MISSISSIPPI LEGISLATURE REGULAR SESSION 2019

By: Senator(s) Carmichael

To: Insurance;
Appropriations

SENATE BILL NO. 2831
(As Sent to Governor)

AN ACT TO ESTABLISH THE INSURANCE DATA SECURITY LAW; TO PROVIDE THE PURPOSE AND INTENT OF THE ACT; TO DEFINE CERTAIN TERMS USED IN THE ACT; TO REQUIRE INSURANCE LICENSEES IN THIS STATE TO DEVELOP, IMPLEMENT AND MAINTAIN AN INFORMATION SECURITY PROGRAM; TO REQUIRE CERTAIN INVESTIGATION OF A CYBERSECURITY EVENT; TO REQUIRE CERTAIN NOTIFICATION OF A CYBERSECURITY EVENT; TO PROVIDE FOR CERTAIN CONFIDENTIALITY; TO PROVIDE EXCEPTIONS TO THE ACT; TO PROVIDE FOR PENALTIES FOR VIOLATIONS OF THE ACT; TO PROVIDE THE COMMISSIONER OF INSURANCE WITH REGULATORY POWERS NECESSARY TO CARRY OUT THE ACT; AND FOR RELATED PURPOSES.

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

SECTION 1. This act shall be known and may be cited as the "Insurance Data Security Law."

SECTION 2. (1) Notwithstanding any other provision of law, this act establishes the exclusive state standards applicable to licensees for data security, the investigation of a cybersecurity event as defined in Section 3 of this act, and notification to the Commissioner of Insurance.

(2) This act may not be construed to create or imply a private cause of action for violation of its provisions nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this act.

SECTION 3. As used in this act, the following terms shall have the following meanings:

(a) "Authorized individual" means an individual known to and screened by the licensee and determined to be necessary and appropriate to have access to the nonpublic information held by the licensee and its information systems.

(b) "Commissioner" means the Commissioner of Insurance.

(c) "Consumer" means an individual, including, but not limited to, applicants, policyholders, insureds, beneficiaries, claimants and certificate holders, who is a resident of this state and whose nonpublic information is in a licensee's possession, custody or control.

(d) "Cybersecurity event" means an event resulting in unauthorized access to, disruption or misuse of, an information system or nonpublic information stored on such information system. The term "cybersecurity event" does not include the unauthorized acquisition of encrypted nonpublic information if the encryption, process or key is not also acquired, released or used without authorization. "Cybersecurity event" does not include an event with regard to which the licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

(e) "Department" means the Mississippi Insurance Department.

(f) "Encrypted" means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.

(g) "Information security program" means the administrative, technical and physical safeguards that a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of or otherwise handle nonpublic information.

(h) "Information system" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic nonpublic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

(i) "Licensee" means any person licensed, authorized to operate, or registered, or required to be licensed, authorized or registered pursuant to the insurance laws of this state, but shall not include a purchasing group or a risk-retention group chartered and licensed in a state other than this state or a person who is acting as an assuming insurer that is domiciled in another state or jurisdiction.

(j) "Multi-factor authentication" means authentication through verification of at least two (2) of the following types of authentication factors:

(i) Knowledge factors, such as a password;

(ii) Possession factors, such as a token or text message on a mobile phone; or

(iii) Inherence factors, such as a biometric characteristic.

(k) "Nonpublic information" means electronic information that is not publicly available information and is:

(i) Any information concerning a consumer which because of name, number, personal mark or other identifier can be used to identify such consumer, in combination with any one or more of the following data elements:

1. Social security number;

2. Driver's license number or nondriver identification card number;

3. Financial account number, credit or debit card number;

4. Any security code, access code or password that would permit access to a consumer's financial account; or

5. Biometric records;

(ii) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a consumer, that can be used to identify a particular consumer, and that relates to:

1. The past, present or future physical, mental or behavioral health or condition of any consumer or a member of the consumer's family;

2. The provision of health care to any consumer; or

3. Payment for the provision of health care to any consumer.

(l) "Person" means any individual or any nongovernmental entity, including, but not limited to, any nongovernmental partnership, corporation, branch, agency or association.

(m) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law. For the purposes of this definition, a licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether a consumer can direct that the information not be made available to the general public and, if so, that such consumer has not done so.

(n) "Risk assessment" means the risk assessment that each licensee is required to conduct under Section 4(3) of this act.

(o) "State" means the State of Mississippi.

(p) "Third-party service provider" means a person, not otherwise defined as a licensee, who contracts with a licensee to maintain, process, store or otherwise is permitted access to nonpublic information through its provision of services to the licensee.

SECTION 4. (1) Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody or control, each licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment and that contains administrative, technical and physical safeguards for the protection of nonpublic information and the licensee's information system.

(2) A licensee's information security program shall be designed to:

(a) Protect the security and confidentiality of nonpublic information and the security of the information system;

(b) Protect against any threats or hazards to the security or integrity of nonpublic information and the information system;

(c) Protect against unauthorized access to or use of nonpublic information, and minimize the likelihood of harm to any consumer; and

(d) Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed.

(3) The licensee shall:

(a) Designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the licensee who is responsible for the information security program;

(b) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of nonpublic information, including the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers;

(c) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the nonpublic information;

(d) Assess the sufficiency of policies, procedures, information systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the licensee's operations, including:

(i) Employee training and management;

(ii) Information systems, including network and software design, as well as information classification, governance, processing, storage, transmission and disposal; and

(iii) Detecting, preventing and responding to attacks, intrusions or other systems failures; and

(e) Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards' key controls, systems and procedures.

(4) Based on its risk assessment, the licensee shall:

(a) Design its information security program to mitigate the identified risks, commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody or control.

(b) Determine which security measures listed below are appropriate and implement such security measures.

(i) Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of nonpublic information;

(ii) Identify and manage the data, personnel, devices, systems and facilities that enable the organization to achieve business purposes in accordance with their relative

importance to business objectives and the organization's risk strategy;

(iii) Restrict physical access to nonpublic information, only to authorized individuals;

(iv) Protect by encryption or other appropriate means, all nonpublic information while being transmitted over an external network and all nonpublic information stored on a laptop computer or other portable computing or storage device or media;

(v) Adopt secure development practices for in-house developed applications utilized by the licensee;

(vi) Modify the information system in accordance with the licensee's information security program;

(vii) Utilize effective controls, which may include multi-factor authentication procedures for employees accessing nonpublic information;

(viii) Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(ix) Include audit trails within the information security program designed to detect and respond to cybersecurity events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee;

(x) Implement measures to protect against destruction, loss, or damage of nonpublic information due to

environmental hazards, such as fire and water damage or other catastrophes or technological failures; and

(xi) Develop, implement, and maintain procedures for the secure disposal of nonpublic information in any format.

(c) Include cybersecurity risks in the licensee's enterprise risk management process.

(d) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared.

(e) Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in the risk assessment.

(5) If the licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

(a) Require the licensee's executive management or its delegates to develop, implement and maintain the licensee's information security program;

(b) Require the licensee's executive management or its delegates to report in writing at least annually, the following information:

(i) The overall status of the information security program and the licensee's compliance with this act; and

(ii) Material matters related to the information security program, addressing issues such as risk assessment, risk

management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events or violations and management's responses thereto, and recommendations for changes in the information security program;

(c) If executive management delegates any of its responsibilities under this section, it shall oversee the development, implementation and maintenance of the licensee's information security program prepared by the delegate(s) and shall receive a report from the delegate(s) complying with the requirements of the report to the board of directors above.

(6) (a) A licensee shall exercise due diligence in selecting its third-party service provider; and

(b) A licensee shall require a third-party service provider to implement appropriate administrative, technical and physical measures to protect and secure the information systems and nonpublic information that are accessible to, or held by, the third-party service provider.

(7) The licensee shall monitor, evaluate and adjust, as appropriate, the information security program consistent with any relevant changes in technology, the sensitivity of its nonpublic information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to information systems.

(8) (a) As part of its information security program, each licensee shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromises the confidentiality, integrity or availability of nonpublic information in its possession, the licensee's information systems, or the continuing functionality of any aspect of the licensee's business or operations.

(b) Such incident response plan shall address the following areas:

(i) The internal process for responding to a cybersecurity event;

(ii) The goals of the incident response plan;

(iii) The definition of clear roles, responsibilities and levels of decision-making authority;

(iv) External and internal communications and information sharing;

(v) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

(vi) Documentation and reporting regarding cybersecurity events and related incident response activities; and

(vii) The evaluation and revision as necessary of the incident response plan following a cybersecurity event.

(9) Annually, each insurer domiciled in this state shall submit to the commissioner a written statement by February 15,

certifying that the insurer is in compliance with the requirements set forth in this section. Each insurer shall maintain for examination by the department all records, schedules and data supporting this certificate for a period of five (5) years. To the extent an insurer has identified areas, systems or processes that require material improvement, updating or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the commissioner.

SECTION 5. (1) If the licensee learns that a cybersecurity event has or may have occurred, then the licensee, or an outside vendor and/or service provider designated to act on behalf of the licensee, shall conduct a prompt investigation.

(2) During the investigation, the licensee, or an outside vendor and/or service provider designated to act on behalf of the licensee, shall, at a minimum, determine as much of the following information as possible:

(a) Determine whether a cybersecurity event has occurred;

(b) Assess the nature and scope of the cybersecurity event;

(c) Identify any nonpublic information that may have been involved in the cybersecurity event; and

(d) Perform or oversee reasonable measures to restore the security of the information systems compromised in the cybersecurity event in order to prevent further unauthorized acquisition, release or use of nonpublic information in the licensee's possession, custody or control.

(3) If the licensee learns that a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, the licensee will complete the steps listed in subsection (2) of this section or confirm and document that the third-party service provider has completed those steps.

(4) The licensee shall maintain records concerning all cybersecurity events for a period of at least five (5) years from the date of the cybersecurity event and shall produce those records upon demand of the commissioner.

SECTION 6. (1) Each licensee shall notify the commissioner as promptly as possible but in no event later than three (3) business days from a determination that a cybersecurity event involving nonpublic information that is in the possession of a licensee has occurred when either of the following criteria has been met:

(a) This state is the licensee's state of domicile, in the case of an insurer, or this state is the licensee's home state, in the case of a producer, as those terms are defined in Section 83-17-53, and the cybersecurity event has a reasonable likelihood of materially harming a consumer residing in this state

or reasonable likelihood of materially harming any material part of the normal operation(s) of the licensee; or

(b) The licensee reasonably believes that the nonpublic information involved is of two hundred fifty (250) or more consumers residing in this state and that is either of the following:

(i) A cybersecurity event impacting the licensee of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body pursuant to any state or federal law; or

(ii) A cybersecurity event that has a reasonable likelihood of materially harming:

1. Any consumer residing in this state; or

2. Any material part of the normal operation(s) of the licensee.

(2) The licensee shall provide as much of the following information as possible. The licensee shall provide the information in electronic form as directed by the commissioner. The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner regarding material changes to previously provided information relating to the cybersecurity event.

(a) Date of the cybersecurity event;

(b) Description of how the information was exposed, lost, stolen or breached, including the specific roles and responsibilities of third-party service providers, if any;

(c) How the cybersecurity event was discovered;

(d) Whether any lost, stolen, or breached information has been recovered and if so, how this was done;

(e) The identity of the source of the cybersecurity event;

(f) Whether the licensee has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;

(g) Description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information or types of information allowing identification of the consumer;

(h) The period during which the information system was compromised by the cybersecurity event;

(i) The number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner pursuant to this section;

(j) The results of any internal review identifying a lapse in either automated controls or internal procedures, or

confirming that all automated controls or internal procedures were followed;

(k) Description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur;

(l) A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event; and

(m) Name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.

(3) Licensee shall comply with Section 75-24-29, as applicable, and provide a copy of the notice sent to consumers under that statute to the commissioner, when a licensee is required to notify the commissioner under subsection (1) of this section.

(4) (a) In the case of a cybersecurity event in a system maintained by a third-party service provider, of which the licensee has become aware, the licensee shall treat such event as it would under subsection (1) of this section unless the third-party service provider provides the notice required under subsection (1) of this section to the commissioner.

(b) The computation of licensee's deadlines shall begin on the day after the third-party service provider notifies the

licensee of the cybersecurity event or the licensee otherwise has actual knowledge of the cybersecurity event, whichever is sooner.

(c) Nothing in this act shall prevent or abrogate an agreement between a licensee and another licensee, a third-party service provider or any other party to fulfill any of the investigation requirements imposed under Section 5 of this act or notice requirements imposed under this section.

(5) (a) (i) In the case of a cybersecurity event involving nonpublic information that is used by the licensee who is acting as an assuming insurer or in the possession, custody or control of a licensee who is acting as an assuming insurer and that does not have a direct contractual relationship with the affected consumers, the assuming insurer shall notify its affected ceding insurers and the commissioner of its state of domicile within three (3) business days of making the determination that a cybersecurity event has occurred.

(ii) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under Section 75-24-29 and any other notification requirements relating to a cybersecurity event imposed under this section.

(b) (i) In the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of a third-party service provider of a licensee who is an assuming insurer, the assuming insurer shall notify its affected

ceding insurers and the commissioner of its state of domicile within three (3) business days of receiving notice from its third-party service provider that a cybersecurity event has occurred.

(ii) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under Section 75-24-29 and any other notification requirements relating to a cybersecurity event imposed under this section.

(c) Any licensee acting as assuming insurer shall have no other notice obligations relating to a cybersecurity event or other data breach under this section or any other law of this state.

(6) In the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of a licensee who is an insurer or its third-party service provider for which a consumer accessed the insurer's services through an independent insurance producer, and for which consumer notice is required under Section 75-24-29, the insurer shall notify the producers of record of all affected consumers of the cybersecurity event no later than the time at which notice is provided to the affected consumers. The insurer is excused from this obligation for any producers who are not authorized by law or contract to sell, solicit or negotiate on behalf of the insurer, and in those

instances in which the insurer does not have the current producer of record information for any individual consumer.

SECTION 7. (1) The commissioner shall have power to examine and investigate into the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of this act. This power is in addition to the powers which the commissioner has under Section 83-5-201 et seq. Any such investigation or examination shall be conducted pursuant to Section 83-5-201 et seq.

(2) Whenever the commissioner has reason to believe that a licensee has been or is engaged in conduct in this state which violates this act, the commissioner may take action that is necessary or appropriate to enforce the provisions of this act.

SECTION 8. (1) Any documents, materials or other information in the control or possession of the department that are furnished by a licensee or an employee or agent thereof acting on behalf of a licensee pursuant to Section 4(9) of this act, Section 6(2)(b), (c), (d), (e), (h), (j) and (k) of this act, or that are obtained by the commissioner in an investigation or examination pursuant to Section 7 of this act shall be confidential by law and privileged, shall not be subject to the Mississippi Public Records Act, shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the commissioner is authorized to use the documents, materials or other information in the

furtherance of any regulatory or legal action brought as a part of the commissioner's duties. The commissioner shall not otherwise make the documents, materials or other information public without the prior written consent of the licensee.

(2) Neither the commissioner nor any person who received documents, materials or other information while acting under the authority of the commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials or information subject to subsection (1) of this section.

(3) In order to assist in the performance of the commissioner's duties under this act, the commissioner:

(a) May share documents, materials or other information, including the confidential and privileged documents, materials or information subject to subsection (1) of this section, with other state, federal and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal and international law enforcement authorities, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material or other information;

(b) May receive documents, materials or information, including otherwise confidential and privileged documents, materials or information, from the National Association of

Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material or information;

(c) May share documents, materials or other information subject to subsection (1) of this section with a third-party consultant or vendor provided the consultant agrees in writing to maintain the confidentiality and privileged status of the document, material or other information; and

(d) May enter into agreements governing sharing and use of information consistent with this subsection (3).

(4) No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the commissioner under this section or as a result of sharing as authorized in subsection (3) of this section.

(5) Nothing in this act shall prohibit the commissioner from releasing final, adjudicated actions that are open to public inspection pursuant to the Mississippi Public Records Act, to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates or subsidiaries.

(6) Documents, materials or other information in the possession or control of the National Association of Insurance Commissioners or a third-party consultant or vendor pursuant to this act shall be confidential by law and privileged, shall not be subject to the Mississippi Public Records Act, shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action.

SECTION 9. (1) The following exceptions shall apply to this act:

(a) A licensee meeting any of the following criteria is exempt from Sections 4, 5(3) and 6(4)(a) and (b) of this act:

(i) Fewer than fifty (50) employees, excluding any independent contractors;

(ii) Less than Five Million Dollars ($5,000,000.00) in gross annual revenue;

(iii) Less than Ten Million Dollars ($10,000,000.00) in year-end total assets; or

(iv) Insurance producers and adjusters.

(b) A licensee subject to Public Law 104-191, 110 Stat. 1936, enacted August 21, 1996, (Health Insurance Portability and Accountability Act) that has established and maintains an information security program pursuant to such statutes, rules, regulations, procedures or guidelines established thereunder, will be considered to meet the requirements of Section 4 of this act,

provided that the licensee is compliant with, and submits a written statement certifying its compliance with, the same.

(c) An employee, agent, representative or designee of a licensee, who is also a licensee, is exempt from Section 4 of this act and need not develop its own information security program to the extent that the employee, agent, representative or designee is covered by the information security program of the other licensee.

(d) A licensee affiliated with a depository institution that maintains an information security program in compliance with the *Interagency Guidelines Establishing Standards for Safeguarding Customer Information* as set forth pursuant to Sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805) shall be considered to meet the requirements of Section 4 of this act, provided that the licensee produces, upon request, documentation satisfactory to the commissioner that independently validates the affiliated depository institution's adoption of an information security program that satisfies the Interagency Guidelines.

(2) In the event that a licensee ceases to qualify for an exception, such licensee shall have one hundred eighty (180) days to comply with this act.

SECTION 10. In the case of a violation of this act, a licensee may be penalized in accordance with Section 83-5-85.

SECTION 11. The commissioner may issue such regulations as shall be necessary to carry out the provisions of this act.

SECTION 12. If any provisions of this act or the application thereof to any person or circumstance is for any reason held to be invalid, the remainder of the act and the application of such provision to other persons or circumstances shall not be affected thereby.

SECTION 13. Licensees shall have one (1) year from the effective date of this act to implement Section 4 of this act and two (2) years from the effective date of this act to implement Section 4(6) of this act.

SECTION 14. This act shall take effect and be in force from and after July 1, 2019.