consisting of sections numbered 59.1-550 through 59.1-553, as follows:

CHAPTER 4.3.

COMMONWEALTH IDENTITY MANAGEMENT STANDARDS.

§ 2.2-435.9. Approval of electronic identity standards.

A. The Secretary of Technology and the Secretary of Transportation shall review and approve or disapprove, upon the recommendation of the Identity Management Standards Advisory Council pursuant to § 2.2-435.10, guidance documents that adopt (i) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions, (ii) the minimum specifications and standards that should be included in an identity trust framework, as defined in § 59.1-550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§ 59.1-550 et seq.), and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

B. Final guidance documents approved pursuant to subsection A shall be posted on the Virginia Regulatory Town Hall and published in the Virginia Register of Regulations as a general notice. The Secretaries shall also jointly annually file a list of available guidance documents developed pursuant to this chapter pursuant to § 2.2-4008 of the Virginia Administrative Process Act (§ 2.2-4000 et seq.).

§ 2.2-435.10. Identity Management Standards Advisory Council.

A. The Identity Management Standards Advisory Council is established to advise the Secretary of Technology and the Secretary of Transportation on the adoption of identity management standards. The Advisory Council shall advise the Secretaries of Technology and Transportation on the creation of guidance documents concerning (i) the utilization of nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions, (ii) the minimum specifications and standards that should be included in an identity trust framework, as defined in § 59.1-550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§ 59.1-550 et seq.), and (iii) the use or adoption of any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

B. 1. The Advisory Council shall consist of seven members, to be appointed by the Governor, with expertise in electronic identity management and information technology . Members shall include a representative of the Department of Motor Vehicles, a representative of the Virginia Information Technologies Agency, and five representatives of the business community with appropriate experience and expertise. In addition to the seven appointed members, the Chief Information Officer of the Commonwealth, or his designee, may also serve as an ex officio member of the Advisory Council.

2. The Advisory Council shall designate one of its members as chairman.

3. Members appointed to the Advisory Council shall serve four-year terms, subject to the pleasure of the Governor, and may be reappointed.

4. Members shall serve without compensation but shall be reimbursed for all reasonable and necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.

C. Proposed guidance documents and general opportunity for oral or written submittals as to those guidance documents shall be posted on the Virginia Regulatory Town Hall and published in the Virginia Register of Regulations as a general notice following the processes and procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§ 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written comments following the posting and publication and shall hold at least one meeting dedicated to the receipt of oral comment no less than 15 days after the posting and publication. The Advisory Council shall also develop methods

for the identification and notification of interested parties and specific means of seeking input from interested persons and groups.

CHAPTER 50.

ELECTRONIC IDENTITY MANAGEMENT ACT.

§ 59.1-550. Definitions.

As used in this chapter, unless the context requires a different meaning:

"Attribute provider" means an entity, or a supplier, employee, or agent thereof, who acts as the authoritative record of identifying information about an identity credential holder.

"Commonwealth identity management standards" means the minimum specifications and standards that must be included in an identity trust framework so as to warrant liability protection pursuant to this chapter that are set forth in guidance documents approved by the Secretary of Technology and the Secretary of Transportation pursuant to Chapter 4.3 (§ 2.2-435.9 et seq.) of Title 2.2.

"Identity attribute" means identifying information associated with an identity credential holder.

"Identity credential" means the data, or the physical object upon which the data may reside, that an identity credential holder may present to verify or authenticate his identity in a digital or online transaction.

"Identity credential holder" means a person bound to or in possession of an identity credential who has agreed to the terms and conditions of the identity provider.

"Identity proofer" means a person or entity authorized to act as a representative of an identity provider in the confirmation of a potential identity credential holder's identification and identity attributes prior to issuing an identity credential to a person.

"Identity provider" means an entity, or a supplier, employee, or agent thereof, certified by an identity trust framework operator to provide identity credentials that may be used by an identity credential holder to assert his identity, or any related attributes, in a digital or online transaction. For purposes of this chapter, "identity provider" includes an attribute provider, an identity proofer, and any suppliers, employees, or agents thereof.

"Identity trust framework" means a digital identity system with established identity, security, privacy, technology, and enforcement rules and policies adhered to by certified identity providers that are members of the identity trust framework. Members of an identity trust framework include identity trust framework operators and identity providers. Relying parties may be, but are not required to be, a member of an identity trust framework in order to accept an identity credential issued by a certified identity provider to verify an identity credential holder's identity.

"Identity trust framework operator" means the entity that (i) defines rules and policies for member parties to an identity trust framework, (ii) certifies identity providers to be members of and issue identity credentials pursuant to the identity trust framework, and (iii) evaluates participation in the identity trust framework to ensure compliance by members of the identity trust framework with its rules and policies, including the ability to request audits of participants for verification of compliance.

"Relying party" is an individual or entity that relies on the validity of an identity credential or an associated trustmark.

"Trustmark" means a machine-readable official seal, authentication feature, certification, license, or logo that may be provided by an identity trust framework operator to certified identity providers within its identity trust framework to signify that the identity provider complies with the identity trust framework rules and policies.

§ 59.1-551. Trustmark; warranty.

The use of a trustmark on an identity credential provides a warranty by the identity provider that the rules and policies of the identity trust framework of which it is a member have been adhered to in asserting the identity and any related attributes contained on the identity credential. No other warranties are applicable unless expressly provided by the identity provider.

§ 59.1-552. Civil immunity.

A. An identity trust framework operator shall be immune from civil liability for any act or omission relating to (i) the issuance of an identity credential or assignment of an identity attribute to an identity credential holder or (ii) the issuance of a trustmark to an identity provider, provided that the credential, attribute, or trustmark was issued in accordance with the specifications of the operator's identity trust framework that meets or exceeds the Commonwealth's identity management standards.

B. An identity provider shall be immune from civil liability for any act or omission relating to the issuance of an identity credential or assignment of an identity attribute to an identity credential holder, provided that the identity credential or identity attribute was issued or assigned in accordance with the specifications of the identity trust framework of which the identity provider is a member that meets or exceeds the Commonwealth's identity management standards.

C. Nothing in subsection A or B shall prevent or limit the liability of an identity trust framework operator or an identity provider if such operator or provider commits an act or omission that (i) constitutes gross negligence or willful misconduct or (ii) does not adhere to the rules and policies of its

respective identity trust framework that meets or exceeds Commonwealth identity management standards.

§ 59.1-553. Sovereign immunity.

No provisions of this chapter nor any act or omission of a state, regional, or local governmental entity related to the issuance of electronic identity credentials or attributes or the administration or participation in an identity trust framework related to the issuance of electronic identity credentials or attributes shall be deemed a waiver of sovereign immunity to which the governmental entity or its officers, employees, or agents are otherwise entitled.