CHAPTER 483

An Act to amend the Code of Virginia by adding in Title 2.2 a chapter numbered 4.3, consisting of sections numbered 2.2-436 and 2.2-437, and by adding in Title 59.1 a chapter numbered 50, consisting of sections numbered 59.1-550 through 59.1-555, relating to electronic identity management; standards; liability.

[S 814]

Approved March 23, 2015

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 2.2-436 and 2.2-437, and by adding in Title 59.1 a chapter numbered 50, consisting of sections numbered 59.1-550 through 59.1-555, as follows:

CHAPTER 4.3.

COMMONWEALTH IDENTITY MANAGEMENT STANDARDS.

§ 2.2-436. Approval of electronic identity standards.

A. The Secretary of Technology, in consultation with the Secretary of Transportation, shall review and approve or disapprove, upon the recommendation of the Identity Management Standards Advisory Council pursuant to § 2.2-437, 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 Secretary of Technology shall send a copy of the final guidance documents to the Joint Commission on Administrative Rules established pursuant to § 30-73.1 at least 90 days prior to the effective date of such guidance documents. The Secretary of Technology shall also 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.) and shall send a copy of such list to the Joint Commission on Administrative Rules.

§ 2.2-437. Identity Management Standards Advisory Council.

A. The Identity Management Standards Advisory Council (the Advisory Council) is established to advise the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to § 2.2-436.

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.

5. Staff to the Advisory Council shall be provided by the Office of the Secretary of Technology.

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. The Advisory Council shall send a copy of such notices, comments, and other background material relative to the development of the recommended guidance documents to the Joint Commission on Administrative Rules.

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, that 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 define liability pursuant to this chapter that are set forth in guidance documents approved by the Secretary of Technology pursuant to Chapter 4.3 (§ 2.2-436 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 written rules and policies of the identity trust framework.

§ 59.1-551. Trustmark; warranty.

The use of a trustmark on an identity credential provides a warranty by the identity provider that the written 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. Establishment of liability; limitation of liability.

A. An identity trust framework operator or identity provider shall be liable if the issuance of an identity credential or assignment of an identity attribute, or a trustmark, is not in compliance with the Commonwealth's identity management standards in place at the time of issuance. Further, the identity trust framework operator or identity provider shall be liable for noncompliance with applicable terms of any contractual agreement with a contracting party and any written rules and policies of the identity trust framework of which it is a member.

B. An identity trust framework operator or identity provider shall not be liable if the issuance of the identity credential or assignment of an identity attribute or a trustmark was in compliance with (i) the Commonwealth's identity management standards in place at the time of issuance or assignment, (ii) applicable terms of any contractual agreement with a contracting party, and (iii) any written rules and policies of the identity trust framework of which it is a member, provided such identity trust framework operator or identity provider did not commit an act or omission that constitutes gross negligence or willful misconduct. An identity trust framework operator or identity provider shall not be liable for misuse of an identity credential by the identity credential holder or by any other person who misuses an identity credential.

§ 59.1-553. Commercially reasonable security procedures for electronic fund transfers.

Use of an identity credential or identity attribute shall satisfy any requirement for a commercially reasonable security or attribution procedure in Title 8.4A, the Uniform Electronic Transactions Act

(§ 59.1-479 et seq.), and the Uniform Computer Information Transactions Act (§ 59.1-501.1 et seq.), provided that the identity credential or identity attribute was issued or assigned in accordance with (i) the Commonwealth's identity management standards in place at the time of issuance or assignment, (ii) the terms of any contractual agreement, and (iii) any written rules and policies of the identity trust framework of which the issuer is a member.

§ 59.1-554. Applicability of chapter.

The provisions of this chapter shall not be construed to require any individual or entity to rely on or accept any identity credential or attribute issued in accordance with Commonwealth identity management standards or this chapter.

§ 59.1-555. 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.