

1 A bill to be entitled
 2 An act relating to cybersecurity incident liability;
 3 creating s. 768.401, F.S.; providing definitions;
 4 providing that a county, municipality, other political
 5 subdivision of the state, covered entity, or third-
 6 party agent that complies with certain requirements is
 7 not liable in connection with a cybersecurity incident
 8 under certain circumstances; requiring covered
 9 entities and third-party agents to adopt revised
 10 frameworks, standards, laws, or regulations within a
 11 specified time period; providing that a private cause
 12 of action is not established; providing that certain
 13 failures are not evidence of negligence, do not
 14 constitute negligence per se, and cannot be used as
 15 evidence of fault; specifying that the defendant in
 16 certain actions has a certain burden of proof;
 17 providing applicability; providing an effective date.

18
 19 Be It Enacted by the Legislature of the State of Florida:

20
 21 **Section 1. Section 768.401, Florida Statutes, is created**
 22 **to read:**

23 768.401 Limitation on liability for cybersecurity
 24 incidents.-

25 (1) As used in this section, the term:

26 (a) "Covered entity" means a sole proprietorship,
27 partnership, corporation, trust, estate, cooperative,
28 association, or other commercial entity.

29 (b) "Cybersecurity standards or frameworks" means one or
30 more of the following:

31 1. The National Institute of Standards and Technology
32 (NIST) Framework for Improving Critical Infrastructure
33 Cybersecurity;

34 2. NIST special publication 800-171;

35 3. NIST special publications 800-53 and 800-53A;

36 4. The Federal Risk and Authorization Management Program
37 security assessment framework;

38 5. The Center for Internet Security (CIS) Critical
39 Security Controls;

40 6. The International Organization for
41 Standardization/International Electrotechnical Commission 27000-
42 57 series (ISO/IEC 27000) family of standards;

43 7. HITRUST Common Security Framework (CSF);

44 8. Service Organization Control Type 2 Framework (SOC 2);

45 9. Secure Controls Framework; or

46 10. Other similar industry frameworks or standards, or a
47 reasonable combination of one or more of the above.

48 (c) "Third-party agent" means an entity that has been
49 contracted to maintain, store, or process personal information
50 on behalf of a covered entity.

51 (2) A county or municipality is not liable in connection
 52 with a cybersecurity incident if the county or municipality has:

53 (a)1. One or more policies that substantially align with
 54 cybersecurity standards or frameworks;

55 2. Disaster recovery plans for cybersecurity incidents;
 56 and

57 3. Multi-factor authentication as required by the
 58 cybersecurity standards or frameworks relied on in sub-
 59 subparagraph (3) (b)1.a.; or

60 (b) Applied to the Local Government Cybersecurity Grant
 61 Program and shares telemetry data with the state's cybersecurity
 62 operations center.

63 (3) A covered entity or third-party agent that acquires,
 64 maintains, stores, processes, or uses personal information is
 65 not liable in a class action resulting from a cybersecurity
 66 incident if the covered entity or third-party agent does all of
 67 the following, as applicable:

68 (a) Substantially complies with s. 501.171(3)-(6), as
 69 applicable.

70 (b) Has adopted or implemented:

71 1.a. One or more policies that substantially align with
 72 cybersecurity standards or frameworks;

73 b. A disaster recovery plan for cybersecurity incidents;
 74 and

75 c. Multi-factor authentication as required by the

76 cybersecurity standards or frameworks relied on in sub-
77 subparagraph a.; or

78 2. If regulated by the state or Federal Government, or
79 both, or if otherwise subject to the requirements of any of the
80 following laws and regulations, a cybersecurity program that
81 substantially aligns with the current version of the following,
82 as applicable:

83 a. The Health Insurance Portability and Accountability Act
84 of 1996 security requirements in 45 C.F.R. part 160 and part 164
85 subparts A and C.

86 b. Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L.
87 No. 106-102, as amended, and its implementing regulations.

88 c. The Federal Information Security Modernization Act of
89 2014, Pub. L. No. 113-283.

90 d. The Health Information Technology for Economic and
91 Clinical Health Act requirements in 45 C.F.R. parts 160 and 164.

92 e. The Criminal Justice Information Services (CJIS)
93 Security Policy.

94 f. Other similar requirements mandated by state or federal
95 law or regulation.

96 (4) A covered entity's or third-party agent's substantial
97 alignment with a framework or standard under subparagraph
98 (3)(b)1. or with a law or regulation under subparagraph (3)(b)2.
99 may be demonstrated by providing documentation or other evidence
100 of an assessment, conducted internally or by a third-party,

101 reflecting that the covered entity's or third-party agent's
102 cybersecurity program is substantially aligned with the relevant
103 framework or standard or with the applicable state or federal
104 law or regulation.

105 (5) Any covered entity or third-party agent must
106 substantially align its cybersecurity program with any revisions
107 of relevant frameworks or standards or of applicable state or
108 federal laws or regulations within 1 year after the latest
109 publication date stated in any such revisions in order to retain
110 protection from liability.

111 (6) This section does not establish a private cause of
112 action.

113 (7) Failure of a county, municipality, other political
114 subdivision of the state, covered entity, or third-party agent
115 to substantially implement a cybersecurity program that is in
116 compliance with this section is not evidence of negligence, does
117 not constitute negligence per se, and cannot be used as evidence
118 of fault under any other theory of liability.

119 (8) In an action relating to a cybersecurity incident, if
120 the defendant is a county, municipality, or political
121 subdivision covered by subsection (2) or a covered entity or
122 third-party agent covered by subsection (3), the defendant has
123 the burden of proof to establish substantial compliance.

124 **Section 2.** The amendments made by this act apply to any
125 putative class action filed on or after the effective date of

HB 1183

2025

126 | this act.

127 | **Section 3.** This act shall take effect upon becoming a law.