

**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, by adding in article 35 of Chapter 26 of Title 2.2 a  
3 sectioned numbered 2.2-2699.8 and by adding in Chapter 3 of Title 8.01 an article numbered 26,  
4 consisting of sections numbered 8.01-227.24 through 8.01-227.27, relating to electronic identity  
5 providers; liability.

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

7 **1. That the Code of Virginia is amended by adding in Title 2.2 a Chapter 4.3, consisting of**  
8 **sections numbered 2.2-435.9 and 2.2-435.10, by adding in article 35 of Chapter 26 of Title 2.2 a**  
9 **sectioned numbered 2.2-2699.8 and by adding in Chapter 3 of Title 8.01 an article numbered 26,**  
10 **consisting of sections numbered 8.01-227.24 through 8.01-227.27, as follows:**

11 CHAPTER 4.3

12 COMMONWEALTH IDENTITY MANAGEMENT STANDARDS

13 § 2.2-435.9. Approval of Electronic Identity Standards.

14 The Secretary of Technology and the Secretary of Transportation shall review and approve or  
15 disprove, upon the recommendation of the Information Technology Advisory Council pursuant to § 2.2-  
16 2699.6, the adoption of (a) nationally recognized technical and data standards regarding the verification  
17 and authentication of identity in digital and online transactions, (b) the minimum specifications and  
18 standards that should be included in an identity trust framework so as to warrant liability protection  
19 pursuant to the Electronic Identity Liability Protection Act (§ 8.01-227.24 et seq.), and (c) any other  
20 related data standards or specifications concerning reliance by third parties on identity credentials.

21 § 2.2-435.10. Publication of Standards

22 The Secretary of Technology and the Secretary of Transportation shall cause the standards and  
23 specifications adopted pursuant to this Chapter be published in multiple locations, including but not  
24 limited in the Virginia Administrative Code and on the website of the Secretary of Technology, the  
25 Secretary of Transportation, and the Virginia Economic Development Partnership, the minimum

26 specifications and standards that must be included in an identity trust framework so as to warrant  
27 liability protection pursuant to the Electronic Identity Liability Protection Act (§ 8.01-227.24 et seq.).

28 **§ 2.2-2699.6. Powers and duties of the ITAC.**

29 A. The ITAC shall have the power and duty to:

30 1. Adopt rules and procedures for the conduct of its business;

31 2. Advise the CIO on the development of all major information technology projects as defined in  
32 § 2.2-2006;

33 3. Advise the CIO on strategies, standards, and priorities for the use of information technology  
34 for state agencies in the executive branch of state government;

35 4. Advise the CIO on developing the two-year plan for information technology projects;

36 5. Advise the CIO on statewide technical and data standards for information technology and  
37 related systems, including the utilization of nationally recognized technical and data standards for health  
38 information technology systems or software purchased by a state agency of the Commonwealth;

39 6. Advise the CIO on statewide information technology architecture and related system  
40 standards;

41 7. Advise the CIO on assessing and meeting the Commonwealth's business needs through the  
42 application of information technology;

43 8. Advise the CIO on the prioritization, development, and implementation of enterprise-wide  
44 technology applications; annually review all agency technology applications budgets; and advise the  
45 CIO on infrastructure expenditures; ~~and~~

46 9. Advise the CIO on the development, implementation, and execution of a technology  
47 applications governance framework for executive branch agencies. Such framework shall establish the  
48 categories of use by which technology applications shall be classified, including but not limited to  
49 enterprise-wide, multiagency, or agency-specific. The framework shall also provide the policies and  
50 procedures for determining within each category of use (i) the ownership and sponsorship of  
51 applications, (ii) the proper development of technology applications, (iii) the schedule for maintenance  
52 or enhancement of applications, and (iv) the methodology for retirement or replacement of applications.

53 ITAC shall include the participation of agency leaders who are necessary for defining agency business  
54 needs, as well as agency information technology managers who are necessary for overseeing technology  
55 applications performance relative to agency business needs. Agency representatives shall assist ITAC in  
56 determining the potential information technology solutions that can meet agency business needs, as well  
57 as how those solutions may be funded; and

58 10. Advise the Secretary of Technology and the Secretary of Transportation, upon the  
59 recommendation of the Electronic Identity Standards Advisory Committee pursuant to § 2.2-2699.8, on  
60 the adoption of (a) nationally recognized technical and data standards regarding the verification and  
61 authentication of identity in digital and online transactions, (b) the minimum specifications and  
62 standards that should be included in an identity trust framework so as to warrant liability protection  
63 pursuant to the Electronic Identity Liability Protection Act (§ 8.01-227.24 et seq.), and (c) any other  
64 related data standards or specifications concerning reliance by third parties on identity credentials.

65 B. Definitions.

66 As used in this section, the term "technology applications" includes, but is not limited to,  
67 hardware, software, maintenance, facilities, contractor services, goods, and services that promote  
68 business functionality and facilitate the storage, flow, use or processing of information by agencies of  
69 the Commonwealth in the execution of their business activities.

70 § 2.2-2699.8. Electronic Identity Standards Advisory Committee.

71 A. The ITAC shall appoint an advisory committee of persons with expertise in electronic identity  
72 management and information technology to advise the ITAC on (i) the utilization of nationally  
73 recognized technical and data standards regarding the verification and authentication of identity in  
74 digital and online transactions, (ii) the minimum specifications and standards that should be included in  
75 an identity trust framework so as to warrant liability protection pursuant to the Electronic Identity  
76 Liability Protection Act (§ 8.01-227.24 et seq.), and (iii) the use or adoption of any other related data  
77 standards or specifications concerning reliance by third parties on identity credentials.

78 B. The advisory committee shall consist of seven members. Members shall be appointed based  
79 upon recommendations of the Secretary of Technology and the Secretary of Transportation, and shall

80 include a representative of the Department of Motor Vehicles, the Virginia Information Technology  
81 Agency, and representatives of the business community with appropriate experience and expertise.  
82 Members appointed to serve on the advisory committee shall serve without compensation, but shall be  
83 reimbursed for all reasonable and necessary expenses incurred in the performance of their duties as  
84 provided in § 2.2-2825. In addition to the appointed members, the CIO, the Secretary of Technology,  
85 and the Secretary of Transportation, or their designees, may also serve on the advisory committee.

86 C. The advisory committee shall collaborate with relevant state agencies and private sector  
87 entities as necessary and appropriate to develop its recommendations.

88 D. Terms used in this section shall have the same meaning as set forth in § 8.01-227.24.

#### 89 Article 26.

#### 90 Electronic Identity Liability Protection Act

#### 91 § 8.01-227.24. Definitions.

92 As used in this article unless the context requires a different meaning:

93 "Commonwealth identity management standards" means the standards and specifications  
94 approved by the Secretary of Technology and the Secretary of Transportation pursuant to Chapter 4.3 (§  
95 2.2-435.9 et seq.) of Title 2.2 that establish the minimum specifications and standards that must be  
96 included in an identity trust framework so as to warrant liability protection pursuant to this article.

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

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

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

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

106 "Identity provider" means an entity, or a supplier, employee, or agent thereof, certified by an  
107 identity trust framework to provide identity credentials that may be used by an identity credential holder  
108 to assert his identity, or any related attributes, in a digital or online environment. For purposes of this  
109 article, "identity provider" shall also include an attribute provider, an identity proofer, and any suppliers,  
110 employees, or agents thereof.

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

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

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

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

128 § 8.01-227.25. Trustmark; warranty.

129 A. The use of a trustmark on an electronic identity credential provides a warranty solely for the  
130 assertion of the identity and any attributes of the identity credential holder contained on the identity  
131 credential, but does not create an implied warranty for any other element of the specific transaction for  
132 which the identity is asserted.

133 §8.01-227.26. Civil immunity.

134 A. No identity trust framework operator shall be liable for civil damages arising from any acts or  
135 omissions relating to (i) the issuance of an identity credential or assignment of an identity attribute to an  
136 identity credential holder, or (ii) the issuance of a trustmark to a identity provider, provided that the  
137 credential, attribute, or trustmark was issued in accordance with the specifications of the operator's  
138 identity trust framework that meets or exceeds the Commonwealth's identity management standards.

139 B. No identity provider shall be liable for civil damages arising from any acts or omissions  
140 relating to the issuance of an identity credential or assignment of an attribute to an identity credential  
141 holder, provided that the credential or attribute was issued or assignend in accordance with the  
142 specifications of the trust framework of which the provider is a member that meets or exceeds the  
143 Commonwealth's identity management standards.

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

148 § 8.01-227.27. Sovereign Immunity.

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

154 #