MISSISSIPPI LEGISLATURE REGULAR SESSION 2024

By: Senator(s) Boyd, McCaughn

To: Technology; Judiciary, Division A

SENATE BILL NO. 2777

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 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) (a) A county, municipality, the state or any of its political subdivision 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. 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.

(2) There shall be a rebuttable presumption that a sole proprietorship, partnership, company, 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 is in substantial compliance with this section by having:

(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 C.F.R. part 160 and part 164 subparts A and C;

(ii) Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended;

(iii) The Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283; or

(iv) The Health Information Technology for Economic and Clinical Health Act requirements in 45 C.F.R. 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; and

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

(4) Any commercial entity or third-party agent covered by subsection (2) that substantially complies with a combination of industry-recognized cybersecurity frameworks or standards to gain the presumption against liability pursuant to subsection (2) must, upon the revision of two 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 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.

(6) (a) In an action in connection with a cybersecurity incident, if the defendant is an entity under subsection (1), 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.

(b) In an action in connection with a cybersecurity incident, if the defendant is an entity under subsection (2), the defendant has the burden of proof to establish a prima facie case of substantial compliance with this section. After the defendant meets its initial burden, the plaintiff shall have the burden of demonstrating by clear and convincing evidence that the entity was not in substantial compliance with this section.

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