MISSISSIPPI LEGISLATURE REGULAR SESSION 2024

By: Representative Aguirre

To: Judiciary A

HOUSE BILL NO. 1575

AN ACT TO PROVIDE THAT A LOCAL GOVERNMENTAL ENTITY OR COMMERCIAL ENTITY THAT ADOPTS AND SUBSTANTIALLY COMPLIES WITH CERTAIN CYBERSECURITY STANDARDS IS NOT LIABLE IN CONNECTION WITH A CYBERSECURITY INCIDENT; TO REQUIRE CYBERSECURITY PROGRAMS TO ALIGN WITH THE STANDARDS ESTABLISHED BY CERTAIN NATIONAL ORGANIZATIONS AND THE REQUIREMENTS OF SPECIFIED FEDERAL LAWS; TO DECLARE THAT THIS ACT DOES NOT ESTABLISH A PRIVATE CAUSE OF ACTION AND THAT AN ENTITY'S FAILURE TO COMPLY WITH CYBERSECURITY REQUIREMENTS IS NOT EVIDENCE OF NEGLIGENCE; TO REQUIRE A DEFENDANT THAT IS AN ENTITY COVERED BY THE ACT TO BEAR THE BURDEN OF PROVING SUBSTANTIAL COMPLIANCE WITH STANDARDS IN AN ACTION IN CONNECTION WITH A CYBERSECURITY INCIDENT; AND FOR RELATED PURPOSES.

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

SECTION 1. (1) A county, municipality or other political subdivision that adopts and substantially complies with cybersecurity standards that are consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework, in order to safeguard the entity's data, information technology and information technology resources is not liable in connection with a cybersecurity incident.

(2) A sole proprietorship, partnership, corporation, trust, estate, cooperative, association or other commercial entity or

third-party agent that acquires, maintains, stores or uses personal information is not liable in connection with a cybersecurity incident if the entity 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.

(ii) NIST special publication 800-171.

(iii) NIST special publications 800-53 and 800-53A.

(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 CFR 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.

(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.

(3) The scale and scope of substantial alignment with a standard, law or regulation under paragraph (2)(a) or paragraph (2)(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.

(4) A commercial entity or third-party agent covered by subsection (2) which substantially complies with a combination of industry-recognized cybersecurity frameworks or standards to gain the presumption against liability pursuant to subsection (2) must

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

(5) This section does not establish a private cause of action. Failure of a county, municipality, other political subdivision of the state, or commercial 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.

(6) In an action in connection with a cybersecurity incident, if the defendant is an entity covered by subsection (1) or (2), the defendant has the burden of proof to establish substantial compliance.

SECTION 2. This act shall take effect and be in force from and after July 1, 2024.