20102986D

SENATE BILL NO. 665

Offered January 8, 2020

Prefiled January 7, 2020

A BILL to amend and reenact §§ 59.1-550 through 59.1-553 and 59.1-555 of the Code of Virginia, relating to the Electronic Identity Management Act; federated digital identity systems.

Patron—Boysko

Referred to Committee on Commerce and Labor

Be it enacted by the General Assembly of Virginia:

1. That §§ 59.1-550 through 59.1-553 and 59.1-555 of the Code of Virginia are amended and reenacted as follows:

§ 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.

"Federated digital identity system" or "federation" means a digital identity system that (i) utilizes federated identity management to enable the portability of identity information across otherwise autonomous security domains; (ii) is compliant with the Commonwealth's identity management standards and with the provisions of the governing identity trust framework; (iii) has established identity, security, privacy, technology, and enforcement rules and policies adhered to by certified identity providers that are members of the federated digital identity system; (iv) includes as members identity trust framework operators and identity providers; and (v) allows, but does not require, relying parties to be members of the federated digital identity system in order to accept an identity credential issued by a certified identity provider to verify an identity credential holder's identity.

"Federated identity management" means a process that allows the conveyance of identity credentials and authentication information across digital identity systems through the use of a common set of policies, practices, and protocols for managing the identity of users and devices across security domains.

"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 *or federation* to signify that the identity provider complies with the written rules and policies of the identity trust framework *or federation*.

§ 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 *or federation* 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 *or federation* 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 *or federation* 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 *or federation* of which the issuer is a member.

§ 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 *or federation* 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.