

## SENATE BILL NO. \_\_\_\_\_ HOUSE BILL NO. \_\_\_\_\_

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

5 **Be it enacted by the General Assembly of Virginia:**

6 **1. That the Code of Virginia is amended by adding in Title 2.2 a Chapter 4.3, consisting of**  
7 **sections numbered 2.2-435.9 and 2.2-435.10, and by adding in Title 59.1 a chapter numbered**  
8 **50, consisting of sections numbered 59.1-550 through 59.1-553, as follows:**

9 CHAPTER 4.3

10 COMMONWEALTH IDENTITY MANAGEMENT STANDARDS

11 § 2.2-435.9. Approval of Electronic Identity Standards.

12 A. The Secretary of Technology and the Secretary of Transportation shall review and approve or  
13 disprove, upon the recommendation of the Identity Management Standards Advisory Council, guidance  
14 documents that adopt (a) nationally recognized technical and data standards regarding the verification  
15 and authentication of identity in digital and online transactions, (b) the minimum specifications and  
16 standards that should be included in an identity trust framework so as to warrant liability protection  
17 pursuant to the Electronic Identity Liability Protection Act (§ 8.01-227.24 et seq.), and (c) any other  
18 related data standards or specifications concerning reliance by third parties on identity credentials.

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

23 § 2.2-435.10. Identity Management Standards Advisory Council

24 A. The Governor shall appoint an advisory committee of persons with expertise in electronic  
25 identity management and information technology to advise the Secretaries of Technology and

26 Transportation on the creation of guidance documents concerning (i) the utilization of nationally  
27 recognized technical and data standards regarding the verification and authentication of identity in  
28 digital and online transactions, (ii) the minimum specifications and standards that should be included in  
29 an identity trust framework so as to warrant liability protection pursuant to the Electronic Identity  
30 Liability Protection Act (§ 8.01-227.24 et seq.), and (iii) the use or adoption of any other related data  
31 standards or specifications concerning reliance by third parties on identity credentials.

32 B. 1. The advisory committee shall consist of seven members. Members shall include a  
33 representative of the Department of Motor Vehicles, the Virginia Information Technology Agency, and  
34 representatives of the business community with appropriate experience and expertise. In addition to the  
35 seven appointed members, the Chief Information Officer of the Commonwealth, or his designee, may  
36 also serve as an ex officio member of the advisory committee.

37 2. The advisory committee shall designate one of its members as chairman.

38 3. Members appointed to the advisory committee shall serve four year terms, subject to the  
39 pleasure of the Governor, and may be reappointed.

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

42 C. Proposed guidance documents and general opportunity for oral or written submittals as to  
43 those guidance documents shall be posted on the Virginia Regulatory Town Hall and published in the  
44 Virginia Register of Regulations as a general notice following the processes and procedures set forth in  
45 subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§ 2.2-4000 et seq.). The  
46 Advisory Committee shall allow at least 30 days for the submission of written comments following the  
47 posting and publication, and shall hold at least one meeting dedicated to the receipt of oral comment no  
48 less than 15 days after the posting and publication. The Advisory Committee shall also develop methods  
49 for the identification and notification of interested parties and specific means of seeking input from  
50 interested persons and groups.

51 CHAPTER 50.

52 Electronic Identity Management Act

53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78

§ 59.1-550. Definitions.

As used in this article 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 article 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" is 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 article, "identity provider" shall also include 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, but are not required, to be a

79 member of an identity trust framework in order to accept an identity credential issued by a certified  
80 identity provider to verify an identity credential holder's identity.

81 "Identity trust framework operator" means the entity that (a) defines rules and policies for  
82 member parties to a trust framework, (b) certifies identity providers to be members of and issue identity  
83 credentials pursuant to the trust framework, and (c) evaluates participation in the trust framework to  
84 ensure compliance by members of the identity trust framework with its rules and policies, including the  
85 ability to request audits of participants for verification of compliance.

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

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

92 § 59.1-551. Trustmark; warranty.

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

97 §59.1-552. Civil immunity.

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

103 B. An identity provider shall be immune from civil liability for any acts or omissions relating to  
104 the issuance of an identity credential or assignment of an attribute to an identity credential holder,  
105 provided that the credential or attribute was issued or assigned in accordance with the specifications of

106 the trust framework of which the provider is a member that meets or exceeds the Commonwealth's  
107 identity management standards.

108 C. Nothing in subsection A or B shall prevent or limit the liability of an identity trust framework  
109 operator or an identity provider if the operator or provider commits and act or omission that (i)  
110 constitutes gross negligence or willful misconduct, or (ii) does not adhere to the rules and policies of its  
111 respective trust framework that meets or exceeds Commonwealth identity management standards.

112 § 59.1-553. Sovereign Immunity.

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

118 #