MISSISSIPPI LEGISLATURE REGULAR SESSION 2025

By: Senator(s) Williams, Boyd

To: Judiciary, Division A

SENATE BILL NO. 2471

AN ACT TO PROVIDE THAT A COUNTY OR MUNICIPALITY AND ANY OTHER POLITICAL SUBDIVISION OF THE STATE SHALL NOT BE LIABLE IN CONNECTION WITH A CYBERSECURITY INCIDENT IF THE ENTITY ADOPTS CERTAIN CYBERSECURITY STANDARDS; TO REQUIRE CYBERSECURITY PROGRAMS TO ALIGN WITH NATIONALLY-RECOGNIZED STANDARDS AND THE REQUIREMENTS OF SPECIFIED FEDERAL LAWS; TO PROVIDE A REBUTTABLE PRESUMPTION AGAINST LIABILITY FOR COMMERCIAL ENTITIES THAT ARE IN SUBSTANTIAL COMPLIANCE WITH THIS ACT BY ADOPTING A CYBERSECURITY PROGRAM THAT SUBSTANTIALLY ALIGNS WITH CERTAIN SPECIFIED CYBERSECURITY STANDARDS; AND FOR RELATED PURPOSES.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MISSISSIPPI:

SECTION 1. (1) As used in this act, the following terms shall have the meanings herein ascribed:

(a) "Covered entity" means a sole proprietorship, partnership, company, corporation, trust, estate, cooperative, association, or a financial institution organized, chartered, or holding a license authorizing operation under the laws of this state, another state, or another country, or other commercial entity.

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

(2) (a) A county, municipality, county hospital, the state or any of its political subdivisions shall not be liable in connection with a cybersecurity incident if the entity adopts cybersecurity standards that:

(i) Safeguard its data, information technology, and information technology resources to ensure availability, confidentiality and integrity; and

(ii) Are consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework.

(b) This statement of immunity shall not be construed to waive any immunity granted to a county, municipality or any other political subdivision under Title 11, Chapter 46, Mississippi Code of 1972.

(3) There shall be a rebuttable presumption that a covered entity or third-party agent that acquires, maintains, stores or uses personal information is not liable in connection with a cybersecurity incident if the covered entity or third-party agent, in good faith, substantially complies with reasonable measures to protect and secure data in electronic form containing personal information and has:

(a) Adopted a cybersecurity program that substantially aligns with the current version of any standards, guidelines or regulations that implement any of the following:

(i) The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity and the implementing regulations or publications.

(ii) NIST special publication 800-171 or its most current update, revision, or replacement.

(iii) NIST special publications 800-53 and 800-53A or their most current update, revision, or replacement.

(iv) The Federal Risk and Authorization Management Program security assessment framework.

(v) The Center for Internet Security (CIS) Critical Security Controls.

(vi) The International Organization for Standardization/International Electrotechnical Commission 27000-series (ISO/IEC 27000) family of standards; or

(b) If regulated by the state or federal government, or both, or if otherwise subject to the requirements of any of the following laws and regulations, substantially aligned its cybersecurity program to the current version of the following, as applicable:

(i) The Health Insurance Portability and Accountability Act of 1996 security requirements in 45 C.F.R. part 160 and part 164 subparts A and C;

(ii) Title V of the Gramm-Leach-Bliley Act of 1999, Public Law 57 No. 106-102, as amended, and the implementing regulations;

(iii) The Federal Information Security Modernization Act of 2014, Public Law No. 113-283.

(iv) The Health Information Technology for Economic and Clinical Health Act requirements in 45 CFR parts 160 and 164.

(4) A covered entity's or third-party agent's alignment with a framework or standard under paragraph (3)(a) or paragraph (3)(b), may be demonstrated by providing documentation or other evidence of an assessment, conducted internally or by a third-party, reflecting that the covered entity's or third-party agent's cybersecurity program is substantially aligned with the relevant framework or standard or with the applicable state or federal law or regulation.

(5) The scale and scope of substantial alignment with a standard, law or regulation under paragraph (3)(a) or paragraph (3)(b) by a covered entity or third-party agent, as applicable, is appropriate if it is based on all of the following factors:

(a) The size and complexity of the covered entity or third-party agent.

(b) The nature and scope of the activities of the covered entity or third-party agent.

(c) The sensitivity of the information to be protected.

(6) Any commercial entity or third-party agent covered by subsection (3) which substantially complies with a combination of industry-recognized cybersecurity frameworks or standards to gain

the presumption against liability pursuant to subsection (3) must, upon the revision of two (2) or more of the frameworks or standards with which the entity complies, adopt the revised frameworks or standards within one (1) year after the latest publication date or latest compliance or effective date stated in the revisions and, if applicable, comply with the Payment Card Industry Data Security Standard (PCI DSS).

(7) In an action in connection with a cybersecurity incident, if the defendant is an entity covered by subsection (2), the plaintiff shall have the initial burden of demonstrating by clear and convincing evidence that the entity was not in substantial compliance with this section.

(8) In an action in connection with a cybersecurity incident, if the defendant is an entity under subsection (3), the defendant has the burden of proof to establish a prima facie case of compliance with industry-recognized cybersecurity frameworks or standards to gain the presumption against liability pursuant to this Act. After the defendant meets its initial burden, the burden of proof will then shift to the plaintiff to overcome this presumption against liability by proving by clear and convincing evidence, that the defendant failed to substantially comply with applicable industry-recognized cybersecurity frameworks or standards.

(9) This act does not establish a private cause of action, including a class action, if a covered entity or third-party agent fails to comply with a provision of this act.

(10) Failure of a county, municipality, county hospital, other political subdivision of the state, or covered entity to substantially implement a cybersecurity program that is in compliance with this section is not evidence of negligence and does not constitute negligence per se.

(11) A choice of law provision in an agreement that designates this state as the governing law shall apply this act, if applicable, to the fullest extent possible in a civil action brought against a person regardless of whether the civil action is brought in this state or another state.

(12) This section shall apply to any civil action filed on or after July 1, 2025.

SECTION 2. This act shall take effect and be in force from and after July 1, 2025.