ENROLLED

2020 Regular Session

ACT No. 283

HOUSE BILL NO. 614

BY REPRESENTATIVE SEABAUGH

AN ACT

To amend and reenact R.S. 44:4.1(B)(11) and to enact Chapter 21 of Title 22 of the Louisiana Revised Statutes of 1950, to be comprised of R.S. 22:2501 through 2511, relative to data security for persons regulated by the commissioner of insurance; to define key terms; to require licensees to maintain an information security program; to provide for the investigation of data security breaches; to require notification of data security breaches; to provide for the confidentiality of certain information; to authorize penalties for violations; to provide for defenses; to establish a public records exception; to provide for effectiveness; and to provide for related matters.

Be it enacted by the Legislature of Louisiana:

Section 1. Chapter 21 of Title 22 of the Louisiana Revised Statutes of 1950, comprised of R.S. 22:2501 through 2511, is hereby enacted to read as follows:

CHAPTER 21. INSURANCE DATA SECURITY

§2501. Short title

This Chapter shall be known and may be cited as the "Insurance Data Security Law".

§2502. Purpose and intent

A. This Chapter establishes the exclusive standards for this state applicable to licensees for data security, the investigation of a cybersecurity event, and notification to the commissioner.

B. This Chapter shall not be construed to create or imply a private cause of action for violation of its provisions nor shall it be construed to curtail a private cause of action that would otherwise exist in the absence of this Chapter.

§2503. Definitions

As used in this Chapter, the following definitions apply:

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

(2) "Consumer" means a natural person who is a resident of this state and whose nonpublic information is in a licensee's possession, custody, or control.

(3)(a) "Cybersecurity event" means an event resulting in unauthorized access to or disruption or misuse of an information system or nonpublic information stored on an information system.

(b) "Cybersecurity event" shall not include either of the following:

(i) The unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization.

(ii) 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.

(4) "Encrypted" means the transformation of data into a form that has a low probability of assigning meaning without the use of a protective process or key.

(5) "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.

(6) "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. "Information system" shall include any specialized system such as industrial or process controls

systems, telephone switching and private branch exchange systems, and environmental control systems.

(7)(a) "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.

(b) "Licensee" shall not include either of the following:

(i) A purchasing group or a risk retention group chartered and licensed in a state other than this state.

(ii) A person that is acting as an assuming insurer that is domiciled in another state or jurisdiction.

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

(a) Knowledge factors, such as a password.

(b) Possession factors, such as a token or text message on a mobile phone.

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

(9) "Nonpublic information" means electronic information that is not publicly available information and is any of the following:

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

(i) Social Security number.

(ii) Driver's license number or nondriver identification card number.

(iii) Financial account number or credit or debit card number.

(iv) Any security code, access code, or password that would permit access to a consumer's financial account.

(v) Biometric records.

(b) Any information or data, except age or gender, in any form or medium created by or derived from a healthcare provider or a consumer, that can be used to identify a particular consumer, and that relates to any of the following:

(i) The past, present, or future physical, mental, or behavioral health or condition of any consumer.

(ii) The provision of health care to any consumer.

(iii) Payment for the provision of health care to any consumer.

(10) "Person" means any natural person or any nongovernmental juridical person.

(11) "Publicly available information" means any information that a licensee reasonably believes is lawfully made available to the general public when all of the following occur:

(a) The information is available to the general public from any of the following sources:

(i) Federal, state, or local government records.

(ii) Widely distributed media.

(iii) Disclosures to the general public required to be made by federal, state, or local law.

(b) 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 all of the following:

(i) That the information is of a type that is available to the general public.

(ii) That a consumer who can direct that the information not be made available to the general public has not done so.

(12) "Risk assessment" means the risk assessment that each licensee is required to conduct pursuant to R.S. 22:2504(C).

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

§2504. Information security program

A. A licensee shall develop, implement, and maintain a comprehensive, written information security program which satisfies all of the following criteria:

(1) Is based on the licensee's risk assessment.

(2) Contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

(3) Is commensurate with all of the following:

(a) Size and complexity of the licensee.

(b) Nature and scope of the licensee's activities including its use of third-party service providers.

(c) Sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control.

B. A licensee's information security program shall be designed to do all of the following:

(1) Protect the security and confidentiality of nonpublic information and the security of the information system.

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

(3) Protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to any consumer.

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

C. A licensee shall conduct a risk assessment by doing all of the following:

(1) Designate one or more employees, an affiliate, or an outside vendor to act on behalf of the licensee and to be responsible for the information security program.

(2) 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.

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

(4) 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 all of the following:

(a) Employee training and management.

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

(c) Detecting, preventing, and responding to attacks, intrusions, or other systems failures.

(5) 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.

D. Based on the licensee's risk assessment, a licensee shall do all of the following:

(1) Design an 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 the 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.

(2) Implement all of the following security measures that the licensee determines are appropriate:

(a) 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.

(b) 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.

(c) Restrict physical access to nonpublic information to authorized individuals.

(d) 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.

(e) Adopt secure development practices for in-house developed applications used by the licensee and procedures for evaluating, assessing, or testing the security of externally developed applications used by the licensee.

(f) Modify the information system in accordance with the licensee's information security program.

(g) Use effective controls, which may include multifactor authentication procedures for any individual accessing nonpublic information.

(h) Regularly test and monitor systems and procedures to detect actual and attempted attacks on or intrusions into information systems.

(i) 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.

(j) 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.

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

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

(4) Stay informed regarding emerging threats or vulnerabilities.

(5) Use reasonable security measures when sharing information relative to the character of the sharing and the type of information shared.

(6) Provide its personnel with cybersecurity awareness training that reflects current risks identified by the licensee in the risk assessment.

E. If a licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum, require a licensee's executive management or its delegates to do all of the following:

(1) Develop, implement, and maintain the licensee's information security program.

(2) Report in writing, at least annually, all of the following information:

(a) The overall status of the information security program and the licensee's compliance with this Chapter.

(b) 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.

(3) If executive management delegates any of the responsibilities provided for in this Section, management shall oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegates and shall receive a report from the delegates complying with the requirements of the report to the board of directors above.

F. With regard to third-party service providers, a licensee shall do all of the following:

(1) Exercise due diligence in selecting a third-party service provider.

(2) Require third-party service providers 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.

G. A 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, including but not limited to mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

H.(1) 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.

(2) The incident response plan shall address all of the following:

(a) The internal process for responding to a cybersecurity event.

(b) The goals of the incident response plan.

(c) The definition of clear roles, responsibilities, and levels of decisionmaking authority.

(d) External and internal communications and information sharing.

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

(f) Documentation and reporting regarding cybersecurity events and related incident response activities.

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

I.(1) 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 R.S. 22:2504.

(2) Each insurer shall maintain for examination by the commissioner all records, schedules, and data supporting the certificate for a period of five years.

(3) To the extent an insurer identifies areas, systems, or processes that require material improvement, update, or redesign, the insurer shall document the identification and the remediation efforts planned and underway to address the areas, systems, or processes. The documentation shall be made available for inspection by the commissioner.

§2505. Investigation of a cybersecurity event

A. If a licensee learns that a cybersecurity event has or may have occurred, the licensee, or an outside vendor or service provider designated to act on behalf of the licensee, shall conduct a prompt investigation.

B. During the investigation, the licensee, or an outside vendor or service provider designated to act on behalf of the licensee, shall do all of the following to the extent possible:

(1) Determine whether a cybersecurity event has occurred.

(2) Assess the nature and scope of the cybersecurity event.

(3) Identify any nonpublic information that may have been involved in the cybersecurity event.

(4) Undertake 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.

C. If a licensee learns that a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, the licensee shall make reasonable efforts to complete the steps required pursuant to Subsection B of this Section or make reasonable efforts to confirm and document that the third-party service provider has completed those steps.

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

§2506. Notification of a cybersecurity event

A. A licensee shall notify the commissioner without unreasonable delay but in no event later than three business days from a determination that a cybersecurity event involving nonpublic information that is in the possession of the licensee has occurred when either of the following criteria has been met:

(1) 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, an adjuster, or public adjuster as those terms are defined in R.S. 22:1542, 1661, or 1692, and the cybersecurity event has reasonable likelihood of materially harming either of the following:

(a) Any consumer residing in this state.

(b) Any material part of the normal operations of the licensee.

(2) A licensee reasonably believes that the nonpublic information involved is for two hundred fifty or more consumers residing in this state and that either of the following has occurred:

(a) A cybersecurity event affecting 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.

(b) A cybersecurity event that has a reasonable likelihood of materially harming any of the following:

(i) Any consumer residing in this state.

(ii) Any material part of the normal operations of the licensee.

B.(1) 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 relative to the cybersecurity event.

(2) The licensee making the notification required in Subsection A of this Section shall provide as much of the following information as possible in electronic form as directed by the commissioner:

(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 any third-party service providers.

(c) How the cybersecurity event was discovered.

(d) Whether any lost, stolen, or breached information has been recovered and, if so, how reocvery was accomplished.

(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 when the notification was provided.

(g)(i) Description of the specific types of information acquired without authorization.

(ii) For the purposes of this Subparagraph, "specific types of information" means particular data elements including but not limited to types of medical information, types of financial information, or types of information allowing identification of the consumer.

(h) The period during which the cybersecurity event compromised the information system.

(i)(i) The total number of consumers in this state affected by the cybersecurity event.

(ii) 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.

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

C. A licensee shall comply with the Database Security Breach Notification Law, R.S. 51:3071 et seq., as applicable, and shall provide to the commissioner a copy of the notice sent to consumers if the licensee is required to notify the commissioner pursuant to Subsection A of this Section.

D.(1) In the case of a cybersecurity event in a system maintained by a third-party service provider of which the licensee has become aware, all of the following shall apply:

(a) The licensee shall treat the cybersecurity event as it would pursuant to Subsection A of this Section, unless the third-party service provider gives the notice required in Subsection A of this Section.

(b) The computation of the 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 occurs first.

(2) Nothing in this Chapter shall be construed to 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 pursuant to R.S. 22:2505 or notice requirements pursuant to this Section.

E.(1)(a) In the case of a cybersecurity event involving nonpublic information used by a licensee acting as an assuming insurer or in the possession, custody, or control of a licensee 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 business days of making the determination that a cybersecurity event has occurred.

(b) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements pursuant to the Database Security Breach Notification Law and any other notification requirements relating to a cybersecurity event pursuant to this Section.

(2)(a) 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 that is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the commissioner of its state of domicile within three business days of receiving notice from its third-party service provider that a cybersecurity event has occurred.

(b) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements pursuant to the Database Security Breach Notification Law and any other notification requirements relating to a cybersecurity event pursuant to this Section.

F. In the case of a cybersecurity event involving nonpublic information that is in the possession, custody, or control of a licensee that 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 by the Database Security Breach Notification Law, 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 shall be 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 an individual consumer.

§2507. Powers of the commissioner

A. The commissioner may 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 Chapter. This power is in addition to the powers which the commissioner has pursuant to R.S. 22:1981, 1983, and 1984. Any investigation or examination shall be conducted pursuant to R.S. 22:1983 and 1984.

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

§2508. Confidentiality

A. Any documents, materials, or other information in the control or possession of the commissioner that are furnished by a licensee or an employee or agent acting on behalf of a licensee pursuant to R.S. 22:2504 or 2506 or that are obtained by the commissioner in an investigation or examination pursuant to R.S. 22:2507 shall be confidential by law and privileged, shall not be subject to release pursuant to the Public Records Law, R.S. 44:1 et seq., 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 may 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.

B. Neither the commissioner nor any person who received documents, materials, or other information while acting pursuant to the authority of the commissioner shall testify in any private civil action concerning any confidential documents, materials, or information subject to Subsection A of this Section.

C. In order to assist in the performance of the commissioner's duties pursuant to this Chapter, the commissioner may do any of the following:

(1) Share documents, materials, or other information, including the confidential and privileged documents, materials, or information subject to Subsection A of this Section, with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners (NAIC), its affiliates, or subsidiaries, and with state, federal, and international law enforcement

authorities, if the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information.

(2)(a) Receive documents, materials, or information, including otherwise confidential and privileged documents, materials, or information, from the NAIC, its affiliates, or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions.

(b) The commissioner shall maintain as confidential or privileged any document, material, or information received with notice or the understanding that the document, material, or information is confidential or privileged pursuant to the laws of the jurisdiction that is the source of the document, material, or information.

(3) Share documents, materials, or other information subject to Subsection A of this Section with a third-party consultant or vendor if the consultant agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information.

(4) Enter into agreements governing the sharing and use of information consistent with this Subsection.

D. 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 pursuant to this Section or as a result of sharing pursuant to Subsection C of this Section.

E. Nothing in this Chapter shall be construed to prohibit the commissioner from releasing final, adjudicated actions that are open to public inspection pursuant to the Public Records Law or to a database or other clearinghouse service maintained by the NAIC, its affiliates, or subsidiaries.

F. Documents, materials, or other information in the possession or control of the NAIC or a third-party consultant or vendor pursuant to this Chapter shall be confidential by law and privileged, shall not be subject to release pursuant to the Public Records Law, R.S. 44:1 et seq., shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action.

§2509. Exemptions

A. A licensee shall be exempt from the provisions of R.S. 22:2504 if the licensee meets any of the following criteria:

(1) Having fewer than twenty-five employees.

(2) Less than five million dollars in gross annual revenue.

(3) Less than ten million dollars in year-end total assets.

(4) Being subject to the Health Insurance Portability and Accountability Act, Pub.L. 104-191, 110 Stat. 1936, and doing all of the following:

(a) Establishing and maintaining an information security program pursuant to any statutes, rules, regulations, procedures, or guidelines established pursuant to the Health Insurance Portability and Accountability Act.

(b) Complying with and submitting, upon request of the commissioner, a written statement certifying compliance with the information security program established and maintained pursuant to Subparagraph (a) of this Paragraph.

(5) Being an employee, agent, representative, or designee of a licensee, who is also a licensee, to the extent that the employee, agent, representative, or designee is covered by the information security program of the other licensee.

(6) Being affiliated with a depository institution subject to the Interagency Guidelines Establishing Information Security Standards pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 and 6805, and doing all of the following:

(a) Establishing and maintaining an information security program pursuant to any statutes, rules, regulations, procedures, or guidelines established pursuant to the Gramm-Leach-Bliley Act.

(b) Complying with and submitting, upon request of the commissioner, a written statement certifying compliance with the information security program established and maintained pursuant to Subparagraph (a) of this Paragraph.

(7) Being subject to another jurisdiction approved by the commissioner and doing all of the following:

(a) Establishing and maintaining an information security program pursuant to such statutes, rules, regulations, procedures, or guidelines established by another jurisdiction.

(b) Complying with and submitting a written statement certifying its compliance with the information security program established and maintained pursuant to Subparagraph (a) of this Paragraph.

B. In the event that a licensee ceases to qualify for an exemption pursuant to Subsection A of this Section, the licensee shall have one hundred eighty days to comply with the provisions of this Chapter.

C. A licensee that is subject to R.S. 51:3076 shall be exempt from the provisions of R.S. 22:2506 if the licensee does all of the following:

(1) Notifies affected consumers of cybersecurity events relating to the licensee's insurance business in a manner consistent with the requirements of the Gramm-Leach-Bliley Act.

(2) Notifies the commissioner of cybersecurity events relating to the licensee's insurance business in a manner consistent with and at the same time as the notice the licensee gives to federal regulatory authorities.

§2510. Penalties

In the case of a violation of this Chapter, the commissioner may impose a penalty pursuant to R.S. 22:18.

§2511. Defenses

A licensee that satisfies the provisions of this Chapter may assert an affirmative defense to any cause of action arising in tort that is brought pursuant to the laws of this state or in the courts of this state and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning nonpublic information.

Section 2. R.S. 44:4.1(B)(11) is hereby amended and reenacted to read as follows:

§4.1. Exceptions

* * *

B. The legislature further recognizes that there exist exceptions, exemptions, and limitations to the laws pertaining to public records throughout the revised statutes and codes of this state. Therefore, the following exceptions, exemptions, and limitations are hereby continued in effect by incorporation into this Chapter by citation:

* * *

(11) R.S. 22:2, 14, 31, 42.1, 88, 244, 263, 265, 461, 550.7, 571, 572, 572.1, 574, 618, 639, 691.4, 691.5, 691.6, 691.7, 691.8, 691.9, 691.9.1, 691.10, 691.38, 691.56, 732, 752, 753, 771, 834, 972(D), 976, 1008, 1019.2, 1203, 1290.1, 1460, 1464, 1466, 1488, 1546, 1559, 1566(D), 1644, 1656, 1657.1, 1723, 1796, 1801, 1808.3, 1927, 1929, 1983, 1984, 2036, 2045, 2056, 2085, 2091, 2293, 2303<u>, 2508</u>

* * *

Section 3.(A) The provisions of R.S. 22:2504(F) as enacted by Section 1 of this Act shall become effective on August 1, 2022.

(B) The remaining provisions of R.S. 22:2504 as enacted by Section 1 of this Act shall become effective on August 1, 2021.

Section 4. This Section and Sections 1, 2, and 3 shall become effective on August 1, 2020.

SPEAKER OF THE HOUSE OF REPRESENTATIVES

PRESIDENT OF THE SENATE

GOVERNOR OF THE STATE OF LOUISIANA

APPROVED: ____________________